Position-Based Routing and MAC Protocols for Wireless Ad-Hoc Networks

Hadi Noureddine

A Thesis Submitted in fulfilment of the requirements
For the Degree of Doctor of Philosophy (PhD)

Electronic and Computer Engineering
School of Engineering and Design
Brunel University, London
United Kingdom

-May 2011-

Abstract

This thesis presents the Forecasting Routing Technique (FORTEL), a routing protocol for Mobile Ad-Hoc Networks (MANETs) based on the nodes' Location Information. FORTEL stores the nodes' location information in the Location Table (LT) in order to construct routes between the source and the destination nodes. FORTEL follows the source routing strategy, which has rarely been applied in position-based routing. According to the source routing strategy, the end-to-end route is attached to the packet, therefore, the processing cost, in regards to the intermediate nodes that simply relay the packet according to route, is minimized. FORTEL's key mechanisms include: first, the location update scheme, employed to keep the LT entries up-to-date with the network topology. Besides the mobility variation and the constant rate location update schemes applied, a window location update scheme is presented to increase the LT's information accuracy. Second, the switching mechanism, between "Hello" message and location update employed, to reduce the protocol's routing overhead. Third and most important is the route computation mechanism, which is integrated with a topology forecasting technique to construct up-to-date routes between the communication peers, aiming to achieve high delivery rate and increase the protocol robustness against the nodes' movement. FORTEL demonstrates higher performance as compared to other MANET's routing protocols, and it delivers up to 20% more packets than AODV and up to 60 % more than DSR and OLSR, while maintaining low levels of routing overhead and network delay at the same time. The effectiveness of the window update scheme is also discussed, and it proves to increase FORTEL's delivery rate by up to 30% as compared to the other update schemes.

A common and frequently occurring phenomenon, in wireless networks, is the Hidden Terminal problem that significantly impacts the communication performance and the efficiency of the routing and MAC protocols. Beaconless routing approach in MANETs, which delivers data packets without prior knowledge of any sort `of information, suffers from packet duplication caused by the hidden nodes during the contention process. Moreover, the throughput of the IEEE MAC protocol decreases dramatically when the hidden terminal problem occurs. RTS/CTS mechanism fails to eliminate the problem and can further degrade the network's performance by introducing additional overhead. To tackle these challenges, this thesis presents two techniques, the Sender Suppression Algorithm and the Location-Aided MAC, where both rely on the nodes' position to eliminate packet duplication in the beaconless routing and improve the performance of the 802.11 MAC respectively. Both schemes are based on the concept of grouping the nodes into zones and assign different time delay to each one. According to the Sender Suppression Algorithm, the sender's forwarding area is divided into three zones, therefore, the local timer, set to define the time that the receiver has to wait before responding to the sender's transmission, is added to the assigned zone delay. Following the first response, the sender interferes and suppresses the receivers with active timer of. On the other hand, the Location-Aided MAC, essentially a hybrid MAC, combines the concepts of time division and carrier sensing. The radio range of the wireless receiver is partitioned into four zones with different zone delays assigned to each zone. Channel access within the zone is purely controlled by CSMA/CA protocol, while it is time-based amongst zones. The effectiveness of the proposed techniques is demonstrated through simulation tests. Location-Aided MAC considerably improves the network's throughput compared to CSMA/CA and RTS/CTS. However, remarkable results come when the proposed technique and the RTS/CTS are combined, which achieves up to 20% more throughput as compared to the standalone RTS/CTS. Finally, the thesis presents a novel link lifetime estimation method for greedy forwarding to compute the link duration between two nodes. Based on a newly introduced Stability-Aware Greedy (SAG) scheme, the proposed method incorporates the destination node in the computation process and thus has a significant advantage over the conventional method, which only considers the information of the nodes composing the link.

To My Parents

Acknowledgments

First of all, I would like to express my appreciation and gratefulness to Altajir Trust for funding my PhD study.

I would like to thank my supervisor Professor Hamed Al-Raweshidy for his valuable advices and guidance during the PhD period. He has been very helpful and supportive for all these years.

I am thankful to my second supervisor Dr. Qiang Ni for his encouragement and support. My gratitude goes to my colleagues in the Wireless Networks and Communications Centre (WNCC), who have been supportive throughout this period. I would like to acknowledge the great attitude of all the staff members that I have interacted with at Brunel University and specifically in the department of Electronic and Computer Engineering.

All my relatives in Lebanon have played an important role in supporting me throughout this period. I would like to thank them all, especially my cousins Dr. Ali and Abdallah Noureddine.

I am very grateful to all my friends who always show their care and support. A special thank to my best friends Abbass Abou Abbass, Hussein Chammout and Youssef Fadel whose support was precious.

To Vasiliki, thank you for being in my life. Thank you for all of your support during this period, for sharing all the tough and stressful moments I went through to draw to this successful end.

Finally, to my parents, sisters, brother and brother-in-law: thank you for being beside me as a source of care, love, motivation and encouragement, which travel the distance that separates us, and fill me with patience and commitment. Especially to my father, who has always been my main inspiration and always urged me to pursue higher level of education and complete my PhD studies.

Table of Contents

List of Figures

List of tables

List of Abbreviations

AODV	Ad hoc On-demand Distance Vector
AP	Access Point
BSS	Basic Service Set
CAP	Controlled Access Period
CBF	Contention-Based Forwarding
CFP	Contention Free Period
CS	Carrier Sensing
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CTS	Clear To Send
CW	Contention Window
DCF	Distributed Coordination Function
DCT	Destination Connectivity Tree
DIFS	DCF IFS
DLA	Distributed Location Aided
DREAM	Distance Routing Effect Algorithm for Mobility
DS	Distribution System
DSR	Dynamic Source Routing
EIFS	Extended IFS
ERP	Extended Rate PHY
FDCT	Forecasted Destination Connectivity Tree
FLT	Forecasted Location Table
FORTEL	Forecasting Routing Technique using Location Information
FORTEL-B	FORTEL with Mobility variation update scheme
FORTEL-C	FORTEL with constant rate update scheme
FORTEL-W	FORTEL with window update scheme
FORTEL-E	FORTEL Epidemic
IBSS	Independent Basic Service Set
IFS	Inter Frame Spaces
LAR	Location-Aided Routing
LR-WPAN	Low-Rate Wireless Personal Area Network
LT	Location Table
MAC	Medium Access Control
MANET	Mobile Ad-hoc Network
MPDU	MAC Protocol Data Unit
MPR	Multipoint relays
MSDU	MAC Service Data Unit
NAV	Network Allocation Vector
OLSR	Optimized Link State Routing
OSI	Open Systems Interconnections
PCF	Point Coordinated Function
PIFS	PCF IFS
PMD	PHY Media Dependent
PPDU	PLCP protocol data unit
PSDU	PLCP Service Data Unit
QoS	Quality of Service
RREP	Route Reply

RREQ	Route Request
RTS	Request To Send
SAG	Stability Aware Greedy
SIFS	Short IFS
SSA	Sender Suppression Algorithm
STA	(IEEE 802.11 conformant) Station
TTL	Time to Live
VANET	Vehicular Ad-hoc Network
WLAN	Wireless Local Area Network
WPAN	Wireless Personal Area Network

Chapter 1

Introduction

1.1 Aims of research

This thesis aims at the following:

- Designing and developing a new position-based source routing protocol for Mobile Ad-hoc Networks (MANETs), with the aim of increasing the routing deliverability in mobile networks by incorporating mobility prediction. The protocol is expected to be adaptive to the topology variation of the mobile network and responds to the nodes' movement. Ultimately, the high deliverability of the new protocol should be achieved with a low routing overhead, while maintaining a tolerable level of network delay.
- Improving the beaconless routing protocols by eliminating packet duplication due to the hidden nodes during the contention process. This can be achieved by developing a suppression technique to control the receiver's response to the sender's transmission. The suppression technique is anticipated to eliminate the multiple transmissions, at the lowest cost possible, with no other significant addition required.
- Developing a new link lifetime estimation method for greedy forwarding. The estimation method will carefully consider the special characteristics of such forwarding strategy to improve, in consequence, the network's performance.
- Designing a MAC protocol to reduce the effect of the hidden terminal problem by taking into consideration the nodes' position. Packet retransmission is expected to be reduced

to the minimum if possible. Finally, the proposed scheme should require no great modification to MAC standard, in order to increase the algorithm's applicability.

1.2 Main contributions

The key contributions of this work are summarised in the following points:

1. A new position-based routing protocol called FORTEL, specifically designed for mobility, makes use of the nodes' location information to forecast the network topology and construct end-to-end routes to the desired destination. FORTEL employs a source routing strategy, according to which the end-to-end route is included in the data packet, therefore, the intermediate nodes simply take on the role of relaying the packet. This source strategy has rarely been introduced in geographical routing protocol.
    a. FORTEL employs a novel update scheme to disseminate the location information throughout the network based on the concept of window update. In order to increase the routing performance, the window update scheme is designed to keep each and every node in the network aware of the location information changes occurring to the other nodes.
    b. In addition, a mechanism for switching between "Hello" messages and location update packets is introduced to reduce the amount of control messages.
    c. The routes leading to the destination nodes are constructed at the source nodes using a newly modified version of Dijkstra algorithm.
2. A Suppression technique for beaconless routing that eliminates packet duplication caused by hidden nodes during the contention process.
3. A new Link lifetime estimation method, specifically designed for greedy forwarding, to estimate the lifetime of the link between two neighbouring nodes.
4. A greedy forwarding scheme called Stability-Aware Greedy forwarding (SAG) that considers the link lifetime in the forwarding decision.
5. A hybrid time division and carrier sensing MAC protocol to mitigate the effect of hidden terminal problem on the network's performance. The protocol is based on the Distributed Location-Aided (DLA) algorithm that makes use of the nodes position to control their channel access.

1.3 Research methodology

The research methodology followed in this thesis, is summarized as follows:

1. An overview of the IEEE 802.11 WLAN [1] technology, highlighting the basic of the MAC and PHY layers' operations, to facilitate the design of the proposed Location-Aided MAC protocol.
2. An introduction to Mobile Ad-hoc Networks (MANETs) is further presented, allowing the development of FORTEL protocol, the added improvement to the beaconless routing schemes, as well as the design of the link lifetime estimation method.
3. A comprehensive analysis of various published work on routing protocols for MANETs, mainly position-based protocols, highlighting the various issues that need to be tackled in the proposed techniques.
4. Reviewing the different beaconless routing schemes in MANETs, specifically those who study includes hidden node suppression techniques.
5. A review of the existing link lifetime estimation methods is conducted, particularly those that involve location information.
6. Various MAC collision avoidance techniques developed to eliminate or reduce the effect of hidden nodes have been reviewed.
7. Designing FORTEL protocol, Sender Suppression Algorithm (SSA), Link lifetime prediction method and LA-MAC protocol.
8. Developing a simulation model for the proposed protocols and schemes in OPNET [2] network simulator. The development phase includes the design of new "process models", which consist of the Finite State Machine (FSM) and the protocols' specifications that are implemented with the help of a Proto-C/C++ programming language.
9. Validation of the developed models and the protocols' performance in the simulation's environment.
10. Performance evaluation of the proposed solutions with existing work.
11. Analysis of the evaluation results.

1.4 Thesis structure

This thesis consists of seven chapters.

Following the introductory Chapter 1, Chapter 2 gives a brief overview of the IEEE 802.11 WLAN technology and the principles and characteristics of MANETs. The fundamentals of the MAC and PHY layers and the main terminology used in the standard are given in chapter 2 along with a summary of the DCF and PCF coordination functions. Besides, the advantages of MANETs and the various classes of routing protocols, with strong focus on the position-based protocols, which form the literature of Chapter 3 are also being elaborated.

Chapter 3 provides a detailed description of the different components of FORTEL protocol. It also describes FORTEL's simulation model and explains the output of the comparative analysis amongst different versions of FORTEL and amongst FORTEL and existing MANETs' protocols in various scenarios.

Chapter 4 studies the different beaconless routing schemes and analyses the existing suppression techniques and their implications on the protocol's performance. The chapter also describes the simulation model and the output results of the comparison between the proposed technique and existing suppression schemes.

Chapter 5 presents the existing link lifetime estimation methods and reviews the routing protocols that make use of the link lifetime or link stability in the routing process. The chapter discusses the drawbacks of the existing link lifetime estimation method on greedy forwarding [3], [4], [5] and [6], followed by a description of the proposed estimation method and the Stability Aware Greedy (SAG) forwarding scheme. At the end of the chapter, various simulations are run to evaluate the proposed estimation method's performance by the use of SAG scheme.

Chapter 6 gives a detailed insight on the existing mechanisms designed to mitigate the hidden terminal problem. The different aspects of the Distributed Location-Aided (DLA) algorithm are then described, followed by an analysis of the simulation's results.

Eventually, the research findings of the thesis along with the future work are presented in Chapter 7.

References

[1] "IEEE Standard for Information technology-Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," IEEE Std 802.11-2007 (Revision of IEEE Std 802.11-1999), pp.C1-1184, June 12 2007.

[2] OPNET Modeler, OPNET Technologies Incorporation. www.opnet.com

[3] H. Takagi and L. Kleinrock, “Optimal transmission ranges for randomly distributed packet radio terminals,” IEEE Transactions on Communications, Vol. 32, No. 3, pp. 246–257, March 1984.

[4] G.G. Finn, “Routing and Addressing Problems in Large Metropolitan-Scale Internetworks”, Research Report ISU/RR-87-180, Inst. For Scientific information, Mar. 1987.

[5] T.-C. Hou V. Li , “Transmission Range Control in Multihop Packet Radio Networks,” IEEE Transactions on Communications, Vol. 34, No. 1, pp. 38- 44, Jan 1986.

[6] E. Kranakis, H. Singh, and J. Urrutia, “Compass routing on geometric networks,” in the 11th Canadian Conference on Computation Geometry (CCCG 99), 1999.

Chapter 2

IEEE 802.11 Mobile Ad-Hoc Networks: Principles, Characteristics and Routing

2.1 Introduction

The majority of Mobile Ad-Hoc Networks' (MANETs) research work has been developed based on the specifications of WLAN Medium Access Control (MAC) and Physical (PHY) layers. Hence, when studying Mobile Ad-Hoc Networks (MANETs), we implicitly study the Wireless Local Area Networks (WLAN) technology. WLAN has become the widely known technology for wireless networks. Two modes of operations are supported: Infrastructure mode and infrastructure-less mode, also known as ad-hoc. The infrastructure mode requires the existence of a centralised unit, Access Point (AP) to provide the access control to the wireless medium, while in ad-hoc mode the communication between the wireless nodes depends on whether they are within the radio range of each other.

MANETs consist of a collection of wireless hosts spread across a geographical area, connected to each other via wireless links, in the absence of any sort of infrastructure. They are self-organizing, self-configuring and self-healing wireless networks. Disaster recovery, conference and battle-field are some of the environments where MANETs' can be applied that require a rapid deployment. Each wireless host can directly communicate with all the hosts located within its transmission range. When the destination is beyond the source node coverage, multi-hop communication is applied to successfully relay the data traffic to the destination through the intermediate hosts. The main challenge that routing algorithms have to

face in ad-hoc networks is the frequent topology changes that occur due to mobility. Therefore, any routing scheme has to be robust to changes in topology and also needs to consider the power constraint that MANET nodes entail.

Two routing categories in wireless ad-hoc network can be distinguished: topology-based and position-based or geographical routing. Topology-based routing protocols use the wireless links' information to achieve data routing, whereas position-based approaches, mainly, focus on the nodes' location information, in order to route the data traffic. Specifically, topology-based routing is discerned into reactive, proactive and hybrid protocols. The difference among these resides in the way the route, from source to destination, is determined. Reactive protocols discover the route to the destination when needed while proactive protocols determine routes in advance and maintain information about all the possible paths in the network. From the network's performance perspective, the impact of such difference can be observed, mainly, in terms of delay and routing overhead. While reactive scheme require the path to be discovered before data packets can be exchanged between the communication's peers, a time delay introduced before the first packet to be transmitted. On the other side, proactive scheme generates high routing overhead by maintaining routing information of unused paths. Finally, hybrid protocols combines both schemes to achieve higher level of routing efficiency and network scalability by adopting proactive routing in local communication (intra-zone) and reactive routing in global communication (inter-zone).

Position-based routing approach uses information about the nodes' position to eliminate some of the limitations of the topology based approach. The main advantage of position-based routing is network scalability. According to experimental work [1] and [2], routing schemes that exchange routing tables without the use of location information are not scalable. Additionally, [1] showed that the routing table size grows logarithmically for a geographical-based routing scheme, whereas it grows linearly for a comparable topology based routing algorithm. Furthermore, the position-based approach requires from the participating nodes to maintain information about their physical position besides the position of some or all the nodes in the network depending on the adopted forwarding strategy. Three main packet

routing strategies can be distinguished: greedy forwarding, directional forwarding and hierarchical routing. According to the first two schemes, the node forwards the packet to one or more neighbours selected based on the criteria of the algorithm. Hierarchical approach forms a hierarchy to increase the network scalability, which corresponds to the hybrid scheme of the topology-based approach while location information is involved.

This chapter gives an introduction to the Wireless Local Area Network (WLAN) and Mobile Ad-hoc Networks (MANET). Sections 2.2 and 2.3 discuss the architecture of 802.11 WLAN and the fundamentals of its Medium Access Control (MAC) and Physical (PHY) layers. A brief overview of MANETs is presented section 2.4, where we highlight the principal and main characteristic of such networks in Section 2.5. Section 2.6 studies the different routing approaches in MANETs, where we deeply discuss the position-based routing protocols, and eventually Section 2.7 summarises the chapter.

2.2 Wireless Networking Overview

In wireless networking, the data information is sent between the connected devices using radio frequency signals. Various types of wireless networks exist and can be grouped in different ways depending on the criteria chosen for the classification. Such criteria include the network architecture (infrastructure or infrastructure-less), network coverage (personal area networks, local area networks or wide area networks) and network applications (home, sensor, vehicular networks etc...).

2.3 Introduction to 802.11 Wireless Local Area Networks (WLANs)

2.3.1 Architecture

The 802.11 [3] network architecture, illustrated in Figure 2-1, consists of different elements that interact to provide a WLAN. These elements are the Basic Service Set (BSS), Distributed System (DS) and Independent Basic Service Set (IBSS).

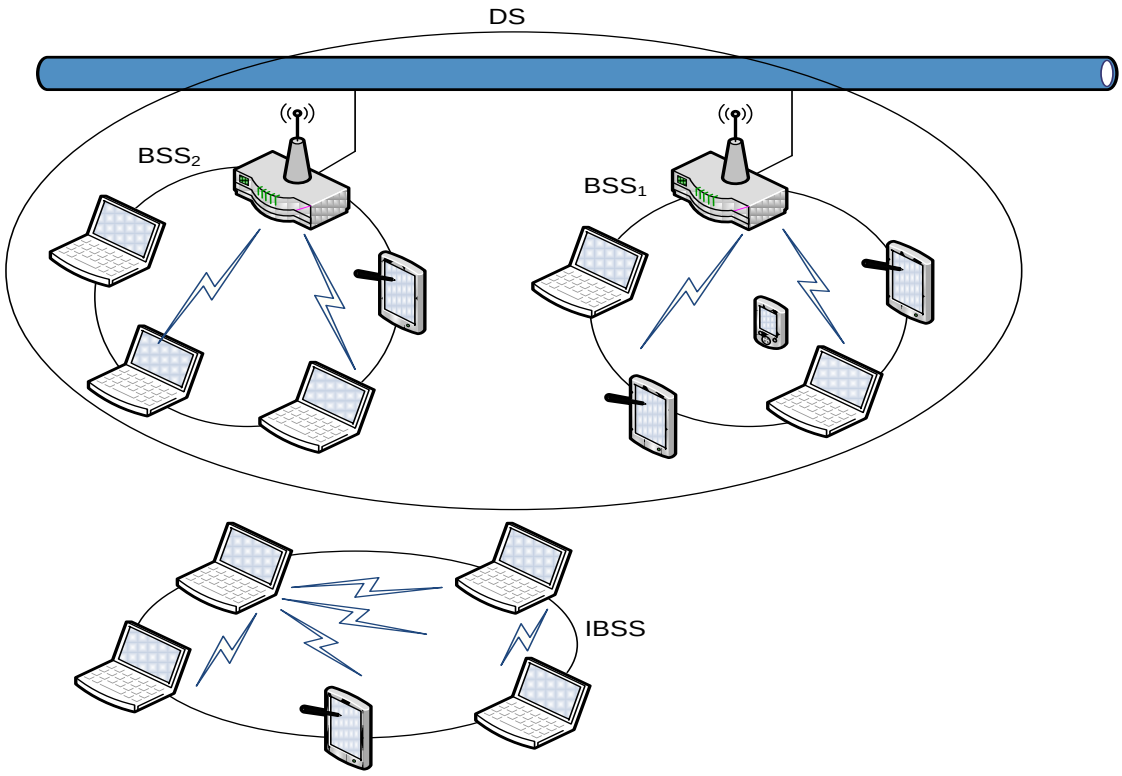

Figure 2- 1: The architecture of 802.11 wireless network

2.3.1.1 Basic Service Set (BSS)

BSS constitutes the basic element of the 802.11 WLAN. It represents a group of wireless stations (STAs) controlled by a Coordination Function (CF). The coordination function is a logical set of rules that manage the stations' access to the wireless medium. The Distributed Coordination Function (DCF) is used by the STA as the basic coordination function, while the Point Coordination Function (PCF) is optional and can be used to support QoS traffic.

2.3.1.2 Independent Basic Service Set (IBSS)

A BSS that operates without a Distributed System (DS) is called an Independent Basic Service Set (IBSS). The WLAN is formed amongst the STAs without a pre-planning phase, for this reason it is called as *Ad-hoc Network*. The mode of operation in the IBSS involves direct communication between the STAs.

2.3.1.3 Distributed System (DS)

DS is the architectural element defined by the 802.11 standard to interconnect multiple BSSs. The DS provides the logical services necessary to handle address to destination mapping and seamless integration of multiple BSSs.

2.3.2 Medium Access Control (MAC)

2.3.2.1 Coordination Function (CF)

The 802.11 standard specifies the coordination function used by MAC to manage access to the wireless medium. The basic coordination function is the Distributed Coordination Function (DCF) that follows the Carrier Sense Multiple Access (CSMA) technique, based on the concept of listen-before-talk. Another optional coordination function, supported by the 802.11 MAC is the Point Coordination Function (PCF) used for traffic with QoS requirements. According to PCF the stations are assigned priorities in accessing the medium coordinated by the Point Coordinator (PC), which usually resides in the Access Point (AP).

2.3.2.2 Carrier Sensing (CS)

DCF uses the Carrier Sense Multiple Access/ Collision Avoidance (CSMA/CA) scheme to share the wireless medium amongst wireless stations. The carrier sense is achieved through two possible ways:

- *Physical-CS:* CSMA/CA implements listen-before-talk scheme, according to which any node willing to transmit data must sense the wireless channel in order to determine whether another station is transmitting. If the channel is detected as being idle the station initiates the transmission, otherwise the transmission is deferred for a random period of time. In addition, CSMA/CA employs an acknowledgment mechanism, in accordance with which the receiving station transmits an acknowledgment (ACK) packet back to the sender, after a short interval of time, to indicate a successful reception. In case the ACK packet is not received, the data packet is considered lost and a retransmission is scheduled.
- *Virtual*-CS: The optional “virtual carrier sensing” mechanism, specified in the IEEE 802.11 standard, is employed by Request-To-Send/Clear-To-Send (RTS/CTS)

handshake. Its purpose is to prevent wireless stations from accessing the wireless channel simultaneously. Therefore, it eliminates the interference caused by the hidden stations and decreases the packet collisions, which improves the network throughput. RTS/CTS packets are exchanged prior to data transmission, if the data frame size is larger than the specified RTS threshold, to reserve the wireless channel for the sending station. The process is initiated by the sending station, which senses the channel and sends RTS packets if it finds the channel idle. The sending station waits for a CTS packet from the receiver before it starts the effective data transmission.

2.3.2.3 Inter-Frame Spaces (IFS)

The time interval between adjacent MAC frames is called "Inter-Frame Space" (IFS). Various IFSs are employed to provide different priorities to the MAC frames. Four IFSs have been specified in the standard and listed below from the shortest to the longest as follows:

1. *Short IFS (SIFS)*

   The SIFS is used before the transmission of the following frames:

   - An acknowledgment (ACK) frame of a data frame.
   - A Clear-To-Send (CTS) frame of a Request-To-Send (RTS) frame.
   - A subsequent MPDU of a fragment of MSDU during fragment burst mode.

   The SIFS is also used before responding to any polling in PCF mode and before any frames from the Access point during the Contention Free Period (CFP).

   For instance, the SIFS for 802.11a [4] MAC is 16 μs and 10 μs for 802.11b/g [5, 6] MAC.

2. *Point Coordination Function IFS (PIFS)*

   PIFS is used to provide the stations, operating under PCF mode (APs), with the highest priority for gaining the medium access.

3. *Distributed Coordination Function IFS (DIFS)*

   DIFS is used by the stations, operating under DCF mode, to transmit data and management frames when the medium is determined as idle.

4. Extended IFS (EIFS)

The EIFS is used by the DCF station whenever the physical (PHY) layer indicates that the frame reception contained an error or the MAC Frame Check Sequence (FCS) value was not correct. Therefore, the receiving stations should wait for a longer period of time before attempting to access the medium. The EIFS is defined to provide the other stations with enough time to complete their ongoing transmission, before the STA that experiences the reception of the erroneous frame commences transmission.

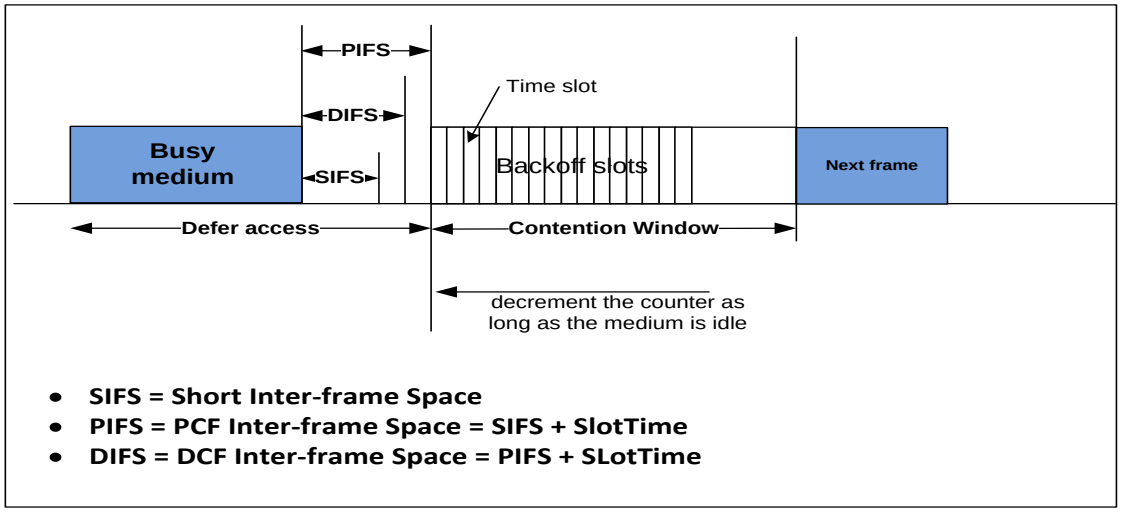

Figure 2- 2: The different inter-frame spaces defined by the IEEE 802.11 MAC

The relationships between the different IFSs, specified in the standard, are defined by the following equations:

$$SIFS = aRxRFDelay + aRxPLCPDelay + aMACProcessingDelay + aRxTxTurnaroundTime \quad (2.1)$$

$$aSlotTime = aCCATime + aRxTxTurnaroundTime + aAirPropagationTime + aMACProcessingDelay \quad (2.2)$$

$$PIFS = SIFS + aSlotTime \quad (2.3)$$

$$DIFS = SIFS + 2 \times aSlotTime \quad (2.4)$$

$$EIFS=SIFS + DIFS + ACKTxTime \quad (2.5)$$

Some of the parameters in the above given equations are PHY layer dependent. The various characteristics of the different PHY layer specifications require the inter-frame spaces to be dependent on the transmission scheme in use.

- *aSlotTime*: is a time unit in microseconds used by the MAC to define the PIFS and DIFS period. The value of aSlotTime is dependent on the PHY characteristics. E.g. the aSlotTime is 9µs for 802.11a.
- *aRxRFDelay*: is the nominal time in microseconds between the end of a symbol in the air interface and the moment the PMD indicates the arrival of data to the PLCP.
- *aRxPLCPDelay:* is the nominal time in microseconds used by the PLCP to deliver the last bit of a received frame from the PMD to the MAC.
- *aMACProcessingDelay:* is the maximum time in microseconds available to the MAC to change the PHY mode either for transmission or for CCA.
- *aRxTxTurnaroundTime:* is the maximum time in microseconds that the PHY requires to change its reception state to transmission state.
- *aCCATime:* is the minimum time in microseconds available for the CCA to sense the medium and determine whether it is busy or idle.
- *aAirPropagationTime:* is twice the time required by a signal to cross the distance between the most distant allowable STAs.
- *ACKTxTime:* is the time in microseconds required to transmit an ACK frame at the lowest PHY mandatory rate.

2.3.2.4 Random backoff time

The CS mechanism is invoked prior to any frame transmission to determine whether the medium is busy or idle. If the medium is found busy, the STA defers its transmission for a time equal to DIFS if the last frame was correctly received or for a time equal to EIFS in the opposite case. When the CS reports the medium state to be idle after DIFS or EIFS, the STA must generate a random backoff period before attempting to access the medium. The random backoff period is used in order to minimise the chance of collision and is calculated as follows:

$$BackoffTime = Random() \times aSlotTime \quad (2.6)$$

Where Random() is a function used to generate a pseudo-random integer from a uniform distribution over the interval [0,CW]. The value of the Contention Window (CW) parameter varies between CW_{min} and CW_{max}. The initial value of CW is CW_{min} and is incremented to the

next higher value after an unsuccessful transmission of an MPDU. When the CW reaches the value of CW_{max}, it remains at that value until the CW is reset.

2.3.2.5 DCF access procedure

The foundation of the DCF procedure is the CSMA/CA access method, which is implemented in all STAs to be used in IBSS and infrastructure network configurations. When a STA has a frame to transmit, the CS mechanism is invoked to determine that the medium is idle for a period greater than DIFS or EIFS, before proceeding with the transmission. The STA will then generate a backoff counter for additional deferral time, unless the counter has a zero value, in which case the STA is allowed to access to the medium immediately. If the medium state changes to *busy* while performing the backoff, the STA freezes the backoff procedure and waits for the medium to become *idle* again.

The basic operation of DCF procedure is illustrated in Figure 2-3.

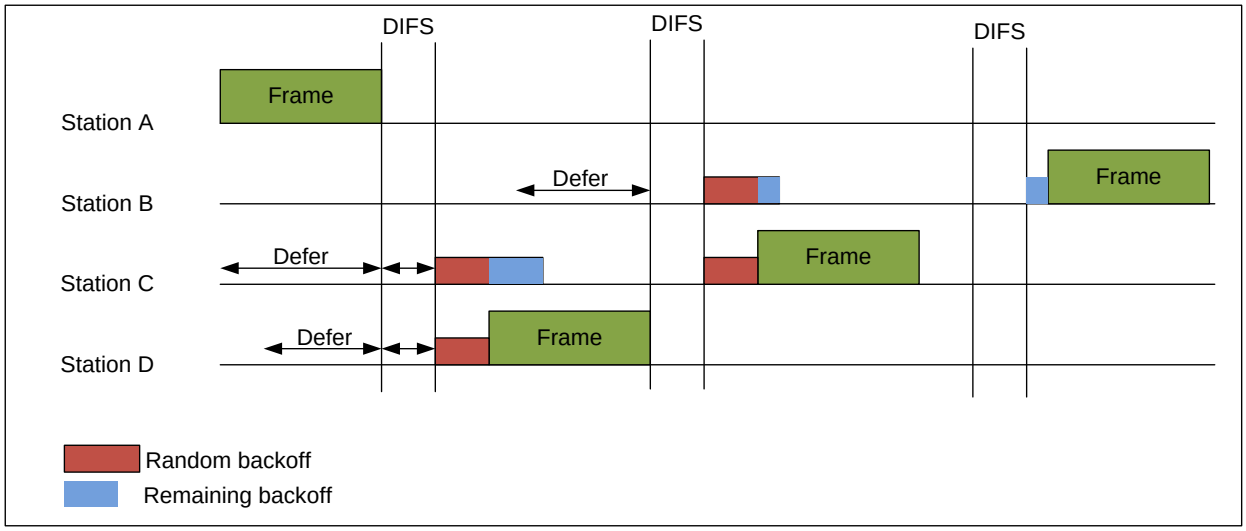

Figure 2- 3: An example of the DCF operation

2.3.2.6 PCF access procedure

The optional PCF access method is used in infrastructure network configurations. PCF requires the use of Point Coordination (PC), which typically operates at the AP of the BSS in order to control the STAs' priority access to the wireless medium. According to PCF, the time is divided into repeated period, called superframe. The start of the superframe is indicated by the beacon, which is a management frame generated by the PC in order to synchronise the timers

of the stations and delivers a set of parameters. Furthermore, a superframe includes a Contention Free Period (CFP), which uses PCF access method, followed by a Contention Period (CP), which involves DCF access method. The Network Allocation Vector (NAV) is employed in order to protect the PCF access from the DCF access. In addition, PC maintains a polling list that includes the selected STAs that are eligible for receiving the CF-polls during CFP. A STA indicates whether or not to be placed on the polling list during the association process. After transmitting a beacon frame and indicating the start of the superframe, the PC waits for SIFS and sends a data frame, a *data+CF-poll* frame, a management frame or a CF-end frame. Finally the duration of the CFP is represented by *CFPMaxDuration parameter*. Given that no traffic exists and the polling list does not include any entry, the CFP can be terminated by the PC before *CFPMaxDuration*.

Figure 2-4 depicts the operation of the PCF access method.

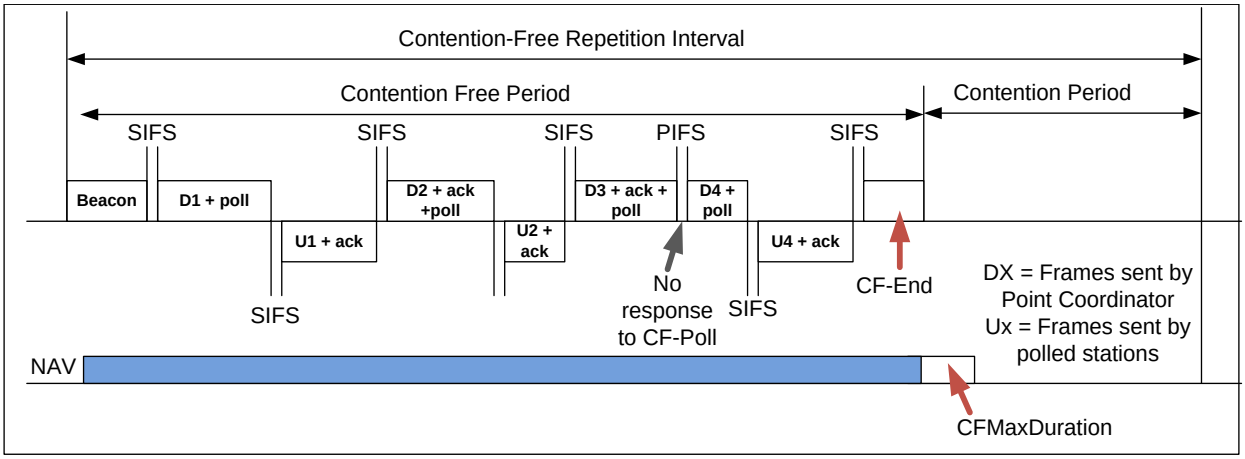

Figure 2- 4: An example of DCF operation

2.3.3 PHY Layer

Different PHYs are defined in the IEEE 802.11 standard. Each PHY consists of two protocol functions:

1. A PHY Media Dependent (PMD) system that defines the characteristics and method of transmitting and receiving data frame through the wireless medium amongst STAs.

2. A PHY layer convergence protocol (PLCP), which defines a method of mapping the IEEE 802.11 MPDUs into a framing format suitable for sending and receiving user data and management information between the STAs using the associated PMD system.

A reference model of 802.11 architecture showing the interaction between the PHY, MAC and higher layers is illustrated in Figure 2-5.

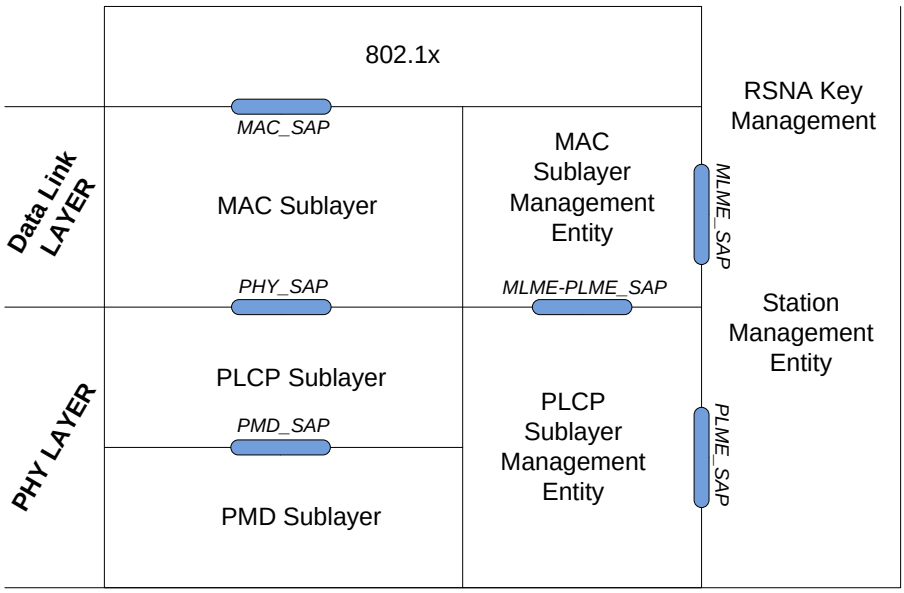

Figure 2- 5: The protocol reference model for the IEEE 802.11 architecture showing the interaction of the PHY sub-layers with the MAC and the higher layers

In order to transmit frames, PLCP forms what has been transferred from the MAC layer into PLCP protocol data unit (PPDUs) from. The PPDU format consists of three parts: a PLCP preamble, a PLCP header, and a PSDU. The PLCP preamble field allows the synchronisation and defines the frame start. The PLCP header is used to specify the length of the whitened PSDU field and provide PLCP management information. The PLCP preamble and PLCP header are transmitted at 1 Mbps, while the PSDU can be transmitted at any supported transmission rate. The fields of the PLCP frame are depicted in Figure 2-6.

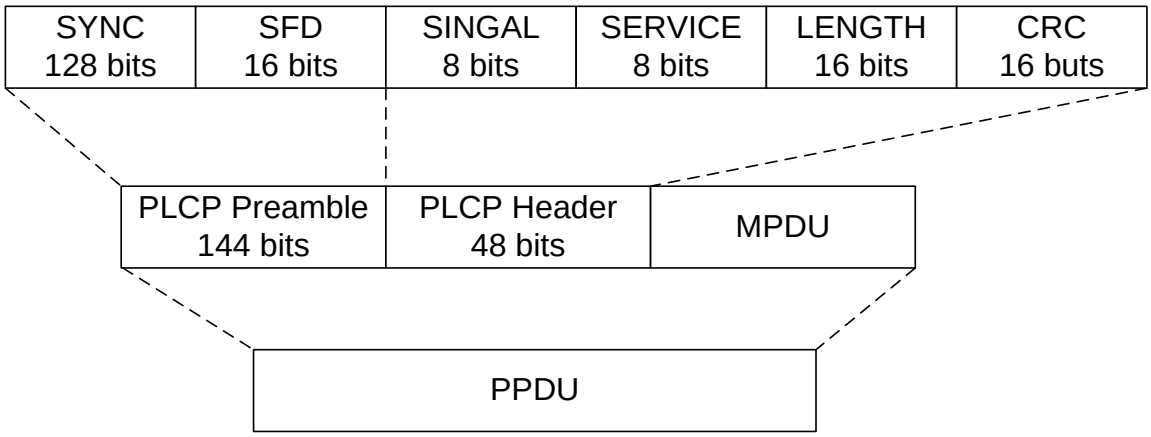

Figure 2- 6: The PPDU packet format

Three different types of PYHs are defined in the original 802.11 standard including Frequency Hopping Spread Spectrum (FHSS), Direct Sequence Spread Spectrum (DSSS) and Infrared (IR).

The static characteristics of FHSS-PHY, DSSS-PHY and IR-PHY are given in table 2-1.

Table 2- 1: The timing characteristics of FHSS, DSSS and IR PHYs

Characteristic	FHSS-PHY	DSSS-PHY	IR-PHY
aSlotTime	50 µs	20 µs	8 µs
aSIFSTime	28 µs	10 µs	10 µs
aCCATime	27 µs	≤ 15 µs	5 µs
aRxTxTurnaroundTime	20 µs	≤ 5 µs	0 µs
aRxPLCPDelay	2 µs	Any[1]	Any[1]
aRxRFDelay	4 µs	Any[2]	1 µs
aAirPropagationTime	1 µs	1 µs	1 µs
aMACProcessingDelay	2 µs	≤ 2 µs	2 µs

In addition, various extensions of the previously mentioned PHYs have been identified, in order to increase the supported data transmission rate. The high rate DSSS (HR/DSSS) is an extension of the DSSS system, which is designed to support higher payload transmission data rates at 5.5 and 11 Mbps. The Extended rate PHY (ERP), which makes use of the Orthogonal Frequency Division Multiplexing (OFDM) PHY, is developed to provide a data transmission rate of up to 54

[1] Any value may be chosen as long as the requirements of *aSIFSTime* and *aCCATime* are met.

[2] Any value may be chosen as long as the requirements of *aRxTxTurnaroundTime* are met.

Mbps. Table 2-2 illustrates the various PHYs and their supported data rates, taking into consideration the 2.4 GHz ISM band.

Table 2- 2: the supported data rates of the various 802.11 PHYs

PHY	Supported Data rate (Mbps)
FHSS	1,2
DSSS	1,2
IR	1,2
HR/DSSS	1,2,5.5,11
ERP	1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48 and 54

Various 802.11 sub-standards have been defined based on the different PHYs specifications and the frequency band used. The 802.11a operates in the 5GHz frequency band and uses the OFDM PHY to support a data rate of up to 54 Mbps. The 802.11b and 802.11g operate in the same 2.4GHz frequency band, however, the 802.11g PHY is based on OFDM to provide high data rate of up to 54 Mbps. Table 2-3 depicts the values for the MAC parameters of the various IEEE 802.11 standards.

Table 2- 3: some MAC parameters in Microseconds for Different PHYs

802.11x	*SIFS*	*DIFS*	*Slot Time*	*CWmin*
802.11a	16	34	9	15
802.11b	10	50	20	31
802.11g	10	50	20	15

Figure 2-7 depicts the wireless channels of the 2.4GHz frequency band allocated to the 802.11 standard showing the three non-overlapping channels.

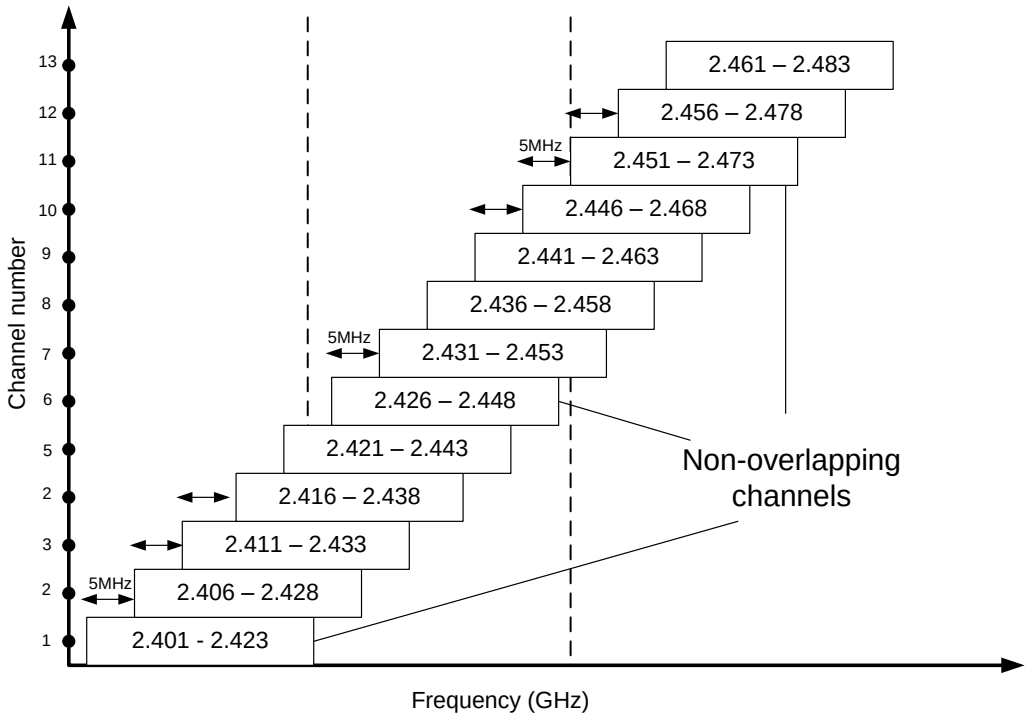

Figure 2- 7: The wireless channels of the 2.4 GHz frequency band

2.4 Mobile Ad-Hoc Networks (MANETs)

Mobile Ad-hoc Networks (MANETs) are a collection of mobile devices (nodes) moving within a geographical area to form a self-healing, self-configuring wireless network. Such type of a wireless network lacks the existence of any sort of infrastructure or centralised entity. Figure 2-8 illustrates an instance of MANET, where a connection to external networks (local area network, internet, etc) can be acquired through one or several devices.

MANET configuration is suitable for networks that require rapid deployment such as meeting rooms, sport stadiums, search and rescue and disaster recovery. It can be applied where the deployment of a wired network is impossible such as in battlefield and maritime scenarios.

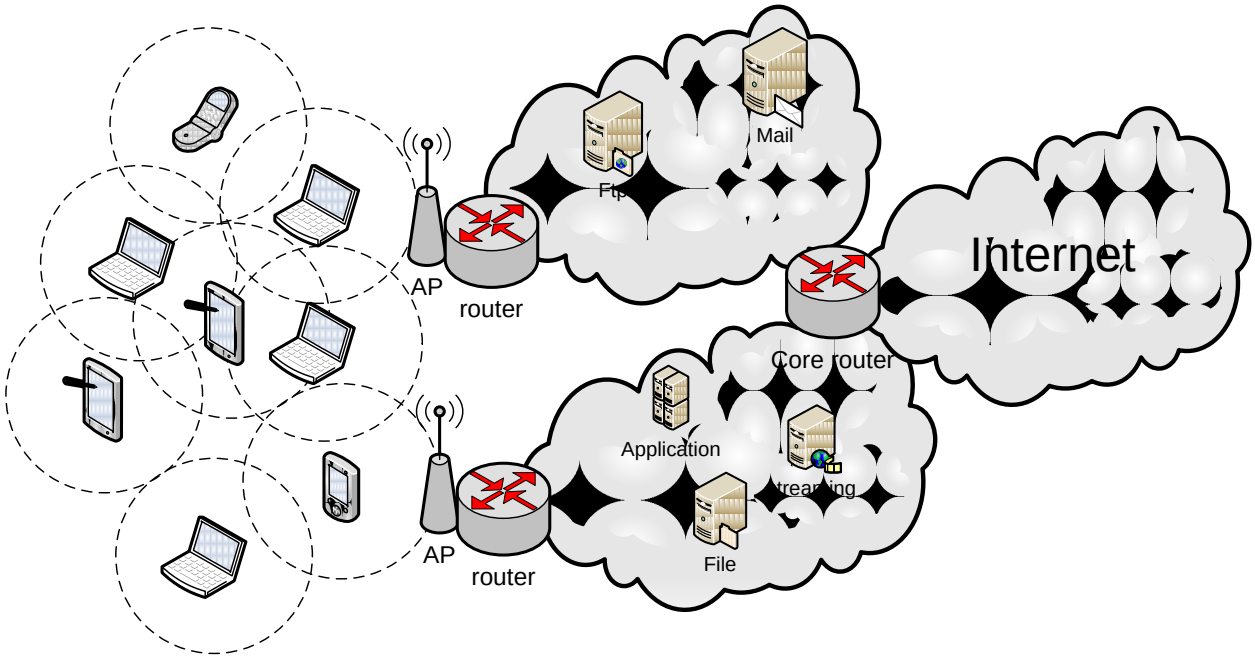

Figure 2- 8: An instance of a MANET connected to external networks

A MANET node is able to communicate with all the other nodes within its transmission range via a direct connection. In case the desired destination node is beyond the transmission range of the source, a multi-hop connection, composed of a set of intermediate nodes, is established to maintain the source-destination communication.

In addition to the multi-hop communication capability, the mobility support is another principal feature that MANET provides, allowing the wireless nodes to freely move within the defined area. However, the link breakage that is caused by the movement of the mobile nodes changes the network topology very frequently, imposing, therefore, serious challenges on the protocol design, in general, and on the routing algorithms, in particular.

2.5 Characteristics and advantages

Mobile Ad-hoc Network (MANET) shares common characteristics with wireless networks and preserves for itself some others that distinguish it as a special

- *Wireless medium*: The MANET nodes communicate with each other wirelessly by sharing the same medium.

- *Multi-hop communications*: The multi-hop feature of MANET allows the MANET node to communicate with any destination in the network, regardless whether the destination is within its radio range or not. Therefore, each node acts as a router to enable information routing between the source and destination.
- *Autonomous and infrastructure-less:* MANET does not rely on any sort of infrastructure. Hence, the network administration and control are performed in a distributed manner, where each node acts as an independent router.
- *Mobility and dynamic topology:* The mobility support in MANET permits the node to move around without interrupting the active communications. The mobility causes link breakage and topology variation, which in turns changes the connection patterns between the mobile nodes.

The above mentioned characteristics give MANETs important advantages over the other types of wireless networks in terms of moving while communicating, multi-hop communication ...etc. On the other hand, several challenges in the protocol design may rise, especially in developing routing protocols that has to cope with the nodes' mobility and the dynamic topology of the network.

2.6 Routing in MANETs

Various criteria can be considered to classify MANET routing protocols. Such criteria include the way that the routes to the destination nodes are established (reactive or proactive), the topology structure (flat or hierarchical), the routing method (hop by hop or source routing) and the type of information that the protocol relies on to perform the routing process (link or position). Based on the latter, routing in MANETs is classified into topology-based and position-based.

2.6.1 Topology-based Routing

Topology-based routing approach performs routing based on links' information. The protocols of this category maintain a routing table, where they store topological information that will be used in the routing process. Three sub-classes may be distinguished: reactive on demand,

proactive or table driven and hybrid routing protocols. The difference amongst them lies on when the information about the routes is obtained. While proactive protocols periodically exchange topological changes to maintain routes to all the possible destinations, reactive protocols discover routes when needed and maintain the routes that are in active communication. From a routing performance's perspective, reactive protocols reduce the injected routing overhead by discovering routes when needed. However, data transmission is deferred for an additional period of time delay, waiting on the completion of the route discovery process. Hybrid protocols aim to combine the advantages of both previously mentioned schemes. Accordingly, the network area is divided into zones. The communication within the zone (intra-zone) is performed in a proactive manner, while routing between the zones (inter-zone) is performed reactively.

2.6.1.1 Ad-Hoc On Demand Distance Vector (AODV)

AODV [7] is a reactive hop-by-hop routing protocol that discovers routes to the destination when needed. It does not require the maintenance of routes to destinations that are not in active communication. When an AODV source node has data to send, it initiates the route discovery process if no valid entry is found in the routing table. The discovery process is started by broadcasting a Route Request (RREQ) message to propagate in the entire network until it reaches either the destination node or an intermediate node with a valid route to the destination. Upon receiving a RREQ message, an intermediate node creates or updates a route to the previous sender of the RREQ. The received RREQ is discarded if the node has received a RREQ with the same originator and RREQ ID within, at least, the last PATH_DISCOVERY_TIME. The node then checks whether a valid entry for the destination exists in its table. If this is the case, a Route Reply (RREP) message is unicasted back to the originator of the RREQ by using the already created reverse path. The same procedure is followed if the RREQ reaches the destination node. In case no valid entry is found in the table, the RREQ message is rebroadcasted after incrementing the hop count value by one. Moreover, AODV uses a sequence number field in its control messages to determine the freshness of the information acquired from the originating node. When the source node receives multiple RREP, the route with the lowest hop count value is selected.

The dissemination of the RREQ is controlled by an expanding ring search technique. The originator of the RREQ sets the Time-To-Live (TTL) of the IP header to TTL_START and waits for a RING_TRAVERSAL_TIME before attempting to broadcast the RREQ with an incremented TTL. This continues until the TTL of the RREQ reaches TTL_THRESHOLD, after which a TTL = NET_DIAMETER is used for each subsequent attempt. In addition, the nodes of an active route monitor the link status of the next hops. If a link breakage is detected, a Route Error (RERR) message is flagged to notify the other nodes and to indicate the destinations that are no longer reachable through the broken link. Finally, as a part of an active route, the mobile node periodically broadcasts HELLO messages. The broadcasting of HELLO messages is restricted to the one hop neighbourhood.

2.6.1.2 Distance Source Routing (DSR)

DSR [8] is a reactive source routing protocol. The entire route to the destination is discovered and consequently made known to the source node prior to data transmission. Similar to AODV, the discovery process is initiated when a source node attempts to transmit data to a destination node with an unknown route. The source node broadcasts a RREQ message throughout the network until the requested destination node or an intermediate node with a valid route to the destination is reached. The DSR RREQ packet is different than AODV's as the former contains the entire discovered route. Upon receiving a RREQ, the node checks its cache for a valid route to the requested destination. If no route is found in the cache, the node adds its address to the RREQ and rebroadcasts it further. If, however, the node has a valid route to the RREQ destination, the complete route (the route included in the RREQ + the cached route) is copied to a RREP message and is sent back to the source node. Finally, when the destination node is reached, it simply sends a RREP to the originator of the RREQ by reversing the route recorded in the RREQ.

DSR introduces the concept of *route salvaging,* according to which an intermediate node uses an alternative route from its cache to the packet's destination, when the next hop link along the packet's route is detected as broken. Therefore, the node *salvages* the packet rather than discarding it by replacing the original source route of the packet with the route of its cache.

In addition, DSR uses *route shortening* mechanism, which is applied when one or more intermediate nodes become unnecessary to the route.

2.6.1.3 Optimised Link State Routing (OLSR)

OLSR [9] is a table-driven proactive routing protocol. The shortest routes to all possible destinations in the network are discovered in advance, by regularly exchanging topology information among the mobile nodes. OLSR significantly minimizes the routing overhead by handing the dissemination process of the control traffic over to the Multi-Point Relays (MPRs) that continuously maintain the routes to the destinations. Each node in the network selects its MPRs in its symmetric 1-hop neighbourhood to forward its messages. The selection is performed in a way that the selected MPRs cover all symmetric 2-hop nodes. Therefore, any two hop neighbour of a node 'N' must have a link to one of 'N''s MPRs. Each MPR maintains information about the set of neighbours that have selected, called MPR-selector set, through the received HELLO messages.

Any changes in the network topology will be advertised in the entire network by the selected MPRs. Each node selected as MPR must at least disseminate the links between itself and the nodes in its MPR-selector set, in order to build a link information base. Each node maintains a routing table that contains routing entries to each destination in the network based on the link information base. Therefore, any changes occurring in the topology result in re-calculation of the routing table.

A routing entry consists of four fields: <R_*dest_addr, R_next_addr, R_dist, R_iface_addr*>, meaning that the destination node *R_dest_addr* is *R_dist hops* away from the current node and the next hop node in the route is *R_next_addr*, reacheable through the interface *R_iface_addr*.

2.6.2 Position-based Routing

2.6.2.1 Existing Position-based Routing Protocols

Several working efforts aim to enhance the routing performance in MANETs by introducing location information into the algorithm have been proposed. A survey of position-

based routing algorithms is extensively discussed in [10] and [11]. Below, we highlight several location-based routing protocols, which are related to our work.

A. Greedy forwarding schemes:

Algorithms that use greedy forwarding strategy, which selects the neighbour that satisfies specific criterion as the next hop relaying node, are proposed in [12], [13], [14], [15] [16], [17], [19] and [20]. Random progress method is proposed in [12] according to which packets destined toward a destination node D are routed with equal probability towards one neighbouring node that makes progress in the direction of D. The source node will select among the (n) neighbours one terminal located in the direction of the destination D as all neighbours having the same probability (1/n). Progress is defined as the distance separating the transmitter and the receiver projected onto the line joining the transmitter and the final destination. In [13] a variant of random progress method called Cartesian Routing is proposed. Progress in Cartesian Routing is defined as the distance between the transmitter (X_t,Y_t) and the final destination (X_d,Y_d). According to this, packets are forwarded to any direct neighbour (X_i,Y_i) for which the distance $[(X_i,Y_i)$ to $(X_d,Y_d)]$ is less than the distance $[(X_t,Y_t)$ to $(X_d,Y_d)]$. In case of no direct neighbour closer to the destination is found, conditioned the network is n-Cartesian regular, a search of no farther than (n-1) hops will lead to a node that makes progress. According to [13], a network is called n-Cartesian regular if for any transmitter node T and any destination node D, some other node Ni exists within n-hopes of T and closer to D. Takagi and Kleinrock [14] proposed the Most Forward within Radius (MFR) routing algorithm. MFR forwards the packet to the next neighbour that maximizes the progress. The progress is defined as the distance between the transmitted node and the neighbouring node projected onto the line joining the transmitter node and the final destination. In MFR strategy, a case might arise where the selected neighbour having the maximum progress is farther from the destination. Nearest with Forward Progress (NFP) routing algorithm is introduced in [15] where the nearest neighbour with forward progress is selected as the next hop node. Furthermore, greedy forwarding schemes are characterized by routing data packet relying on positions of one-hop neighbours only. However, there are topologies in which some of these schemes fail to deliver the packet to the destination even though a route exists, e.g. a topology where the node itself

is closer to the destination than any of its neighbours. This case is referred to as local maxima. Greedy Perimeter Stateless Routing (GPSR) algorithm proposed in [16] maintains information about its direct neighbours' positions to make a routing decision. It consists of two methods of packet forwarding: greedy forwarding and perimeter forwarding. GPSR header includes a field indicating whether the packet is in greedy mode or perimeter mode. Upon receiving a packet for forwarding, a node applies greedy scheme and searches for the neighbour which is geographically closest to the destination. When no neighbour is closer to the destination than the node itself, the packet is marked into perimeter and will be forwarded using simple planar graph traversal.

Stojmenovic and Lin proposed in [17] two hop flooding GEDIR, two hop flooding MFR and two hop flooding DIR, modifications of GEDIR [18], MFR and compass routing schemes to avoid packet dropping. The proposed algorithms are referred to as 2-f- GEDIR, 2-f- MFR and 2-f-DIR respectively. The main idea behind these variants is that the transmitter nodes choose the closest terminal to the destination among the first and second hop neighbours except concave node that floods the packet to all its neighbours. A node is called concave if it is the only neighbour of the selected node for forwarding, closer to the destination. Greedy Routing with Anti-Void Traversal (GAR) is introduced [19] to solve the void problem of greedy forwarding scheme by exploiting the boundary finding technique fort the unit disk graph (UDG). Rolling-ball UDG boundary traversal (RUT) technique is further proposed in [19] to solve the boundary finding problem.

Liu and Feng developed the Largest Forwarding Region (LFR) [20] routing protocol, which selects the neighbour that possesses the largest Extended Forwarding Region (EFR). EFR is associated with every neighbour contains both the distance and the direction information related to the destination. Note that the forwarding region is defined as the area including the closest nodes to the destination. Furthermore, Backward Constraint (BC) and Dead End Recovery (DER) mechanisms are defined to resolve backward loops and dead ends problems in the network. Although LFR resolves the problem of void in the network by transmitting the

packet back to the concave node, it would be more efficient not to consider at all the nodes that lead to void which will be shown in this paper.

B. Directional routing schemes:

Directional routing methods that rely on the direction of the destination to select the next forwarding node algorithms are discussed in [21], [22], [23], [24] and [25]. In Compass Routing presented in [21], the transmitter node T (source or intermediate node) forwards the packet to its closest neighbour N to the destination D that minimizes the angle (TND). The same procedure is applied at every intermediate node until the packet reaches the destination. Ko and Vaidya in [22] demonstrate with their Location Aided Routing (LAR) protocol how the utilization of location information can improve the flood mechanism of route discovery messages and hence reduce the routing overhead. In LAR, the source node defines the expected zone where the destination is expected to be, based on the location information of the destination and the speed that the destination can reach. The source node only broadcasts the discovery request within the request zone which is the smallest rectangle formed by the expected zone and the source node's position. Two algorithms of LAR also presented in [22]; LAR scheme-1 and LAR scheme-2 which differ in the manner that the request zone is specified in the request message. In the scheme-1, the zone is specified explicitly by the source node while in scheme-2 it is implicitly specified, where the source includes in the request message additional information about the destination coordinates and its distance to the destination. Although LAR reduces routing overhead as it reactively discovers a route to the destination, it still requires maintaining an explicit path between every source and destination prior to data transmission. In [23], a challenge of Location Aided-Routing algorithm is discussed and an improved version of the protocol is presented. Although during the route discovery phase, the destination node receives the request from different routes, it only responds to the earliest request received. Therefore any later route breakage will lead to a new route discovery process. The author proposed to select a back up route to be used as a secondary route in case of any failure in the primary route. Location Aided Knowledge Extraction Routing (LAKER) [24] utilizes a combination of caching strategy in Dynamic Source Routing [8] and limited flooding in Location-Aided Routing [22]. The idea of LAKER is to learn the topological characteristics of the

network and use this information to guide the route discovery more precisely in the request zone. Simulation results show that LAKER saves up to 30% broadcast messages as compared to LAR. A variant of LAR protocol is Multipath Location Aided Routing in 2D and 3D, referred to as MLAR [25] which is designed to work efficiently in 3 dimensions by using alternate path caching strategy. MLAR caches several paths although one path is used at a time and the others are alternate routes to be used when the primary path fails.

A close work to FORTEL is Distance Routing Effect Algorithm for Mobility (DREAM) proposed by Basagni et al. [26]. DREAM represents an all-to-all location service that disseminates and updates nodes' location throughout the entire network. The frequency of updates is determined based on the distance between the nodes and the mobility rate. Data packets are transmitted to all the one-hop neighbours that lay in the direction to the destination represented by the angular range that includes the node's position, the destination's position and the zone that the destination is expected to be. The same procedure is applied at every node until the destination had been reached. Although, transmitting data packets through multiple paths may increase the probability of reaching the destination, the protocol lacks scalability due to the communication overhead and data message redundancy.

C. Hierarchical routing schemes:

Hierarchical approach is discussed in [27] and [28]. GRID protocol discussed in [27] exploits location information in route discovery, packer forwarding and route maintenance. It considers the MANET as 2D logical grids controlled by grid gateways. Packet routing is performed gird-by-grid manner and the gateway hosts are responsible of discovering, maintaining the routes and forwarding data packets to the neighbouring grids. Blazevic et al. proposed in [28] the Terminode routing that combines location-based routing and link state routing. Location routing referred as Terminode Remote Routing (TRR) is used when the destination node is far, while link state routing referred to as Terminode Local Routing (TRL) is used when the destination is up to two hops away. Moreover, the concept of anchors, which represent imaginary geographical locations installed in the packet header to assist in the routing process, is introduced. In Position and Neighbourhood based Routing (PNR) [29], the

networks is represented by a set of quadrants. The quadrants are organised in a hierarchical meaner, where each higher level quadrant is divided into four lower level quadrants. PNR requires each node to initiate an initial flooding as a start up phase. Any node moves more than a pre-defined distance must send an update packet. The dissemination of the update packets is optimised using the concept of quadrant. Accordingly, when receiving an update packet, the node maintains the exact location of the packet originator if they are in the same quadrant or it stores the quadrant that the originator belongs otherwise. The routing is based on the shortest path using the concept of greedy forwarding.

D. Other schemes

GPS/Ant-Like Routing Algorithm (GPSAL) routing protocol is described in [30]. The key point of GPSAL is the mobile software agents modeled on ants used to disseminate and collect nodes' location information more rapidly. An ant holds a routing table and is transmitted to a specific destination. Upon receiving an ant packet, older entries are updated by the current host and the ant is passed to another node carrying the most updated routing table. The same procedure is followed until the ant has reached its destination at which point is sent back to the node that created it. Zeng et al. introduced in [31] Geographic On Demand Disjoint Multipath routing protocol to be used instead of blind flooding of route discovery in the network. Every node knows the position of its one-hop neighbours. Before transmitting route request (RREQ) message, the source node selects the k nearest neighbours to the destination and includes their addresses in the packet. Upon receiving RREQ, only intermediate nodes having their addresses stated in the packet forward the request after selecting a new list of nearest neighbours to the destination. This is repeated until the destination has been reached which in turn transmits a route reply (RREP) message back to the source. In addition, the authors described two schemes: Geographic Node-disjoint–paths routing and Geographic Edge-disjoint-paths routing. The difference between these schemes lies in the processing of the duplicate RREQ messages. While the first scheme drops all the duplicate RREQ, edge-disjoint routing may forward duplicate RREQ having been received from a different neighbour.

Recent work is presented in [32], [33] and [34], where different geographic routing algorithms are developed. Predictive Mobility and Location Aware Routing (PMLAR) [32] predicts the movement behaviour of the mobile nodes to assist the routing operation. PMLAR is designed in a way that the source node predicts the current and the future location of the destination to increase the routing efficiency. The prediction is based on a precious location update of the destination acquired through a location service. To transmit data packets, the source node determines the predicted zone, which is expected to include the potential future position of the destination. The route discovery process is then initiated to establish a valid route to the destination. During the discovery phase, the intermediate nodes apply the Velocity-Aided Routing (VAR) mechanism to ensure that the RREQ is forwarded by the nodes that are moving toward the destination along their connecting lines. In [33], Location-Aware Routing for Delay tolerant networks (LAROD) is proposed, which is a beacon-less routing protocol designed for intermittently connected MANETs that combines the store-carry-forward technique with the geographical position. LAROD consists of an enhanced location service and a location dissemination service to update the nodes location information. Finally, Prediction-Based Routing (PBR) protocol for vehicular ad hoc networks is proposed in [34]. PBR takes the advantage of the predictable mobility pattern of vehicles on highways to predict the route lifetimes and pre-emptively create new routes before existing ones fail.

2.6.2.2 Distance Routing Effect Algorithm for Mobility (DREAM)

DREAM [26] is a hop-by-hop position-based routing protocol, specifically designed for mobility that proactively disseminates the location information across the network. Each mobile node maintains a Location Table (LT), which contains the location information of all the other nodes. Therefore, when a source node wants to transmit data to a specific destination, it refers to the LT to select all its one-hop neighbours in the direction of the destination that will be the next hop forwarding nodes. The same process is applied at every intermediate node until the destination is reached. The direction of the destination, as shown in Figure 2-9, is defined as the sector formed by the source node and the zone in which the destination node is expected to be located.

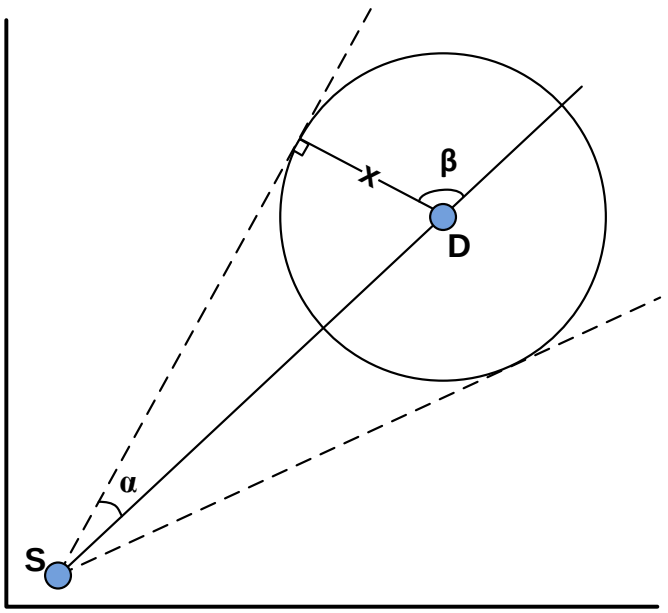

Figure 2- 9: The direction of a destination node D, where x is the maximum distance that D can travel during t_1-t_0. t_0 is the time at which the information of D was received and the t_1 is the time to send data to D

Each node, periodically, broadcasts a control packet containing its own coordinates. To control the routing overhead injected in the network, DREAM uses the distance effect, according to which the further apart the two nodes are, the slower they appear to be moving in respects to each other and subsequently their *LT*s need updating less often. Therefore, an age parameter is associated with every control message to limit the distance that the message travels from the sender. Besides, DREAM introduces a mobility rate factor to determine the frequency at which the control packets are transmitted. Accordingly, the faster the node moves, the more often it must communicate its location.

Furthermore, DREAM supports two types of control messages: *short lived* and *long lived*. Every node broadcasts, periodically, a short lived control message that is meant to be delivered to all the nodes whose Euclidean distance to the originator is less than a predefined distance (*K* grid units). Following the transmission of a specific number (ρ) of short lived messages, one long lived control message is disseminated throughout the network. To further control the frequency of transmitting the control messages, DREAM uses a mobility rate, which allows the node to self optimise its dissemination frequency. Accordingly, the faster a node moves, the more often its updates its location information.

2.6.2.3 Location-Aided Routing (LAR)

LAR [21] protocol is a position-based routing protocol that discovers routes to destinations reactively. It uses location information to reduce the routing overhead caused by the route discovery process. Its main concept is to confine the propagation area of the route request (RREQ) messages to the geographical zone that leads to the destination node. For this reason, LAR defines two zones: expected zone and request zone. The expected zone, illustrated in Figure 2-10, is the circle where the destination node is expected to be located.

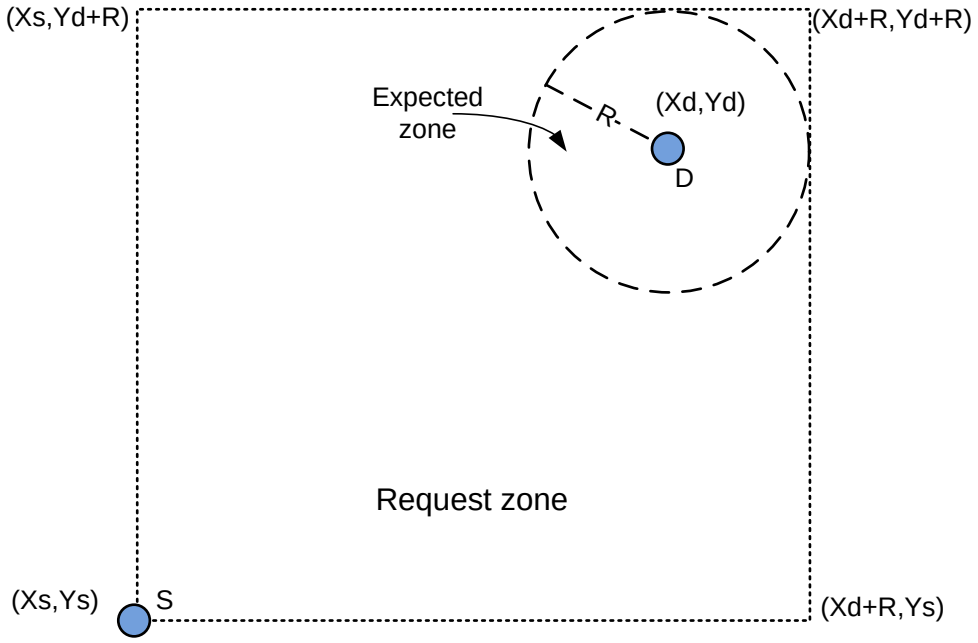

Figure 2- 10: LAR request and expected zones

The source node, only, broadcasts the discovery request within the request zone, which is the smallest rectangle formed by the expected zone and the source node's position. Furthermore, LAR defines two schemes: scheme-1 and scheme-2. The difference resides in the way the request zone is specified within the request message. In the scheme-1, the source node explicitly specifies the request zone by including the coordinates of the zone's four corners in the RREQ. The receivers located outside the specified rectangle discards the RREQ. On the other hand, in scheme-2, the source node includes in the RREQ the destination's coordinates as well as its distance, $Dist_s$, to the destination. The receiving nodes will then calculate their

distance to the destination node, and only the nodes whose distance is greater than $Dist_s$ will forward the RREQ.

2.7 Conclusion

This chapter gives an overview on the IEEE 802.11 Mobile Ad-Hoc Networks. The main objectives are to outline the fundamentals of the WLAN technology by highlighting the basic operations of its MAC and PHY layers, and to explain the principles and the characteristics of MANETs. A detailed study on the routing approaches in MANET is then presented, especially the position-based type of them, which forms the basis of the related discussion in chapter 3.

References

[1] R. Jain, A. Puri and R. Sengupta. “Geographical routing using partial information for wireless ad hocnetworks”. IEEE Personal Communications, 8(1), pp. 48-57, Feb 2001.

[2] J. Li, J. Jannotti, D. De Couto, D. Karger, and R. Morris, “A scalable location service for geographic ad-hoc routing,” in Proceedings of the 6th ACM International Conference on Mobile Computing and Networking (MobiCom ’00, pp. 120–130), August 2000.

[3] "IEEE Std 802.11-1997 Information Technology- telecommunications And Information exchange Between Systems-Local And Metropolitan Area Networks-specific Requirements-part 11: Wireless LAN Medium Access Control (MAC) And Physical Layer (PHY) Specifications," IEEE Std 802.11-1997 , vol., no., pp.i-445, 18 Nov 1997.

[4] "Supplement to IEEE standard for information technology telecommunications and information exchange between systems - local and metropolitan area networks - specific requirements. Part 11: wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: high-speed physical layer in the 5 GHz band," IEEE Std 802.11a-1999 , 1999.

[5] "Supplement To IEEE Standard For Information Technology- Telecommunications And Information Exchange Between Systems- Local And Metropolitan Area Networks- Specific Requirements- Part 11: Wireless LAN Medium Access Control (MAC) And Physical Layer (PHY) Specifications: Higher-speed Physical Layer Extension In The 2.4 GHz Band," IEEE Std 802.11b, 2000.

[6] "IEEE Standard for Information technology-Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," IEEE Std 802.11-2007 (Revision of IEEE Std 802.11-1999) , 2007.

[7] C. E. Perkins, E. Belding-Royer, S.R. Das. Ad hoc on-demand distance vector (AODV) routing. http://www.ietf.org/rfc/rfc3561.txt , July 2003. RFC 3561.

[8] D.B. Johnson, and D. A. Maltz, “Dynamic source routing in ad hoc wireless networks. In Mobile Computing”, T. tiefinski and H. F. Korth, Eds. Kluwer Academic PubUshers, Dordrecht, The Netherlands, pp. 153-181, 1996.

[9] T. Clausen and P. Jaqcquet, Optimized Link State Routing (OLSR) RFC 3626, IETF Networking Group, October 2003.

[10] M. Mauve, A. Widmer, and H. Hartenstein, “A survey on position-based routing in mobile ad hoc networks”. IEEE Network, Vol. 15, No. 6, pp. 30-39, 2001.

[11] I. Stojmenovic, “Position-based routing in ad hoc networks,” IEEE Communications Magazine, July 2002.

[12] R. Nelson and L. Kleinrock, “The spatial capacity of a slotted ALOHA multihop packet radio network with capture,” IEEE Transsactions on Communications, vol. 32, no. 6, pp. 684–694, Jun. 1984.

[13] G.G. Finn, “Routing and Addressing Problems in Large Metropolitan-Scale Internetworks”, Research Report ISU/RR-87-180, Inst. For Scientific information, Mar. 1987.

[14] H. Takagi and L. Kleinrock, “Optimal transmission ranges for randomly distributed packet radio terminals,” IEEE Transactions on Communications, vol. 32, no. 3, pp. 246–257, March 1984.

[15] Ting-Chao Hou Victor Li , “Transmission Range Control in Multihop Packet Radio Networks,” IEEE Transactions on Communications, vol. 34, no. 1, pp. 38- 44, Jan 1986.

[16] B. Karp and H. T. Kung, “GPRS: Greedy perimeter stateless routing for wireless networks,” in ACM/IEEE International Conference on Mobile Computing and Networking, pp. 243-254, 2000.

[17] I. Stojmenovic and X. Lin, “Loop- hybrid single-path/flooding routing algorithms with guaranteed delivery for wireless networks,” IEEE Transactions on Parallel and Distributed Systems, vol. 12, no. 10, pp. 1023 – 1032, October 2001.

[18] I. Stojmenovic and X. Lin, "GEDIR: Loop-free location based routing in wireless networks", IASTED Int. Conf. on Parallel and Distributed Computing and Systems, pp, 1025-1028, 1999.

[19] W.J Liu, K.T Feng, "Greedy Anti-Void Routing Protocol for Wireless Sensor Networks", IEEE Communications Letters, vlo. 11, no. 7, pp. 562-564, July 2007.

[20] Wen-Jiunn Liu; Kai-Ten Feng, Largest Forwarding Region Routing Protocol for Mobile Ad Hoc Networks, Proc. IEEE GLOBECOM, pp. 1 – 5, 2006.

[21] E. Kranakis, H. Singh, and J. Urrutia, "Compass routing on geometric networks", Canadian Conference on Computation Geometry (CCCG), pp. 51-54, 1999.

[22] Young-Bae Ko , Nitin H. Vaidya, "Location-aided routing (LAR) in mobile ad hoc networks", Proceedings of the 4th annual ACM/IEEE international conference on Mobile computing and networking, pp.66-75, 1998.

[23] S. Kalhor, M. Anisi, A.T. Haghighat, "A New Position-Based Routing Protocol for Reducing the Number of Exchanged Route Request Messages in Mobile Ad-hoc Networks", Proc. ICSNC, pp. 13 – 13, 2007.

[24] Jian Li; Mohapatra, P.v, "LAKER: location aided knowledge extraction routing for mobile ad hoc networks", IEEE Wireless Communications and Networking Conference (WCNC), pp. 1180 – 1184, 2003.

[25] S. Nanda, R.S Gray, "Multipath location aided routing in 2d and 3d", IEEE Wireless Communications and Networking Conference (WCNC), pp. 311-317, 2006.

[26] S. Basagni et al., "A Distance Routing Effect Algorithm for Mobility (DREAM)", Proc. of ACM MOBICOM'98, pp.76-84, 1998.

[27] W.H. Liao, Y.C. Tseng, J.P. Sheu, "GRID: a fully location-aware routing protocols for mobile ad hoc networks", Telecommunication Systems 18 (1−3), pp. 37−60, 2001.

[28] L. Blazevic et al., "Self-organization in Mobile Ad Hoc Networks: The Approach of Terminodes," IEEE Commun.Mag., pp. 166–75, 2001.

[29] Hossein Ashtiani, Shahpour Alirezaee, S. mohsen mir hosseini and Hamid Khosravi, “PNR: New Position based Routing Algorithm for Mobile Ad Hoc Networks“, Proceedings of the World Congress on Engineering, Vol 1, 2009.

[30] Daniel Câmara and Antonio A.F. Loureiro, "A Novel Routing Algorithm for Ad Hoc Networks," Hawaii International Conference on System Sciences, vol. 8, pp.8022 2000.

[31] Kai Zeng Kui Ren, Wenjing Lou, “Geographic On-Demand Disjoint Multipath Routing in Wireless Ad Hoc Networks”, Proc IEEE Military Communications Conference MILCOM, pp. 1-7 , 2005.

[32] E. Kuiper and S. N. Tehrani, “Geographic Routing With Location Service in Intermittely Connected MANETS”, IEEE Transaction on Vehicular Technology, Vol. 60, No. 2, pp. 592-604, 2011.

[33] K.T. Feng, C.H. Hsu and T.E. Lu, “Velocity-Assisted Predictive Mobility and Location-Aware Routing Protocols for Mobile Ad Hoc Networks, IEEE Transactions on Vehicular Technology, Vol. 57, No. 1, pp. 448-464, 2008.

[34] V. Namboodiri and L. Gao, “Prediction-Based Routing for Vehicular Ad Hoc Networks”, IEEE Transactions on Vehicular Technology, Vol. 56, No. 4, pp. 2332-2345, 2007.

[35] Bernhard H. Walke, Stefan Mangold and Lars Berlemann, *IEEE 802 Wireless Systems*, West sussex, England, John Wiley & Sons, 2006.

[36] S. Basagni et al., *Mobile Ad Hoc Networking*, IEEE Press and John Wiley & Sons, 2003.

Chapter 3

Forecasting Routing Technique using Location Information (FORTEL)

3.1 Introduction

Routing is one of the most critical challenges in multi-hop wireless networking, in general, and Mobile ad-hoc networks (MANETs), in particular. In the last decade, there has been given immense attention to the design and development of the routing protocols for MANETs, which turned to be a quit challenging research topic. Despite the fact that routing in MANETs has reached its peak in the early 2000s, the advantageous characteristics of MANETs such as ease of deployment and mobility support, urges the researchers to carry on developing new routing techniques. Besides, Vehicular Ad-hoc Networks (VANETs) as an emerging type of MANETs resulted in turning MANET routing protocols, especially the position-based one into a base for VANETs' routing methods. The above ensures that the protocol design for MANETs will remain one of the principal research topics in the area of wireless communications.

Numerous routing protocols and forwarding methods have been proposed and developed to respond the characteristics of MANETs such as lack of infrastructure, node heterogeneity, etc. Their main target is to achieve high routing performance at low cost in mobile scenarios, where the network topology changes frequently due to the nodes' mobility. These protocols cover different approaches and design choices, from topology-based, which utilise links between the mobile nodes as information to discover and maintain end-to-end

routes, to position-based, which decide the next node to forward the packet by looking into the geographical position of the mobile nodes.

The mobility support of MANET imposes serious limitations on the performance of the employed routing protocol. The link breakage that occurs due to nodes movement leads to outdated entries of the routing table rendering the discovered routes invalid. This enforces the protocol to generate control messages in order to either maintain the existing routes or discover new routes to the destinations. The control messages are broadcasted throughout the entire network consuming bandwidth and energy, as well as causing network delays and congestion that become critical in high mobility ad-hoc networks.

The routing table employed by topology-based protocols includes information about the links connecting the mobile nodes. Once a link breaks, the correspondent entry in the routing table becomes invalid and thus ignored by the protocol that will look for up-to-date information. In contrast, the outdated entries may remain useful to position-based approach, where the location table maintained by such protocols contain geographical position and movement information. This outdated information, representing the geographical position of the moving nodes at a past time, can be further utilised to predict their current position or their position at a future time. Such re-utilisation of the location table can be exploited to reduce the control messages by controlling the frequency of the location update messages dissemination.

Geographical or position-based routing uses the geographic position of the nodes to route the packet to the destination. Most protocols referring to this approach have been designed based on the assumption that any mobile node is connected to all the nodes within its radio range. The concept of the position-based or geographical routing is dated back to the 1980's, when several GPS-based methods were proposed [1], [2], [3] and [4]. The basic concept behind this type of routing is its reliance on the position of the destination to forward the data message to the next hop node, given that it satisfies specific criteria. A variety of criteria were proposed including distance, progress and direction; a detailed description can be found in chapter 3. A complementary concept of the geographical routing [5] incorporates location

information into the reactive techniques described in chapter 3. The use of location information improves the route discovery process by narrowing the request propagation area, which can significantly reduce the overhead generated in the network. In addition, all previously mentioned approaches assume that the geographical position of the destination is known by the source. While obtaining the position for a given destination requires the use of a position location service[3][7] and [8], such assumption may mask the real routing performance as the effect of the overhead, collision and congestion caused by the location service must be taken into account. For the sake of increasing the probability of reaching the destination and increasing the routing protocol performance in mobile scenarios, multipath strategy using geographical position was proposed [6]. The location information aids the protocol to engage in the forwarding process the nodes that are located in the direction of the destination. Nevertheless, transmitting data over multiple paths may introduce data redundancy, which impacts the collision level and network congestion, as well increasing the network overhead that includes, beside the location update messages, the unnecessary copies of the data message.

This chapter provides a detailed description of our proposed proactive position-based routing protocol entitled *Forecasting Routing TEchnique using Location information (FORTEL)*. This protocol is designed with the aim of achieving high deliverability in mobile ad-hoc networks, while introducing a low level of overhead, at the same time. FORTEL looks at the mobile network as a set of static networks with different topologies, and relies on the mobility prediction to forecast a future topology state of the network.

FORTEL being a proactive protocol, maintains a Location Table (LT) to store the location information of all the nodes in the network. The location information includes the geographical position, the node's speed and the movement's direction. FORTEL also relies on a forecasted version of the location table (FLT) to compute the end-to-end routes to the desired destinations. A tree representation of the destination's neighbouring nodes called Destination Connectivity Tree (DCT) is constructed from the forecasted location table, for route

[3] Position location service is a network protocol used to obtain the position of a given node in the network.

computation. The tree that includes all the destination's neighbours (1^{st}, 2^{nd} … n^{th} hop neighbours) results in obtaining *k* routes if exist. Furthermore, the key of FORTEL's performance resides in the accuracy of the location table and how up-to-date the stored information is. Therefore, an efficient location update mechanism is employed in order to increase the protocol robustness to the nodes mobility and the accuracy of the forecasted location information.

This chapter includes the following sections: section 4.2 describes FORTEL routing and provides a detailed presentation of the concept, the techniques and the protocol's components. Section 4.3 describes FORTEL's simulation model of and explains the output of the comparative analysis in various scenarios, while section 4.4 concludes the chapter.

3.2 Forecasting Routing Technique using Location information (FORTEL)

3.2.1 Location Information

FORTEL approach is based on the geographical concept of routing. The information required by the protocol is the location parameters of the mobile nodes. The location information consists of the position of the node, its speed and its movement direction. The position, usually in the form of geographic coordinates can be obtained from the Global Positioning System (GPS) or through any position identification system [9]. The direction represents the angle (in degree) that defines the node's movement deviation in respect to a previous position. The mobile nodes compute the above information periodically in order to keep aware of their mobility pattern.

3.2.2 Dissemination of Location Information

3.2.2.1 Hello message

In order to keep track of the nearby travelling nodes, the location parameters must be announced periodically by each mobile node to its one hop neighbours. The announcement is performed through a hello mechanism, according to which a periodic hello message is transmitted at a specified time interval. FORTEL's hello message is a small size packet, which includes the node's address and geographical position (X_i, Y_i), as shown in Figure 3-1. Upon receiving the hello message, the node stores the information in its neighbouring table and destroys it preventing the packet from being transmitted further, as it is a one-hop broadcast message.

Figure 3- 1: The format of FORTEL's hello message

3.2.2.2 Location update message

FORTEL is a proactive protocol, whose main parameter is the location table (LT), which populates information regarding the geographical position of the nodes in the network. As the mobile nodes move, their location information stored at every node's LT becomes invalid, therefore, any changes must be announced to the entire network by broadcasting location

update packets. The format of the FORTEL update packet, illustrated in Figure 3-2, includes the node's address, it location parameters (position, speed and direction) and a timestamp field to assure that only new updates are considered.

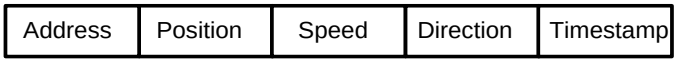

Figure 3- 2: The format of FORTEL location update packet

Thus, location update packets are broadcasted employing the basic flooding[4] mechanism to assure that they will be received by each and every node in the network. When receiving an update packet with a fresh timestamp, the node stores the embedded information in its location table and forwards it to all its neighbours. Updates having older timestamp will be ignored and will not be processed any further. The location update packet is featured by its small size, having therefore, a lower impact on the bandwidth and the medium occupancy than the routing control packets that carry topological information.

Furthermore, FORTEL location update packets may carry a couple of other information that that could potentially improve the routing decision. Such information includes the delay of the Medium Access Control (MAC), the node's residual energy etc.

3.2.2.3 Location Table (LT)

The location table is the main component of FORTEL protocol, according to which the end-to-end routes to any requested destination are computed. It contains the location information of all the nodes in the network and it reflects the network topology at the time the location updates are being received. The different elements of the location table's structure are identified to be the node's address, its geographical position represented by the coordinates (Xi, Yi), the radio range[5], the speed and the direction, as well as, the time the update was sent. An instance of the structure of the FORTEL location table is shown in Table 3-1.

[4] According to the basic flooding mechanism, every node in the network forwards a single copy of the broadcasted message.

[5] It is assumed, in this work, that the radio range is homogenous for all mobile nodes.

Table 3- 1: An instance of FORTEL location table

Node	Position	Speed	Direction	Time
192.168.1.1	(x_1, y_1)	v_1	θ_1	t_0
192.168.1.2	(x_2, y_2)	v_2	θ_1	t_1
192.168.1.3	(x_3, y_3)	v_2	θ_1	t_2

3.2.2.4 Switching mechanism "Hello" message/Location update

"Hello" messages are frequently used by MANET routing protocols as a mechanism to keep the mobile node up-to-date with its one-hop neighbourhood topology. These are exchanged amongst the one-hop neighbours and are not meant to be forwarded any further. On the other hand, FORTEL location updates are transmitted throughout the entire the network via the mobile nodes, which can be, therefore, considered as long-lived "hello" messages with no hop constraint. Thus, location update packets may take over the role of "hello" message. Accordingly, we introduce a switching mechanism between "Hello" and update messages depending on the mobility state of the nodes. FORTEL periodically sends "hello" messages as long as the nodes are stationary. Once the nodes start moving, the location update messages take over. Even though the size of the hello message is considerably small, its periodic broadcast causes overhead, interference with the data transmission, as well as, power consumption. Therefore, reducing the frequency of its transmission is believed to enhance the protocol efficiency and allow a higher bandwidth for data transmission, in addition to low resources utilisation, mainly, in terms of the node's residual energy.

3.2.3 Location update schemes

The routing performance of proactive protocols is completely dependent on the state of the routing information available at the source nodes. An up-to-date location table with accurate information can increase the protocol deliverability and can result in better performance. Moreover, the location update scheme, which carries the location information throughout the entire network, has a significant impact on the accuracy of the location table. The key design for any location update scheme is to determine the best frequency, at which a mobile node updates its location information. In this section, the basic constant rate update and mobility-

based schemes employed by FORTEL are discussed. Furthermore, a new scheme referred to as *window update scheme* is proposed with the aim of improving FORTEL's efficiency.

3.2.3.1 Constant rate update scheme

According to this scheme, the mobile node updates its location information, periodically, at every update interval. The update is performed regardless the speed and the pattern of the nodes' movement. This, however, may lead to a short-term inaccuracy of the location table during the time separating two consecutive updates. For instance, considering the movement trajectory of a mobile node MN shown in Figure4-3, where the points designate the positions at which the node deviates from its previous position and the arrows indicate the time at which the mobile node broadcasts a location update packet. The mobile node MN changes its movement's direction after a location update packet has been sent. The new direction will not be announced in the network and the other nodes deal with the old direction of MN. This continues until the next update is due. It can be clearly noticed that the event of the second deviation is announced after a time 'dt' through the update packet 'upd 5'.

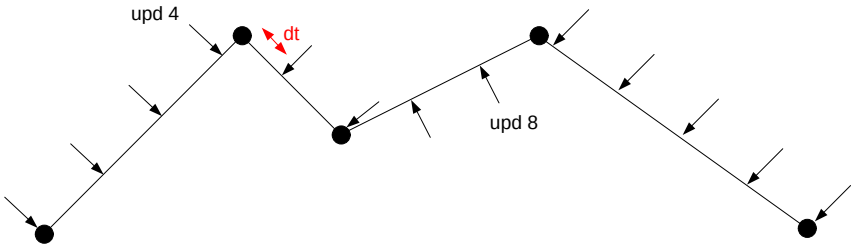

Figure 3- 3: The constant rate update scheme

3.2.3.2 Mobility-based update scheme

This scheme has been utilized by various protocols in order to keep the network up-to-date to the changes in the nodes' location information. Update packets are only being sent whenever changes occur to the movement's speed and/or pattern. Accordingly, a mobile node, MN, moving at constant speed through a fixed trajectory does not broadcast an update packet. Figure 3-4 shows the operation of the mobility-based update scheme, where the moments of broadcasting the update packet are illustrated by the arrows.

The performance of this scheme varies according to the pattern of the nodes' movement. Considering a scenario where slight movement changes occur, the generated overhead is very low as compared to the constant rate scheme. However, it is subject to a small accuracy issue in the location table that may occur, in the case the update packets experience a collision, which is likely to happen in mobile ad-hoc networks. The lost updates due to the collision lead to wrong records in the location tables of the mobile nodes and result in flawed routing operation. In contrast, in high variation mobile scenarios, where the nodes change speed and direction frequently, the mobility-based scheme tends to have similar performance to the constant rate scheme, as the mobile nodes update their location more often.

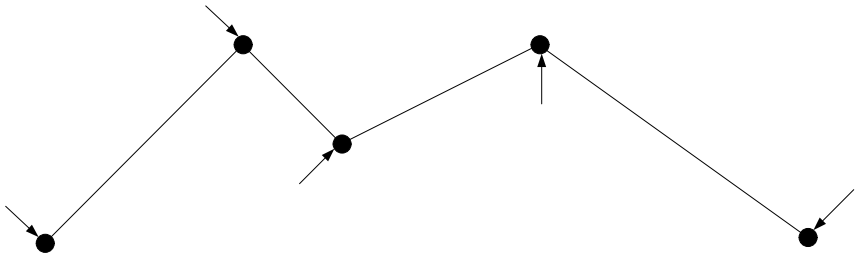

Figure 3- 4: The mobility-based update scheme

3.2.3.3 Window update scheme

Given the disadvantages of the previously mentioned schemes, we propose a new location update scheme that introduces the concept of the update window to the mobility-based update methods. According to the window update scheme, the mobile node updates its location whenever changes occur to its movement in terms of speed and/or direction. In case no variation is detected for a specific duration of time referred to as the "update window", the node must transmit an update packet. This can alleviate the drawback of the mobility-based scheme, increasing the protocol's robustness against topological changes, as well as controlling the overhead level through the update window size parameter. An instance of how the window update scheme works is illustrated in Figure 3-5.

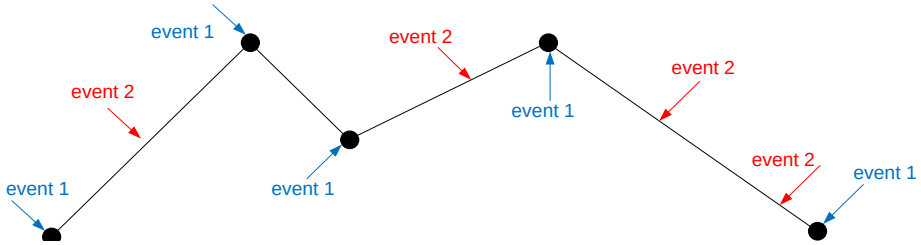

Figure 3- 5: The window update scheme

Thus, according to this scheme, the location information is updated due to two events:

Event 1: a variation occurs to the movement's speed and/or direction of the mobile node.

Event 2: the update window time is due.

However, the occurrence of 'event 2' is conditioned by the stability of the node's movement during the interval separating two incidences of 'event 1'. Therefore, the number of occurrences of 'event 2' could be defined by the following equation:

(4.1)

Where is the updated window size and is the duration separating two consecutive instances of 'event 1' and it is given by:

(4.2)

3.2.4 Destination Connectivity Tree (DCT)

The destination connectivity tree is the tree representation of the destination's neighbours for n hops. It illustrates the possible multi-hop connections that the destination maintains with other nodes in the network. To construct the connectivity tree of a destination D, the source node S refers to its location table to find the D's direct neighbours. The destination's direct neighbours are those nodes, whose Euclidean distance to D (given in equation 4.3) is less than or equal to the transmission range. Hence, the tree construction starts by setting D as the root and the direct neighbours as its children, while the link weights are the distance between D and the correspondent neighbours. The same tactic is applied at every child until the source S turns becomes the leaf of all possible links on the tree. At the end of the tree construction process,

one or several end-to-end routes to the destination are available, unless the network experiences a disconnection that makes the source destination communication impossible.

(4.3)

where (x, y) and (x_i, y_i) are the position coordinates of the given nodes.

The algorithm that computes the destination connectivity tree is a modified version of the Dijkstra [10] algorithm that determines the shortest path. Dijkstra algorithm works on a network, where the only known parameter is the link weight between the nodes. In our case, the know parameters that the designed algorithm is based on are the geographical position of the nodes. The implementation of the destination connectivity tree was accomplished using C programming language under OPNET [11] environment. Figure 3-6 depicts the pseudo-code of the algorithm that constructs the destination connectivity tree and compute route to the desired destination.

```
source node at packet generation
     compute route to destination
     insert route in the data packet if exist
     send packet

Intermediate node at packet reception
     if this node address is in the route forward the packet
     otherwise, discard

Algorithm   Compute Route; executed by the source node to compute a route to a specific destination
Input:      LocationTable, which is the table that includes the location information of all the nodes in the network
Output:     Route, which is the set of intermediate nodes that compose the end-to-end route to the destination
1 :begin
2 :  create a tree and set the desitnation as the root;
3 :    set the tree level 0 (the root);
4 :    insert the destination in a temporary list;
5 :   for each node in locationTable
6 :        if (the distance between the node and the destination is smaller than RadioRange)
7 :             insert the node in the tree as a child of the destination;
8 :        end if;
9 :    end for;
10:  do
11:    increment index;
12:    increment the tree level;
13:    for each currentNode in the current tree level
14:       insert the currentNode in the temporary list;
15:       for each node in locationTable
16:            if (the distance between the node and the currentNode is smaller than RadioRange)
17:            insert the node in the tree as a child of the currentNode;
18:            end if;
19:       end for;
20:    end for;
21:  while (index is smaller than the size of the temporary list);
22: if the size of the tree is positive and the source node is a leaf
23:    select the path with the lowest hop count;
24: end if;
25:end;
```

Figure 3- 6: The pseudo-code of FORTEL's route computation algorithm

For a better understanding of the concept of FORTEL's destination connectivity tree, consider the topology in Figure 3-7, in which node S0 communicates with S9 through intermediate stations in an ad-hoc network. The connectivity tree of the destination node S9 is shown in Figure 3-8, which reveals several possible routes connecting nodes S0 and S9.

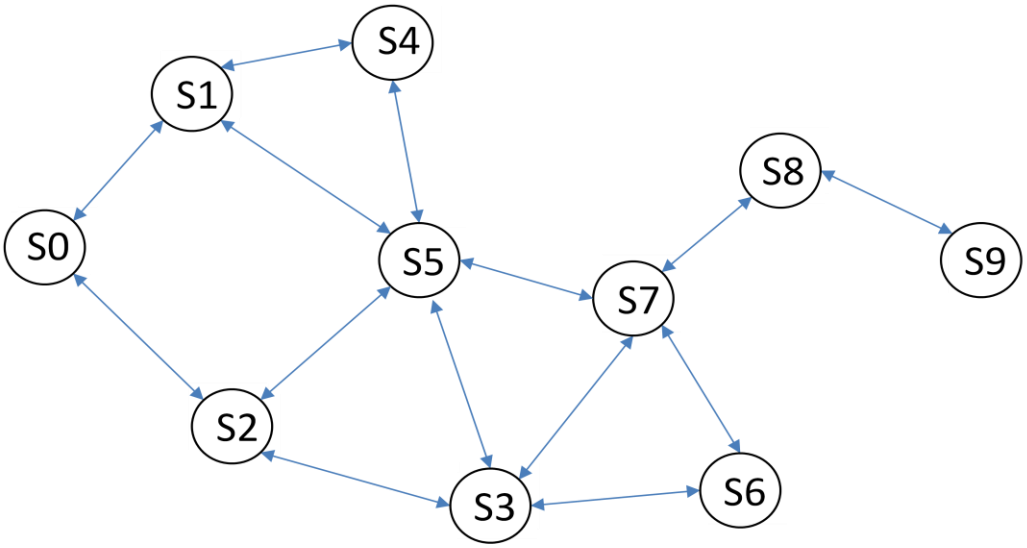

Figure 3- 7: An Ad-hoc network topology showing the possible connections amongst the mobile nodes

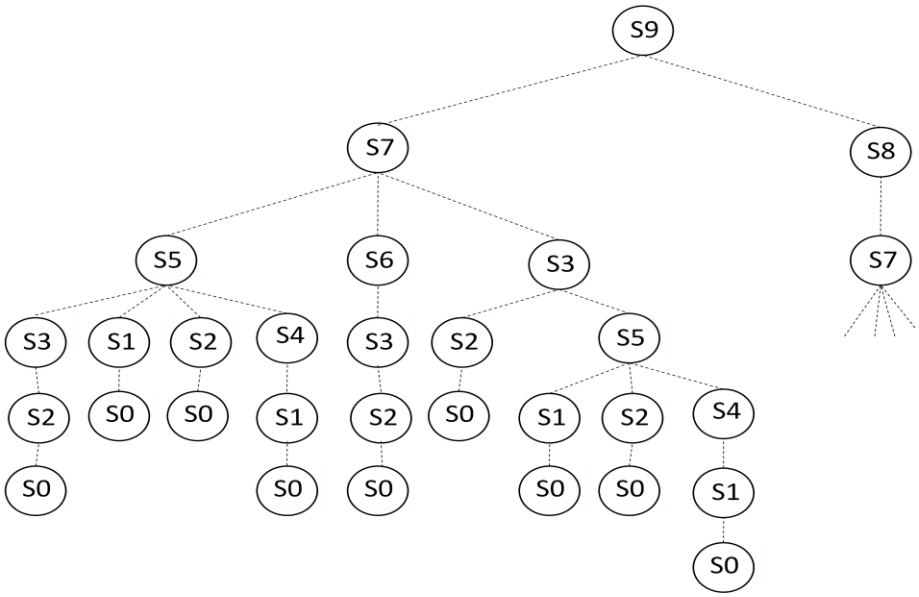

Figure 3- 8: Connectivity tree of the destination node S9

3.2.5 Routing metric

FORTEL's routing metric represents the total number of hops separating the source and the destination nodes. Having the destination connectivity tree of a destination node D constructed, the routing metric used to select and end-to-end route from a source node S is defined as follows:

$$FORTEL_{RM} = \quad (4.4)$$

Where, L_i, represents every link of a route to the destination D. 'TNH' is the total number of hops between the nodes D and S. Multiple routes may exist between source-destination peers, however, the route with the minimum number of hops is selected. In case of multiple routes having the same number of hops, the shortest, in terms of distance, is chosen.

3.2.6 Mobility Awareness

In Mobile Ad-hoc Networks (MANETs), the movement of the mobile nodes imposes serious limitations on the routing protocol, which needs to be responsive, in order to keep the communication active between the source and the destination. According to proactive approach, FORTEL updates the nodes' location information regardless whether or not there is data to transmit. Therefore, the information stored in the location table, which dates back to the time the updates were sent, may become outdated at the data transmission time. This may impact the route selection process and affect, in consequence, FORTEL's routing performance.

In connection with the preceding discussion and with the discussion presented in sections 4.2.2 and 4.2.4 relating to the significance of the location table accuracy, it is essential to define a mobility awareness function to increase FORTEL's robustness to nodes' movement. A forecasting mechanism for predicting the future position of the all the mobile nodes, and therefore, the network topology at a specific time would result in the mobility awareness function.

3.2.7 Mobility Function

3.2.7.1 Mobility prediction

FORTEL's mobility awareness includes the geographical position of the mobile nodes. The predicted positions, denoted by the coordinates (X, Y), are calculated using the equations (4-5) and (4-6).

$$X = \quad (4.5)$$

$$Y = \quad (4.6)$$

Where *'x'* and *'y'* are the initial coordinates stored in the location table and Δt is the time difference between the current time and the time at which the update packet was sent[6]. is the movement direction of the mobile node and is its speed.

3.2.7.2 Forecasted Location Table (FLT)

The objective of the mobility function is to make FORTEL adaptive to the nodes' movement and enhance the efficiency of its route selection process.

A node willing to transmit data to a specific destination should construct an updated version of the location table, referred to as Forecasted Location Table (FLT). This is achieved by predicting the geographical position of the mobile nodes at a given time based on the information of the location table that may be outdated at that time. The Forecasted Location Table (FLT) allows FORTEL to have an idea of the network topology at the transmission time, representing a more accurate view on the nodes' position than the information of the location table. This improves, in turns, the accuracy of the location information involved in the route determination. The corresponding Forecasted Destination Connectivity Tree (FDCT) will then be formed, from which an end-to-end route to the destination can be extracted.

The route computation process, which includes the prediction of location table and the construction of the connectivity tree, may bear computation costs in terms of processing time, power and device resources. The computation cost becomes significant, when the data traffic is generated at a high rate. Furthermore, a network with high mobility variation, in terms of speed and deviation, experiences a frequent exchange of update packets and, consequently, the location table changes more often. Transmitting the data over a single route for a long time may disregard updated information that can lead to a better route to the destination. Therefore, the time at which the mobile node computes new routes to the destination must be initiated at the lowest possible rate, while ensuring that the new location information, received due to the nodes' movement, as well as the data is always transmitted over the best available route.

[6] Corresponds to the packet's timestamp field displaying the position coordinates *'x'* and *'y'*

To fully comprehend the mobility function of FORTEL, we introduce an example presenting FORTEL's routing in mobile scenarios. Consider the mobile ad-hoc network of the Figure 3-9. The location table (LT_0) imitating the network topology at initial time t_0 is given in Table 3-2.

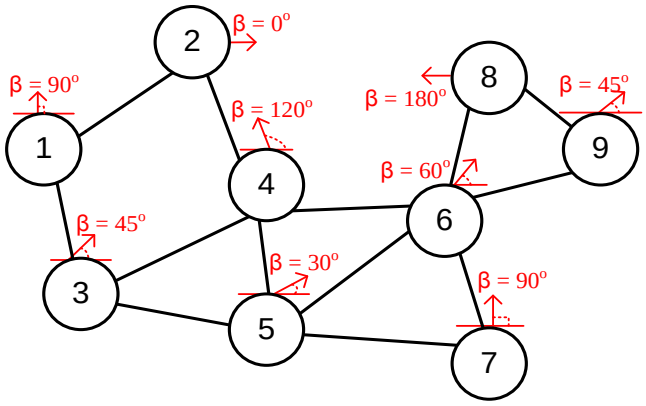

Figure 3- 9: Ad-hoc network topology showing the mobile node's movement directions

Table 3- 2: The Location Table (LT_0) at time t_0 = 0s

Node	(X, Y)	Speed	Direction	Time
192.168.1.1	(30, 110)	-	-	t_0
192.168.1.2	(70, 140)	-	-	t_0
192.168.1.3	(40,70)	-	-	t_0
192.168.1.4	(90, 100)	-	-	t_0
192.168.1.5	(90, 60)	-	-	t_0
192.168.1.6	(140, 90)	-	-	t_0
192.168.1.7	(150, 50)	-	-	t_0
192.168.1.8	(150, 30)	-	-	t_0
192.168.1.9	(180,110)	-	-	t_0

When the nodes start moving at time $t_1 > t_0$, the location table is updated upon receiving the location update messages transmitted by the moving nodes. The new Location Table (LT_1) is given in Table 3-3.

Table 3- 3: The Location Table (LT_1) at time t_1 =10s, following the updates messages

Node	(X, Y)	Speed	Direction	Time
192.168.1.1	(30, 110)	2	90°	$t_1+\varepsilon$
192.168.1.2	(70, 140)	2	0°	$t_1+\varepsilon$
192.168.1.3	(40,70)	2	45°	$t_1+\varepsilon$
192.168.1.4	(90, 100)	2	120°	$t_1+\varepsilon$
192.168.1.5	(90, 60)	2	30°	$t_1+\varepsilon$

192.168.1.6	(140, 90)	2	60^{o}	$t_1+\varepsilon$
192.168.1.7	(150, 50)	2	90^{o}	$t_1+\varepsilon$
192.168.1.8	(150,130)	2	180^{o}	$t_1+\varepsilon$
192.168.1.9	(180, 110)	2	45^{o}	$t_1+\varepsilon$

At a later time $t_2 > t_1$, when there is data ready for transmission, the transmitting nodes predict the future network topology, shown in Figure 3-10, based on the data of (LT_1) and the equations (4-5) and (4-6). The Forecasted Location Table (FLT) is presented in Table 3-3. Finally, each transmitting node can construct a DCT, from which an end-to-end route to the desired destination is extracted.

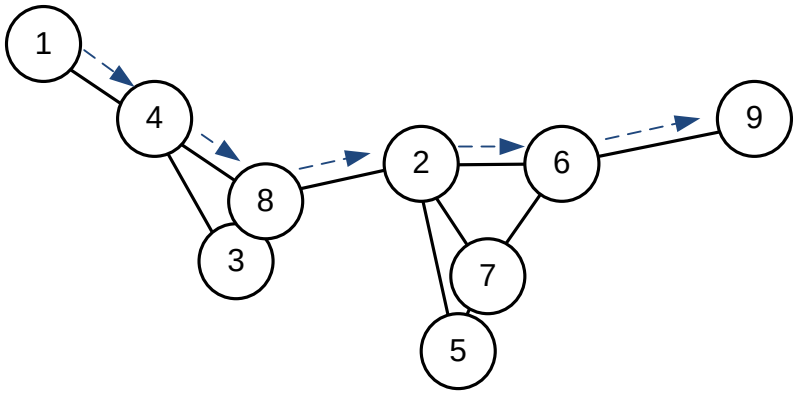

Figure 3- 10: The forecasted topology of the ad-hoc network at data transmission time t_2 = 40s

Table 3- 4: The forecasted location table (FLT) of the ad-hoc network following the mobility prediction process at data transmission time t_2 = 40s

Node	(X, Y)
192.168.1.1	(30, 170)
192.168.1.2	(130, 140)
192.168.1.3	(82.43, 112.43)
192.168.1.4	(60, 151.96)
192.168.1.5	(141.96, 90)
192.168.1.6	(170, 141.96)
192.168.1.7	(150, 110)
192.168.1.8	(90, 130)
192.168.1.9	(222.43, 152.43)

3.3 FORTEL performance evaluation and Results Analysis

3.3.1 Simulation Environment

FORTEL protocol has been implemented in OPNET 14.5 modeller [11]. Several mobile ad-hoc routing protocols were implemented in OPNET modeler such as Ad-hoc On Demand Distance Vector (AODV), Dynamic Source Routing (DSR) and Optimized Link state Routing (OLSR). A brief overview of OPNET 14.5 modeler and the detailed description of FORTEL models can be found in Appendix A.

FORTEL protocol evaluated in the current chapter comes in four versions, corresponding to the different location update schemes employed.

FORTEL mobility-based scheme (FORTEL-B): refers to the FORTEL protocol that employs the mobility-based update scheme, according to which location update messages are sent based on speed variation and movement deviation.

FORTEL constant rate scheme (FORTEL-C): refers to FORTEL the protocol that employs the constant rate update scheme, according to which location update messages are sent periodically at every update interval.

FORTEL window update scheme (FORTEL-W): refers to the FORTEL protocol that employs the window update scheme, according to which location update messages are transmitted based on the nodes' mobility and window update interval, given that no movement variation has been detected during that interval.

FORTEL epidemic (FORTEL-E): this FORTEL protocol version uses the exact position coordinates of the mobile nodes, obtained from the OPNET modeler's internal kernel of using predefined OPNET functions. FORTEL-E is highly accurate in terms of the location table and it performs routing regardless of the existence location update packets. We have introduced FORTEL-E, in the evaluation, to test the accuracy of the mobility prediction and the update scheme in mobile scenarios.

The designed network model consists of 50 wireless mobile nodes deployed in a two dimensional 500 x 500 square meters to form the desired mobile ad-hoc network. The IP addressing scheme is set to IPv4, while the PHY is configured to comply with the IEEE 802.11g (Extended rate PHY). Moreover, the constant bit rate (CBR) is 10 packets/sec with 1024 bits packet size and data rate being 24 Mbps, while the radio transmission radius is set to be homogeneous for all the nodes and equal to 97 meters.

During the simulation, the mobile nodes move within the simulation area based on the Waypoint mobility model [12]. According to the random Waypoint model, a mobile node chooses one random position as the destination and moves towards it at a constant or random speed. At the destination position, the node pauses for a predefined duration of pause time, selects another destination position within the simulation area and repeats the same process until the end of the simulation. In this study we have considered a constant speed, at which every mobile node moves to the randomly selected position. Twelve simulations were performed, while varying the ground speed of the moving nodes. The speed varies from 2m/s up to 40m/s including the following speeds: 4m/s, 6 m/s, 8m/s, 10m/s, 12m/s, 15m/s, 20m/s, 25m/s, 30m/s, 35m/s and 40m/s. Finally, 20 source-destination pairs were considered.

In order to allow a fair comparison, we have considered the same source-destination pairs across all the simulations scenarios, so the performance evaluation of the routing algorithms will be tested under same scenario and mobility conditions.

The simulation parameters are displayed in Table 3-5.

Table 3- 5: Simulation parameters

Network Simulator	**OPNET™ modeler**	
Simulation Area	500 x 500m^2	
Radio Range	97m	
Number of Nodes	50	
Mobility	Model	Random Waypoint
	Speed	[2m/s - 40m/s]
	Pause time	Uniform [5,10]
IP addressing scheme	IPv4	
MAC protocol	IEEE 802.11g	
Data rate	24 Mbps	
Data traffic	Packet inter-arrival time	0.1s
	Packet size	1024 bits
FORTEL parameters	Hello interval	2s
Simulation time	240s	

The performance evaluation of FORTEL is conducted using the following metrics:

- ***Average packet delivery rate:*** The ratio of the data bits received by the destinations to the data bits generated by the sources.
- ***Average network delay (seconds):*** It is the end-to-end delay of the packets for the entire network computed by considering the time elapsed between the time the packet was generated and the time it is received by the destination node. Therefore, it includes all the possible delays caused by the queuing, retransmission and propagation.
- ***Average control messages transmitted (bits/second):*** The number of transmitted routing control packets. In the case of DSR, control packets comprise route request, route reply and error packets while OLSR's and FORTEL's control messages comprise topology control and location update packets, respectively, in addition to "hello" traffic.

3.3.2 Results analysis

3.3.2.1 FORTEL-W for window sizes of 2s, 4s, 6s, 8s and 10s

Figure 3-11 shows the delivery rate achieved by FORTEL protocol. Different values for the update window size are chosen and the performance is conducted against the nodes' speed. The delivery rate and the window size are inversely proportional as it can be observed from the figure. As the update window size increments, FORTEL's delivery rate drops. For instance, FORTEL-W-10 delivers more data messages than FOTEL-W-2, although the latter update the location information more often (every 2 seconds).

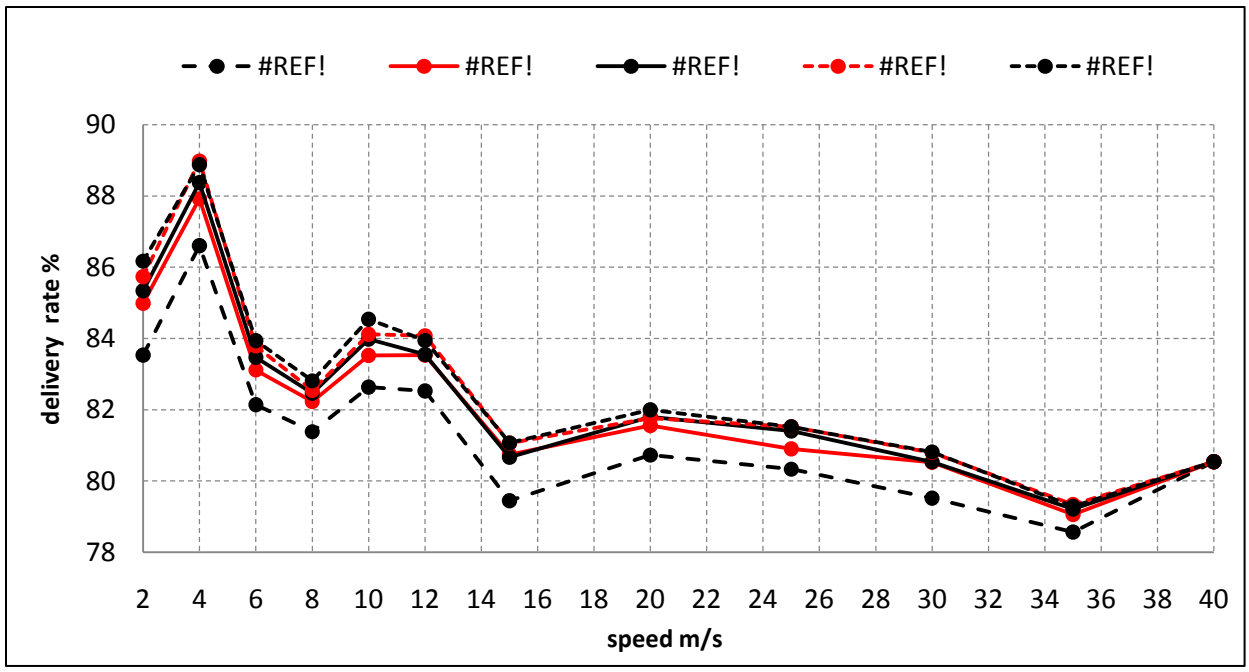

Figure 3- 11: Delivery rate (%) of FORTEL-W versus the nodes' speed

It also noticeable that the general curve of the delivery rate has a decremented shape as the speed increases, despite some fluctuations that are due to the randomness of the nodes' mobility. In theory, the delivery rate for a scenario of 4m/s speed should be less than a scenario of 2m/s speed, given that the trajectories travelled by the nodes during the simulation time are identical. However, according to the random waypoint mobility model, the positions to which the node moves are randomly selected and they differ from one scenario to another.

In Figure 3-12, the routing overhead, introduced by FORTEL to maintain the location table is presented. It is clearly illustrated that the shorter the update window size is, the more location update messages are exchanged, and so does the routing overhead.

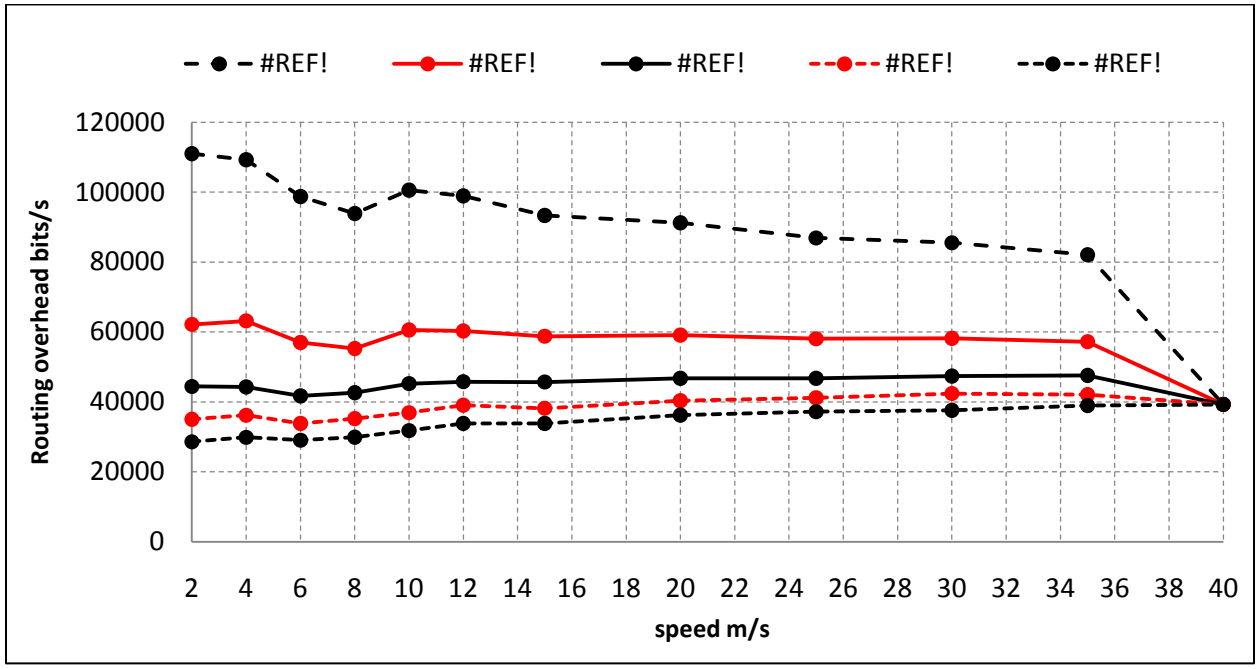

Figure 3- 12: Routing Overhead (bits/sec) versus the nodes' speed

We can also observe initially, that the overhead curve follows a decremented shape, which gradually increments. The two factors that affect FORTEL's routing overhead are: the movement variation and the update windowing. The relation between the two factors is given by the number of occurrences of event 2 'N_{event2}' (defined in equation 4.1) during the period separating two consecutive instances of event 1 'Δt'. Generally, as the nodes' speed increases, the duration 'Δt' becomes shorter and the number of events 2 'N_{event2}'. Therefore, smaller amount of location update messages is propagating in the network, when the speed of the nodes increases. On the other hand, according to the random waypoint model, the variation of the nodes' movement or, in other words, the number of trajectories that the nodes travel across is directly proportional to the nodes' speed. The higher the speed is, the more trajectories the nodes travel, and therefore, the more the location update packets transmitted by FORTEL. As a result, the aforementioned factors that influence the frequency of the location update packets vary oppositely, which, in turns, affect the shape of the routing overhead curve.

Besides, when a variation occurs to the nodes' movement, a location update packet is transmitted and the update window time is reset. Thus, the effect of update window becomes less significant at high speeds because the event of movement variation occurs more frequently and the window update timer is reset more often. Therefore, at high speeds, the location update packets are mainly transmitted due to the movement variation. The significance of the window effect is clearly shown in the figure, where the curves approach each other while the speed increases until they intersect at the speed of 40 m/s.

3.3.2.2 FORTEL-C for update rates of 1s, 2s, 3s, 4s and 5s

Figure 3-13 shows the delivery rate of FORTEL-C protocol that, periodically, broadcasts location update messages when different update rates of 1s, 2s, 3s, 4s and 5s are considered.

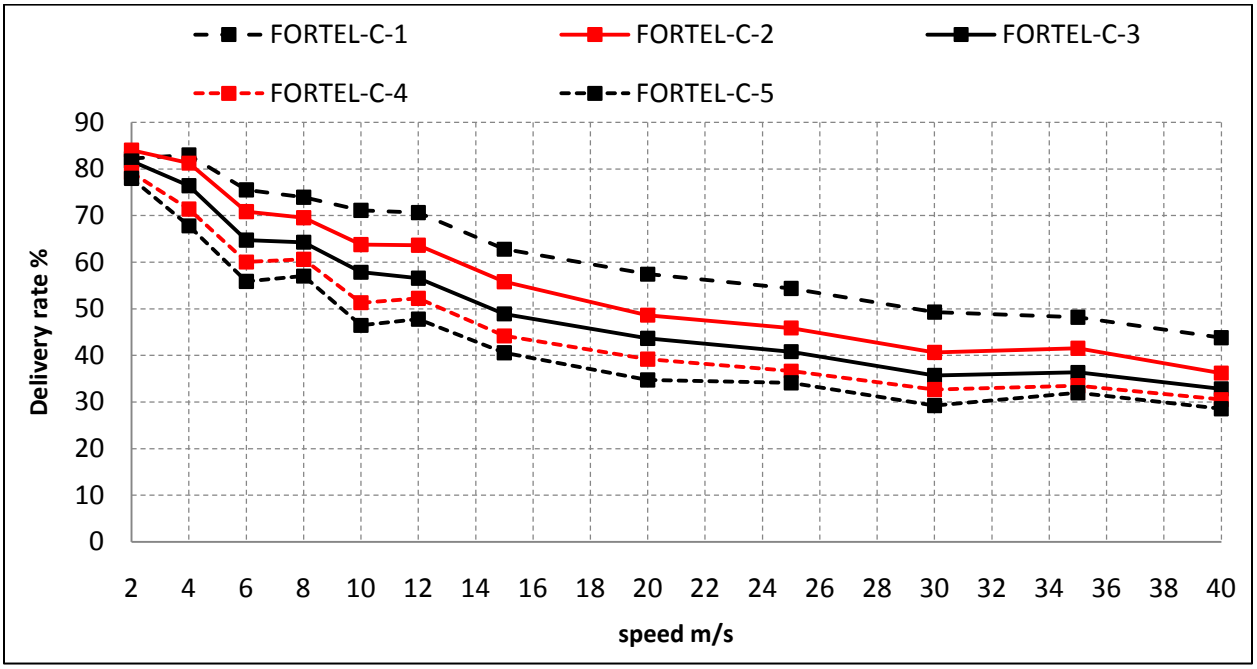

Figure 3- 13: Delivery rate (%) of FORTEL-C versus the nodes' speed

It becomes clear from Figure 3-12 that the percentage of the traffic delivered to the destination nodes decreases as the nodes' speed increases. The reason is that FORTEL-C transmits periodically location update packets regardless the mobility pattern and the movement speed of the mobile nodes. The periodic update may cause a skip of a movement variation event, which will be broadcasted at a later time when the next update is due. This effect introduces inaccuracy in the location table and affects, in turns, the routing performance, especially when

the nodes are moving at a high speed. Moreover, decreasing the rate at which the location update messages are sent can magnify the effect of omitting movement changes, causing therefore, a drop in the delivery rate.

The routing overhead of FORTEL-C for the considered update rates is illustrated in Figure 3-14. The overhead is directly proportional to the rate at which the location update packets are transmitted. As the rate increases, FORTEL-C broadcasts more control messages. Theoretically, the curve of a constant rate update scheme should maintain a constant shape as the update packets are periodically transmitted regardless the nodes' mobility. However, the higher the nodes' speed, the larger the number of trajectories the nodes go through. Therefore, the probability of packet collisions rises, especially when the update rate is high (FORTEL-C-1), leading to a higher level of packet drop. The packet drop impact, in turns, the total number of update packets propagating throughout the network. Finally, this effect becomes less significant for a higher update rate, at which the overhead curve tends to have a more constant shape (FORTEL-C-5).

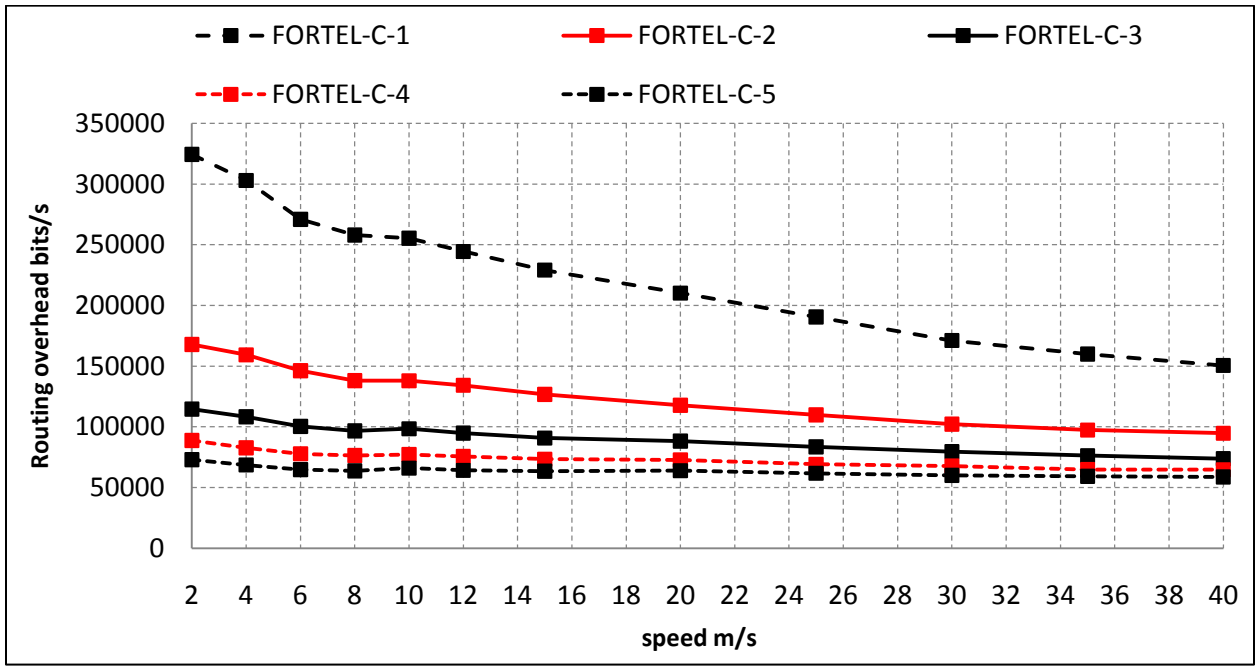

Figure 3- 14: Routing overhead (bits/sec) of FORTEL-C versus the nodes' speed

3.3.2.3 FORTEL-C vs. FORTEL-W vs. FORTEL-B

In this section, we compare the different versions of FORTEL protocol including FORTEL-B, FORTEL-C and FORTEL-W that correspond to the mobility-based, the constant rate and the window update schemes, respectively. Figure 3-15 proves that FORTEL-W protocol achieves the highest delivery rate showing the effectiveness of the window update scheme, especially for high speed movement. Besides, FORTEL-C outperforms FORTEL-B in low speed scenarios. However, as the speed increases, FORTEL-B shows better data delivery rate than FORTEL-C, whose delivery percentage drops dramatically.

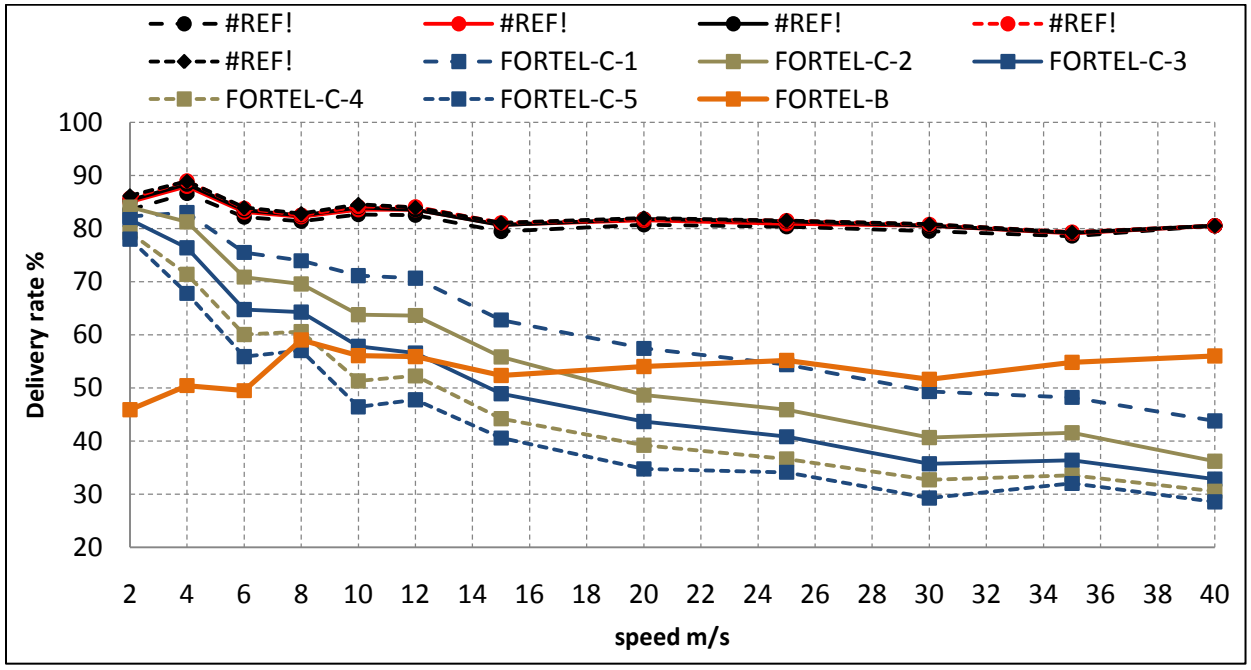

Figure 3- 15: Delivery rate (%) of the different versions of FORTEL (FORTEL-W, FORTEL-C and FORTEL-B) versus the nodes' speed

Figure 3-16 depicts the graph of the routing overhead. In addition to its high delivery rate, FORTEL-W and FORTEL-W-10, in particular, introduces a low routing overhead for different window sizes as compared to FORTEL-C and FORTEL-B, giving this version an overall significant advantage in performance. For instance, the overhead of FORTEL-W-2, which is the highest among FORTEL-W is approximately the same as that of FORTEL-C-3 and lower than that of FORTEL-C-2 by roughly 1200 bits/sec (8%).

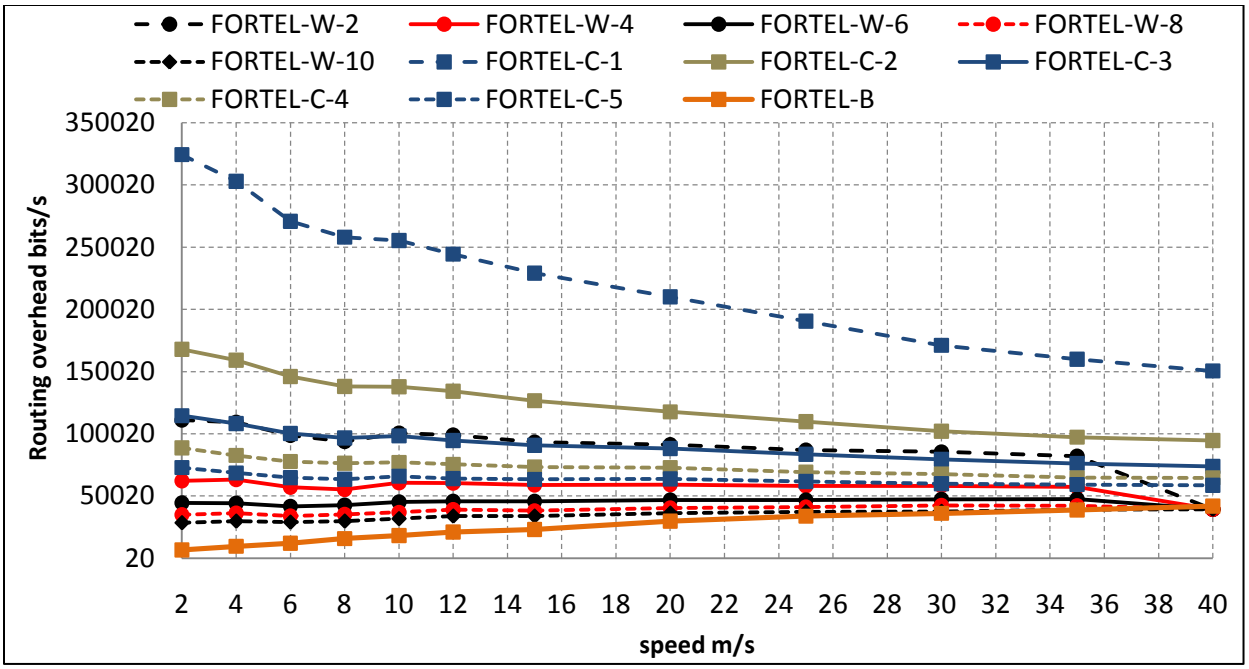

Figure 3- 16: Routing overhead (bits/sec) of the different versions of FORTEL (FORTEL-W, FORTEL-C and FORTEL-B) versus the nodes' speed

3.3.2.4 FORTEL-W vs. FORTEL-E

Figure 3-17 shows the delivery rate of the epidemic FORTEL (FORTE-E) compared with the FORTEL update window (FORTEL-W). FORTEL-E represents the most accurate version of FORTEL protocol that instantly (whenever there is data to transmit) uses the exact positions of the nodes, obtained through the internal kernel of the OPNET modeler, using predefined OPNET functions[7]. These positions will be utilised to construct the destination connectivity tree and then to determine the end-to-end route to the destination. Because the location table is the key element in FORTEL routing, FORTEL-E is expected to achieve the best performance that the FORTEL protocol can achieve in a mobile scenario. As illustrated in the figures below, the delivery rates achieved by FORTEL-W are very close the ones achieved by FORTEL-E, where the gap between does not exceed 2%.

[7] OPNET provides built-in functions to obtain the location of any nodes in the subnet
op_ima_obj_attr_get(node_id,"x position",&x);
op_ima_obj_attr_get(node_id,"y position",&y);

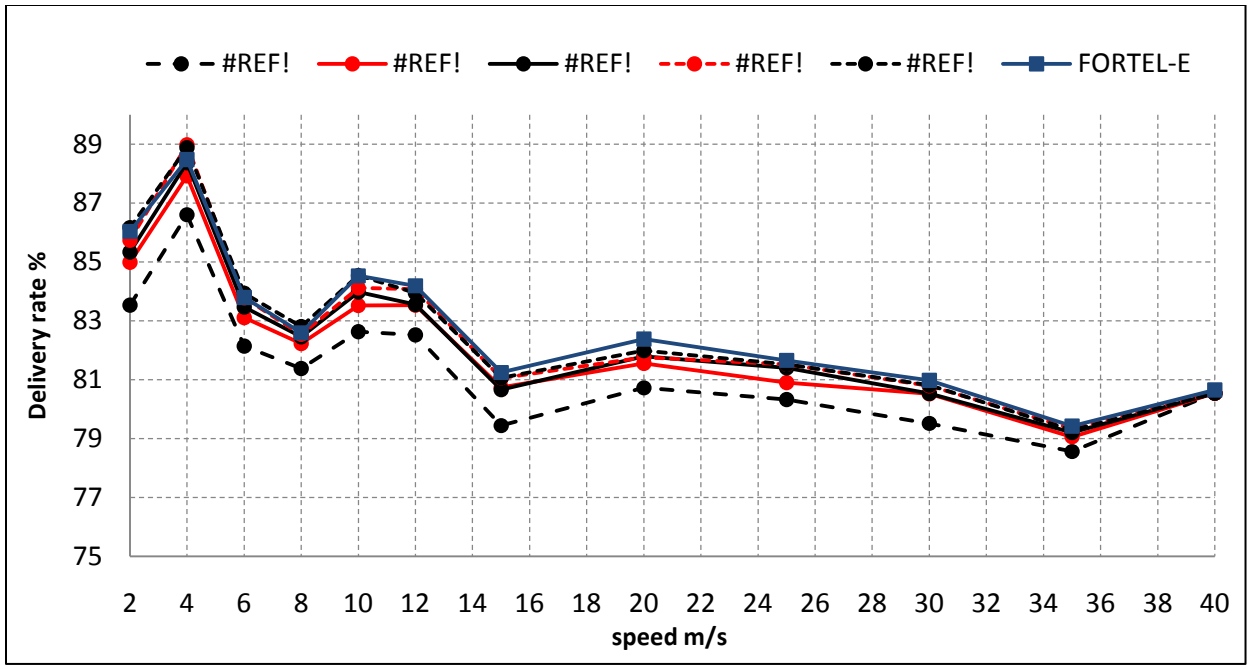

Figure 3- 17: Delivery rate (%) of FORTEL-W and Epidemic FORTEL versus the nodes' speed

The aim of this comparison is to demonstrate how efficient the dissemination of the location information is. As a result, the graphs reflects a significant performance of the window location update scheme employed by FORTEL, especially when considering a large update window size (w = 8 and 10s).

3.3.2.5 FORTEL vs. AODV, DSR and OLSR

In this section, we compare FORTEL protocol to some of the most known MANET protocols, including the reactive Ad-hoc On Demand Distance Vector (AODV), the reactive Dynamic Source Routing (DSR) and the proactive Optimized Link State Routing (OLSR). We have selected three versions of FORTEL each representing different location update schemes. Besides, FORTEL-B, FORTEL-W-10 with 10s window size and FORTEL-C-1 with 1s update rate are chosen for the comparison since they have achieved the best performance in their categories. The comparison is conducted in terms of the delivery rate, the end-to-end delay and the routing overhead against the nodes' speed that varies from 2m/s to 40m/s.

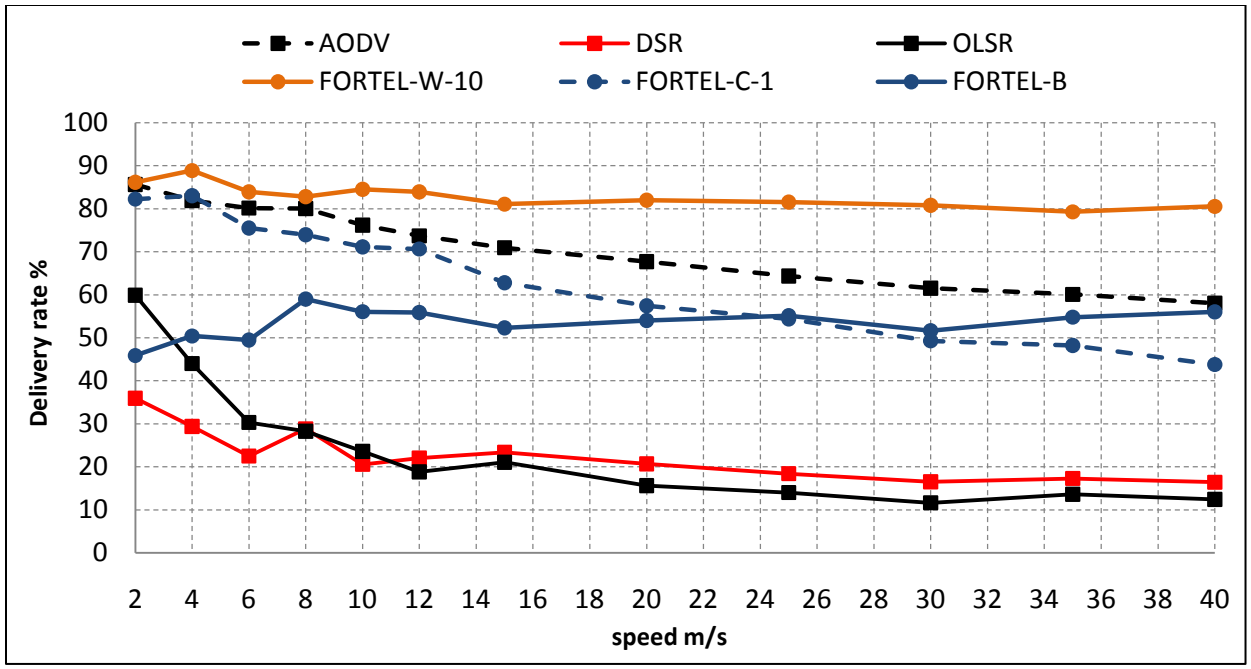

Figure 3- 18: Delivery rate (%) of FORTEL-C-1, FORTEL-W-10, FORTEL-B, AODV, OLSR and DSR versus the nodes' speed

Figure 3-18 depicts the delivery rate of the compared protocols, where it is clearly proven that FORTEL-W-10 achieves the highest delivery rate. In the meantime, while AODV, DSR and OLSR protocols fail to maintain the same level of performance as the speed increases, FORTEL (FORTEL-W-10 and FORTEL-B) show a steadiness in the delivery rate, which reveals its robustness to the nodes' mobility. The low delivery rates of DSR and OLSR are due to the validity of the end-to-end route at the transmission time. Both protocols have to wait for the updated information to be received (the route reply for DSR or the Topology Control (TC) messages for OLSR) to determine the next route to be used for the transmission. This information may, however become invalid at the time of transmission, especially when the speed of the nodes increases, meaning that a high correlation between the speed of the nodes and the route accuracy for DSR and OLSR exists. Such correlation is less significant in FORTEL that considers the future position of nodes in order to compute new routes to the destination. For instance, if a source 'S' is transmitting data to a destination 'D' through a route 'R1' but due to mobility the network topology changes, then the valid route becomes 'R2' instead. In order to switch the transmission over route R2, DSR has to initiate a route discovery and wait for the route reply to know where to direct the packet, while OLSR has to compute a new routing table after receiving a TC message. Whereas FORTEL is able to predict the nodes' positions by being

aware of their previous location information and, , interpret, in consequence, that 'R2' is the valid route to 'D' without the need to wait for any information. Finally, AODV protocol succeeded to achieve high delivery rate in low mobility scenarios. However, its performance drops dramatically as the speed increases.

Figure 3-19 illustrates the transmitted control messages of the compared protocols also known as the routing overhead. It is commonly known that proactive approaches maintain high routing overhead as compared to reactive approaches, since the latte discovers route on demand. However, the frequent link breakage that occurs due to the nodes' mobility initiates the route maintenance operation that introduces additional control messages in order to repair the broken routes. Besides, OLSR adopts efficient flooding to propagate the control messages, in contrast to AODV and DSR that utilise the basic flooding to disseminate the routing control packets.

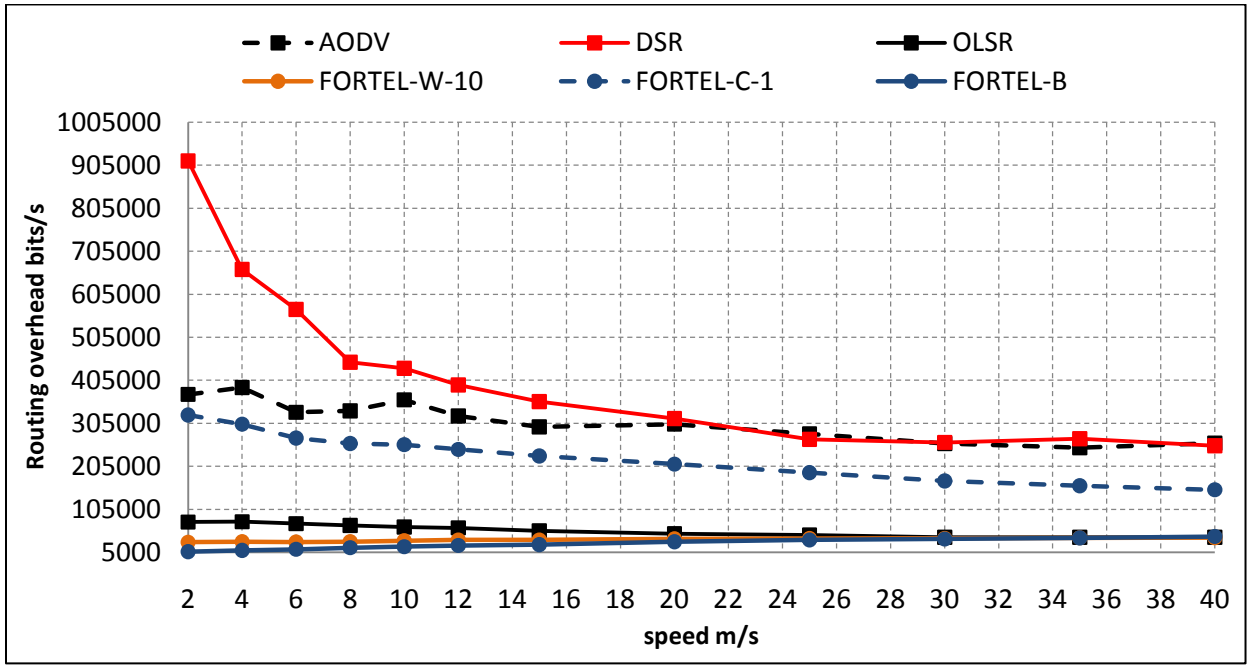

Figure 3- 19: Routing overhead (bits/sec) of FORTEL-C-1, FORTEL-W-10, FORTEL-B, AODV, OLSR and DSR versus the nodes' speed

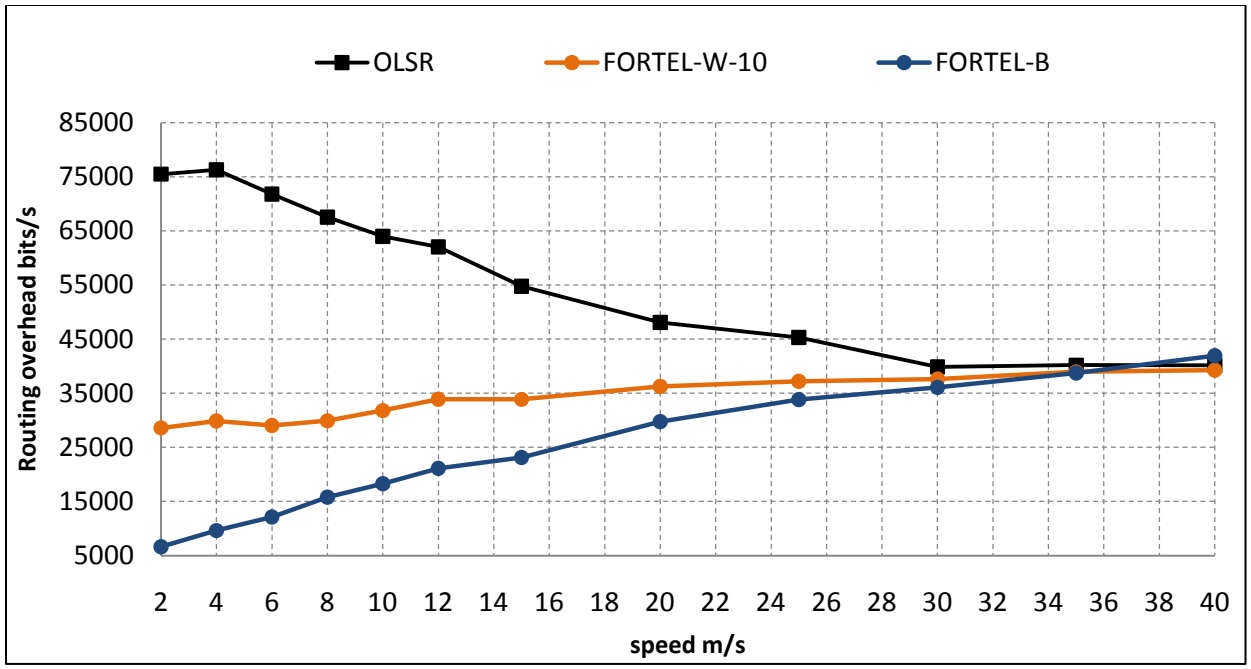

Figure 3- 20: Routing overhead (bits/sec) of FORTEL-W-10, FORTEL-B and OLSR versus the nodes' speed

Figure 3-20 shows the routing overhead of FORTEL-B, FORTEL-W-10 and OLSR protocols. As it is clearly illustrated, FORTEL-W-10 and FORTEL-B maintain lower overhead than OLSR while delivering, approximately, [25% - 60%] more packets.

The low overhead of FORTEL protocol is a result of two main factors. First, FORTEL update packet has a fixed and considerably small size as compared to packets carrying topology information. Second, FORTEL reduces the number of location updates that are transmitted based on the movement variation and the update window size. Despite the fact that OLSR efficiently broadcasts the control messages, FORTEL-B and FORTEL-W-10 that disseminate the location update using the basic flooding still generate lower routing overhead, while achieving significant performance in terms of delivery rate.

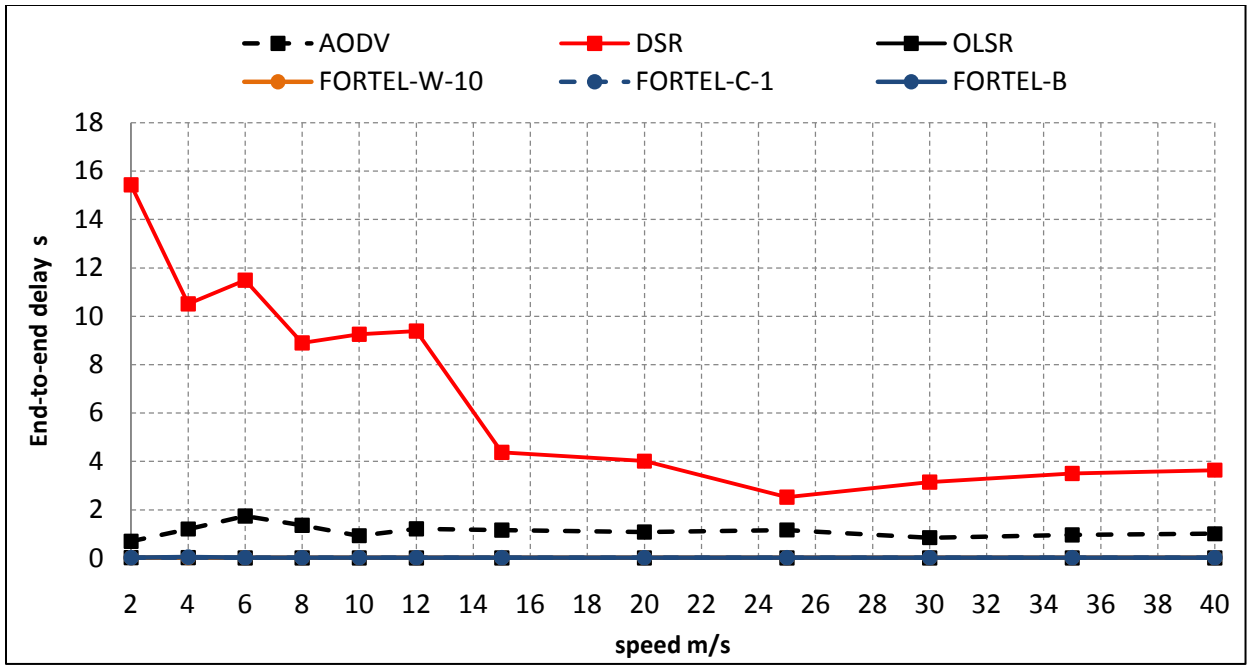

Figure 3- 21: End-to-end delay (sec) of FORTEL-C-1, FORTEL-W-10, FORTEL-B, AODV, OLSR and DSR versus the nodes' speed

Figure 3-21 presents the average delay in the network for AODV, DSR, FORTEL and OLSR. The high delay of AODV and DSR is mainly due to the delay caused by the discovery mechanism that reactive protocols support. According to that, the protocols have to wait for the route request and route reply packets to propagate back and forth to the source, prior to the data transmission. Note that AODV produces lower delay than DSR, which is due to two factors: 1) the reversal path feature that allows AODV to construct more routes to different destinations by propagating route request messages of the transmitting source nodes; 2) the hop by hop routing that turns the protocol to be less sensitive to mobility than the source routing. On the other hand, FORTEL and OLSR maintain lower delay due to routing information being available in advance.

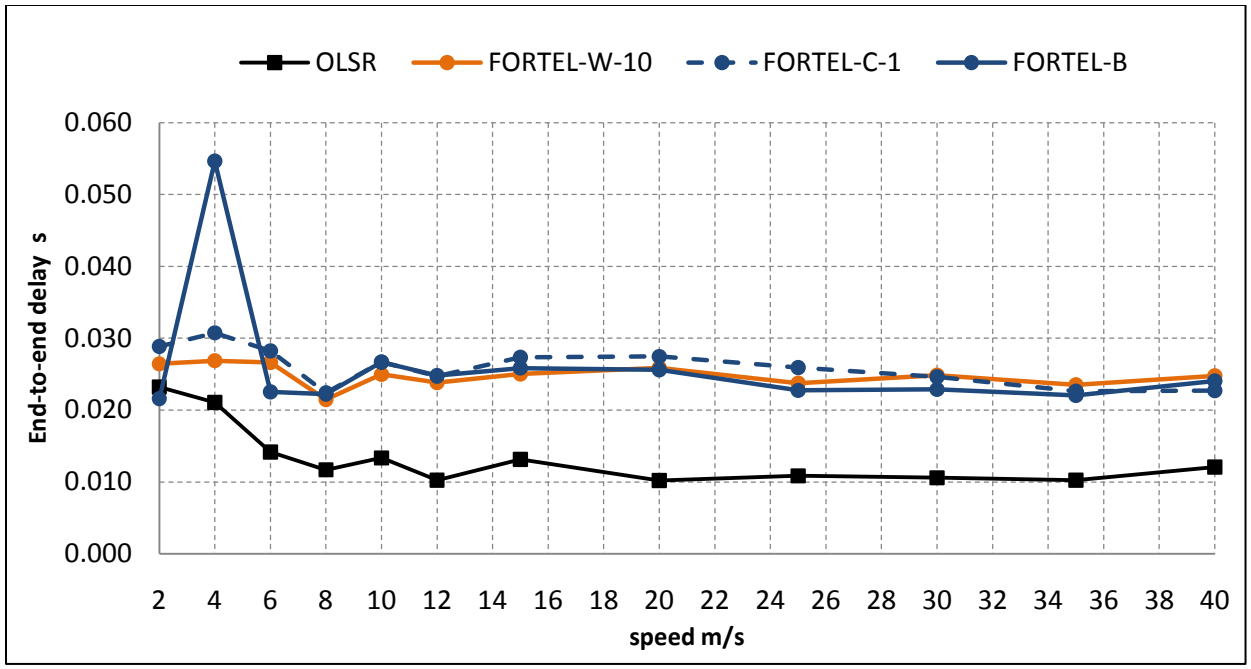

Figure 3- 22: End-to-end delay (sec) of FORTEL-C-1, FORTEL-W-10, FORTEL-B and OLSR versus the nodes' speed

Furthermore, OLSR's delay is lower than FORTEL's as shown in Figure 3-22. The main reason for that, as mentioned previously, is that FORTEL adopts basic flooding mechanism to disseminate location updates in the network, which causes higher network congestion as the number of nodes broadcasting the control packets is equal to the total number of nodes. Whereas, OLSR is designed to optimally disseminate the control packets by introducing the concept of Multi-point relays (MPRs), assigning the packets' dissemination task to a set of nodes. Therefore, the number of nodes broadcasting the control messages is significantly smaller, decreasing, therefore, the contention delay and the end-to-end delay.

3.4 Conclusion

This chapter presented a position-based routing protocol for Mobile Ad-hoc Networks (MANETs) called FORTEL. The proposed protocol utilises the nodes' position and their mobility information to setup and maintain an end-to-end route to the destination. However, the mobility feature of MANETs imposes serious limitations on the performance of the routing protocol. The link breakage that occurs due to nodes' movement leads to outdated link information entries in the routing table, rendering the discovered routes invalid. This enforces the protocol to generate additional control messages in order to maintain the existing routes or discover new routes to the destinations. As a result, the topology-based routing approach is less robust against mobility and fails to maintain good deliverability in high mobility scenarios. On the other hand, by involving location information in the routing process can increase the protocol's performance and reduce the level of overhead introduced to the network. According to the existing position-based approach, the routing process is executed hop-by-hop. Some methods assume that the position of the destination is known by the source node, ignoring, therefore, the effect of the location service, whereas multipath routing is adopted by some others to increase the chances of reaching the destination. FORTEL is designed to route data traffic through a single path to the destination, while the entire end-to-end route is known by the source. Moreover, the key element in any position-based protocol is the update mechanism of the location information that can change significantly the protocol's performance. Two location update schemes have been integrated with FORTEL to keep the location table up-to-date with the position changes. While the first correlates the update function to the movement deviation and speed variation, according to the second, the update messages are transmitted at a constant rate. To further enhance the protocol's performance, we have defined a new scheme referred to as the window update location that serves as an improvement to the first scheme previously mentioned.

Based on simulation tests as well as on the random waypoint mobility model, FORTEL demonstrates high message delivery in high mobility scenarios, while maintaining a low level of routing overhead at the same time. The window update scheme has proven the best performance among the three location update schemes employed and has shown more than

20% improvement in scenarios with high speed movement. Furthermore, the comparison made between FORTEL, AODV, DSR and OLSR demonstrates clearly that FORTEL window (FORTEL-W) achieves the best performance in terms of delivery rate and routing overhead. FORTEL-W outperformed AODV by approximately 10%, and DSR and OLSR protocols by more than 50% in terms of delivery rate, when high speeds were considered.

Finally, the main objective that routing protocol design is trying to achieve, especially when high mobility ad-hoc networks are being considered, is high message delivery rate, while maintaining a tolerable end-to-end delay with a low level of routing overhead, at the same time. Accordingly, FORTEL hits that target by achieving a considerably high delivery rate (FORTEL-W10) and a low level of routing overhead and end-to-end delay.

References

[1] R. Nelson and L. Kleinrock, “The spatial capacity of a slotted ALOHA multihop packet radio network with capture,” IEEE Trans. Commun., vol. 32, no. 6, pp. 684–694, Jun. 1984.

[2] G.G. Finn, “Routing and Addressing Problems in Large Metropolitan-Scale Internetworks”, Research Report ISU/RR-87-180, Inst. For Scientific information, Mar. 1987.

[3] H. Takagi and L. Kleinrock, “Optimal transmission ranges for randomly distributed packet radio terminals,” IEEE Transactions on Communications, vol. 32, no. 3, pp. 246–257, March 1984.

[4] Ting-Chao Hou Victor Li , “Transmission Range Control in Multihop Packet Radio Networks,” IEEE Transactions on Communications, vol. 34, no. 1, pp. 38- 44, Jan 1986.

[5] Y-B Ko and N. H. Vaidya, “Location-Aided Routing (LAR) in Mobile Ad Hoc Networks”, ACN/Baltzer Wireless Networks (WINET) journal, Vol. 6, No. 4, pp. 307–321, 2000.

[6] S. Basagni et al., A Distance Routing Effect Algorithm for Mobility (DREAM). Proc. of ACM MOBICOM, pp.76-84, 1998.

[7] T. Camp, J. Boleng, and L. Wilcox, “Location information services in mobile ad hoc networks”, in IEEE International Conference on Communications, pp. 3318-3324, 2002.

[8] R. FRIEDMAN, AND G. KLIOT,” Location services in wireless ad hoc and hybrid networks: A survey”. Tech. rep. CS-2006-10, Technion, Haifa, 2006.

http://www.cs.technion.ac.il/users/ wwwb/cgi-bin/tr-info.cgi?2006/CS/CS-2006-10.

[9] S. Capkun, M. Hamdi and J.P. Hubaux, “GPS-free positioning in mobile ad-hoc networks”, Hawaii Internat. Conf. on System Sciences, 2001.

[10] DIJKSTRA, E W. A note on two problems m connexion with graphs. Numer. Math. 1 , pp. 269-271, 1959.

[11] OPNET Modeler, OPNET Technologies, Inc ®. Available: http://www.opnet.com.

[12] H. Hartenstein, C. Bettstetter and X. Prez-Costa, “Stochastic Propoerties of the Random Waypoint Mobility Model”, ACM/ Kluwer Wireless Networks, special issue on Modeling and analysis of mobile networks, Vol. 10, No. 5, pp. 555–567, 2004.

Chapter 4

Sender Suppression Algorithm for Beaconless Routing

4.1 Introduction

Mobile Ad-hoc Networks (MANETs) have witnessed intensive research attention in the last decade from both academic and industrial sectors. This is due to their distinctive features in terms of self-organizing, self-configuring, infrastructure-less and multi-hop communication capabilities. Moreover, substantial amount of work has been done across all the OSI layers from the application to the MAC, and the network layer in particular, at which numerous routing algorithms have been proposed in order to provide reliable routing, robust against nodes mobility.

Numerous routing algorithms have been developed to provide the best performance in mobile ad-hoc networks. Some of them rely on a global knowledge of the network, while some others require the neighbouring information by the use of beacon messages technique. The global knowledge of the network costs the protocol a high amount of overhead and may cause congestion and delay problems, especially when dealing with high mobility scenarios. To avoid the before mentioned issues, the one-hop routing strategy is introduced. The only information needed for routing is the neighbouring information that can be obtained through the periodic exchange of beacons. Although the beacon message is a small size packet, its frequent broadcast, may degrade the network performance by producing additional collisions and interference with data packets being routed [1] as well as occupying an important part of the available bandwidth that can be saved data transmission. In addition, the energy consumed by

the beaconing process can raise issues for the wireless nodes in terms of their battery lifetime. Beaconless routing approach has been proposed to overcome the drawbacks of the beaconing mechanism. Its significance lies on the fact that routing is performed reactively without having knowledge of the neighbouring nodes. The selection process of the next hop relaying node is executed in a distributed manner based on the concept of contention delay. Contention-Based Forwarding [2], being a scheme of the beaconless routing approach does not require exchange of any routing or location information between neighbouring nodes, eliminating, therefore, the effects that beacon messages have on the network's performance. The forwarding decision is the responsibility of the receiving nodes that compete with each other for the right to forward the packet. The main idea behind CBF is that the node holding a packet broadcasts it to all its one hop neighbours, while the receivers of the packet set timers based on their distance to the destination. Once a timer runs out, the node re-broadcasts the packet and all the other nodes that have active timers cancel their timers when hearing the retransmission. The same procedure is followed at every hop until the packet has reaches the destination. Thus, the receiver that firstly responds to the timer run out is the next hop node to forward the packet. The operation of preventing one or a set of nodes to proceed with the re-broadcast is called suppression. The basic form of such operation is illustrated when some of the receivers cancel their timer upon hearing the re-broadcast of the packet. Nevertheless, the main challenge of the beaconless routing methods is the packet duplication that occurs mainly due to the hidden node problem. According to the hidden node problem, the receivers of the packet are out of range of each other, this unable to overhear each other's transmission. Additionally, due to the minimum routing overhead required, beaconless approach can be a suitable routing method for vehicular ad-hoc networks (VANETs) ([3], [4], [5] and [6]), which are characterized by high node density and mobility constraint due to traffic regulations (traffic light, speed limit, road signs etc…). The previous discussion underlines the significance and the importance of packet suppression and beaconless routing research area, since vehicular communications is a very recent topic that has been evolving quite rapidly.

Here was the motivation to improve the performance of beaconless routing by solving the packet duplication problem. In this chapter, we propose a new suppression algorithm that

aiming to eliminate the packet duplication issue, at the cost of low overhead, delay and bandwidth occupancy. The algorithm is called Sender Suppression Algorithm (SSA). SSA explores the idea of dividing the forwarding zone of the sender into three zones, as well as introducing a time delay at each of the zones to prevent simultaneous packet forwarding caused by hidden nodes. Moreover, the sending node is involved in the suppression process in order to inform the competing candidates of the actual node that will be forwarding the packet, ensuring, therefore, that the transmitted packet is only relayed once.

The rest of the chapter is organized as follows: Section 5.2 overviews the existing beaconless routing methods and discusses the suppression algorithms. Section 5.3 describes the proposed sender-based suppression algorithm. Section 5.4 presents the simulation results and eventually, section 5.5 concludes the chapter.

4.2 Related Work

4.2.1 Beaconless routing

Several beaconless routing [7] schemes have been proposed to overcome the drawbacks of the conventional routing schemes that require routing information maintenance, regardless it is global (update packets) or local (beacon messages). The routing phase is reactively performed, in which the sender broadcasts the packet without the help of the neighbouring information. Beaconless protocols obey to a similar routing concept and consist of three phases:

1) *Packet broadcast*

   The node holding the data packet at a given time, broadcasts a message to all its neighbours. The broadcasted message can be either the data packet or a special control message, which is used by some beaconless methods to assist in the node selection phase.

2) *Timer setup*

   Upon receiving the broadcasted packet, each node sets a contention timer based on its progress to the destination. The timer's value indicates how much the node's progress towards the destination is.

3) Next hop node selection

The last phase consists of selecting the next hop node to relay the packet. The node that is selected to relay the data packet is the one whose timer runs out first. Once its timer runs out, the node rebroadcasts the data packet to all its neighbours and is implicitly selected as the next hop node. In case the broadcasted packet from phase 1 is a control packet, the node transmits a control packet back to the sender that will explicitly select it as the next hop node using unicast transmission.

In addition, the beaconless routing approach supports a recovery mechanism, which is executed when the node holding the packet has no closer neighbour to the destination than the node itself.

The first beaconless routing algorithms, CBF [2], BLR [8] and IGF [9] use greedy criterions to define the set of candidates that will participate in the contention process. The candidate with the greatest progress towards the destination is given the shortest timeout and, therefore, the privilege to relay the packet. The protocols use a restricted forwarding such as Reuleaux triangle or 60^{o} sector towards the destination (Figure 4-1), which ensures that all the nodes within this area can overhear each other's transmission.

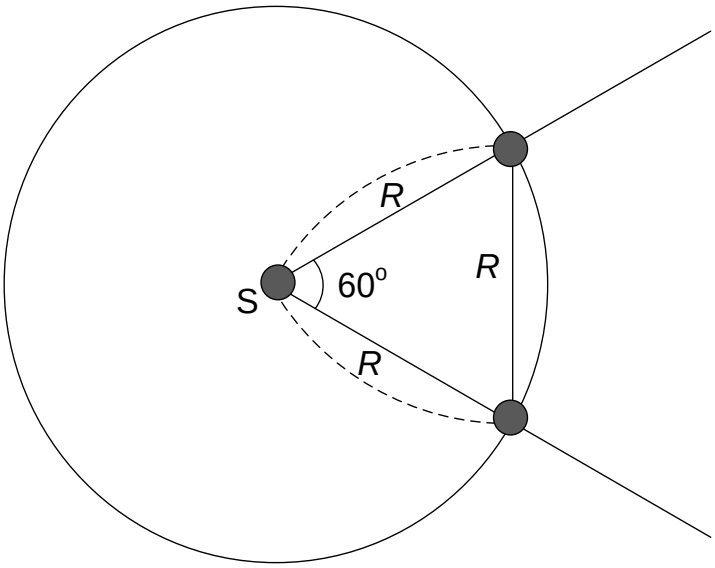

Figure 4- 1: Restricted forwarding area based on Reuleaux triangle and 60^{o} sector

Further studies that address the beaconless concept of routing are those proposed in [10-25], which follow similar contention and node selection processes mentioned above. Similar to CBF scheme, Geographic Random Forwarding (GeRaF) [12] introduces a forwarding technique based on the nodes' geographical location, according to which the relaying node is randomly selected via a contention process among receivers. The main advantage of GeRaF scheme is the collision avoidance mechanism based on the concept of busy tone [13], which is considered to be used before the carrier sensing scheme. In [14], Blind Geographic Routing (BGR) is proposed. The enhancement of BGR resides in the recovery strategy as well as in the newly introduced mechanism called Avoidance of Simultaneous Forwarding, which is used to prevent simultaneous transmissions by nodes almost equidistant with the destination. According to BGR's recovery process, the forwarding area is shifted by 60^{o} to the left or to the right, increasing the chance of finding suitable candidate that can lead the communication towards the destination. Beaconless On Demand Strategy for Geographic Routing (BOSS) [15] has been designed to overcome the loss and collision problems of the radio communications. Three way handshake mechanism (RTS/CTS/ACK) and a Discrete Dynamic Forwarding Delay (DDFD) function are employed to reduce collisions and message duplications produced during the selection phase of the next hop forwarding node. According to the DDFD function, the neighbours providing the maximum progress towards the destination are assigned with smaller delay times. This is achieved by dividing the neighbourhood into a set of subareas, where each subarea consists of neighbours with similar progress the destination (see Figure 4-2). The forwarding delay for nodes located in the same subarea is defined as a common base time plus a random number of milliseconds.

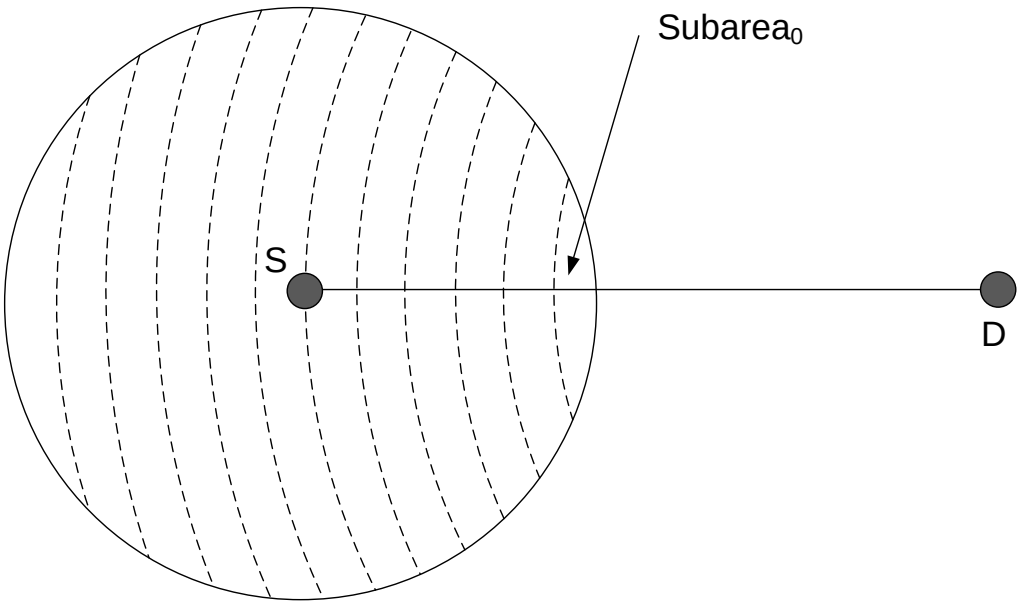

Figure 4- 2: The different subareas defined by BOSS protocol

In addition, BOSS transmits the data payload in the RTS packet in the form of long messages, which are more susceptible to channel error than short messages. Enclosing the data packet with the RTS packet ensures that the selected neighbour will be among the nodes that successfully receive the data packet. A beaconless scheme, designed to satisfy the end-to-end real-time requirements with less energy consumption, is Contention-Based Beaconless Real-Time Routing (CBRR) Protocol [16]. CBRR integrates the contention mechanism and the neighbouring table to relay a packet to its destination. The entries of the neighbouring table are obtained via the contention mechanism instead of beacons. Two CBRR schemes are further proposed: CBRR-OneHop and CBRR-TwoHop, which are based on one hop and two hop neighbour tables respectively. When a node has data to send, CBRR initiates the contention process in order to select a next hop forwarder that will be added to the neighbouring table. The following packets will be transmitted to the selected next hop node using unicast if there is an appropriate entry in the neighbour table that meets the delay and speed constraint.

Moreover, in contrast to the conventional contention based forwarding, On-demand Geographic Forwarding (OGF) [17] does not apply the contention process every time a data packet is ready to be sent. It maintains a forwarding table, where next hop node information collected through contention process is stored, to be utilised for later data forwarding. In

addition, Priority-based Stateless Geo-Routing (PSGR), proposed in [18], states that the receivers of the data packets are able to locally determine their priority to become the next relaying node. The main concept behind PSGR is the dynamic forwarding zone formation mechanism, which is based on the node density estimation and the autonomous acknowledgement. The forwarding region, being the area that includes the potential candidate for next hop packet forwarding, is divided into zones with an acknowledgment timer interval associated with every zone. The candidates determine their response waiting time autonomously, without intervention from the packet's sender, depending on the forwarding zone they belong. Furthermore, selecting a large forwarding zone raises the issue of packet duplications, while a smaller one results in a longer acknowledgment delay. To overcome these extremes, PSGR takes node density estimation into account to dynamically set the forwarding zone to an area that contains one candidate only. Finally, node density is estimated based on the number of neighbours that are within the node's radio range for a certain time window, which is in turns, obtained by considering the number of messages that the node hears/overhears.

An improvement of the BLR algorithm is proposed in [19], which integrates into the delay function of the contention process, the accumulated signal strength of all the received messages in a short period. Contention-based Beaconless Geographic Routing (CBGR) [20] supports two modes of operation, basic and optional mode. CBGR's basic mode is similar to the contention process of typical contention-based beaconless schemes, while the optional mode employs a link forecast mechanism that transmits the subsequent packets to the same node selected in the basic mode. Energy-Efficient Beaconless Geographic Routing (EBGR) [21] incorporates energy consumption in the routing operation. Its key concepts are the ideal relay position that minimizes the total energy consumed when delivering a packet and the relay search zone, which contains the candidates that participate in the contention process. When there is data to transmit, the closest node to the ideal position is selected as the next hop relaying node through the use of the contention process and the RTS/CTS handshake mechanism.

4.2.1.1 Contention-Based Forwarding (CBF)

The forwarding process of CBF [2] includes two phases: the contention process and the suppression phase. The contention process starts after the node, holding the packet at a given time, forwards it to all its neighbours. The process is initiated once all the receivers set a local timer based on their progress to the packet's destination. The timer, which is defined in equations 4-1 and 4-2, indicates the waiting period before the node attempts to reforward the packet.

$$progress = Max(0, (dist(S, D) - dist(N_i, D)/R)) \quad (4.1)$$

$$timer = T * (1 - progress) \quad (4.2)$$

Where, *dist(S, D)* is the distance from the source to the destination, *dist(N_i, D)* is the distance from node N_i to the destination, *R* is the transmission range and *T* is the maximum forwarding delay.

When the timer runs out the node reforwards the packet to all its neighbours. If a receiver with a pending timer hears the retransmission, it cancels its timer and discards the stored packet. The same procedure is followed until the destination is reached. The suppression phase is used to eliminate packet duplications caused by multiple forwarding attempts. Beaconless protocols, including CBF, are embedded with a basic suppression technique, according to which the node with the shortest timeout suppresses all the receivers with a pending timer. A detailed description of the existing suppression techniques is provided in section 4.2.2.

4.2.1.2 Guaranteed Delivery Beaconless Forwarding (GDBF)

GDBF [22] is proposed to guarantee delivery by introducing a scheme for the beaconless recovery mode. GDBF selects the next hop neighbour through the use of RTS (Ready To Send)/ CTS (Clear To Send) mechanism. The RTS packet includes a request message and a field that indicates whether the request is for greedy or recovery mode and is broadcasted to all the one-hop neighbours. In greedy mode, all the nodes receiving of an RTS packet set a timer based on their distance to the destination, which actually means that the closest receiver to the destination has the shortest timeout. A CTS packet is sent back to the source whenever the

timer runs out. If a node with an active timer overhears a CTS packet for the pending request, it automatically cancels its timer. In recovery mode, the timers set by the receivers are based on the receiver's proximity to the sender. The receiver is bound to reply whenever its timer runs out and if none of the other neighbours located within the Gabriel Graph (GG) [26] circle has responded earlier. In case the selected neighbour is not in the GG, the rest of the nodes may protest against the decision by sending 'stop' messages. The sender has then got to change its decision until the protest stops. Transitioning from greedy to recovery mode is supported by GBDF, which is applied when the sender does not receive a CTS response to its RTS.

4.2.1.3 Beaconless Forwarder Planarisation (BFP)

Beaconless Forwarder Planarisation (BFP) is proposed in [23] and [24] to solve the recovery problem that arises in beaconless routing through void[8], while reducing the required message overhead. BFP algorithm consists of the selection and the protest phases. The BFP selection phase is similar to the conventional contention process of the beaconless methods. The sender broadcasts an RTS packet to all its neighbours and waits for a period t_{max}, during which each candidate sets its contention timer using the following function:

$$timer = (d / r).t_{\max} \tag{4.3}$$

Where, d is the distance to the forwarder and r is the transmission range.

Thus, the closest neighbour to the sender maintains the shortest timeout. When the contention timer expires, the candidate transmits a CTS packet back to the sender. If a candidate hears the CTS of another node that lies in its proximity region[9], it cancels its timer. The protest phase comes when the hidden nodes to protest against the nodes violating the timer cancellation condition.

Figure 4-3 illustrates the select and protest phases of the BFP algorithm. Following the RTS packet transmitted by 'S', the nodes responding with a CTS packet are in the following order: N_1, N_2, N_3 and N_6. The timers of hidden nodes N_4 and N_5 are cancelled since they are within the

[8] A void refers to the case when the node holding a packet has no closer neighbour to the destination than the node itself.

[9] It is denoted by the Gabriel circle or the Relative Neighbourhood Graph (RNG) [27] Lune.

proximity region of N_3 and N_2 respectively. The protest phase is initiated after the CTS transmission of N_6 by the nodes N_4 and N_5.

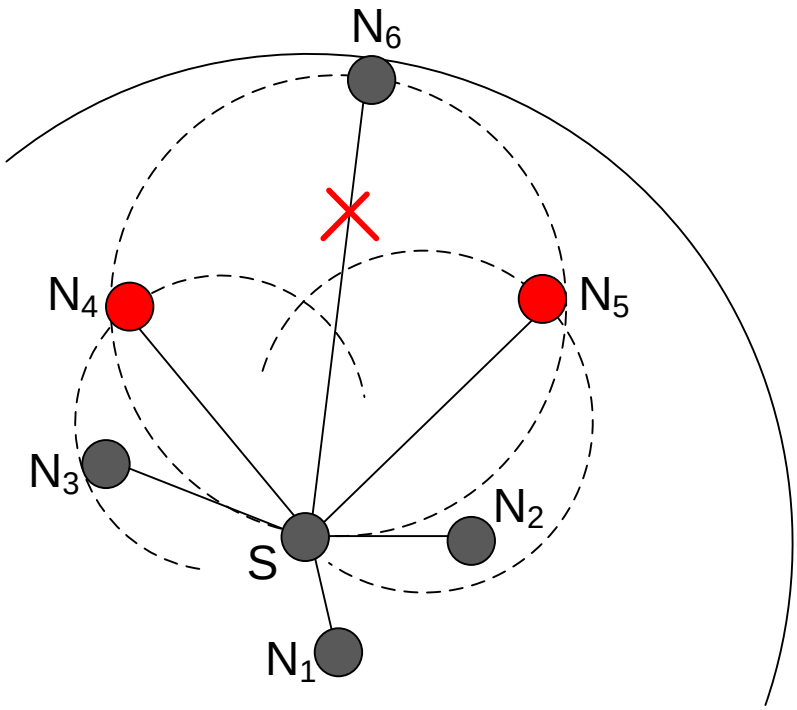

Figure 4- 3: The select and protest mechanism, showing the order of the nodes that respond to S (N_1, N_2, N_3 and N_6) and the protest of the hidden nodes N_4 and N_5 against N_6

4.2.1.4 Pizza Forwarding

Pizza forwarding [25] consists of two forwarding strategies: greedy forwarding and optimized recovery strategy. According tot this, the node's transmission range is portioned into eight sectors of 45^o area, as shown in Figure 4-4. Sectors 1, 2, 3 and 4 are used in greedy mode, while sectors 5 and 6 are used in recovery mode. The main concept of pizza forwarding is similar to that of the CBF's enhanced, by the use of a multiple retransmissions avoidance mechanism.

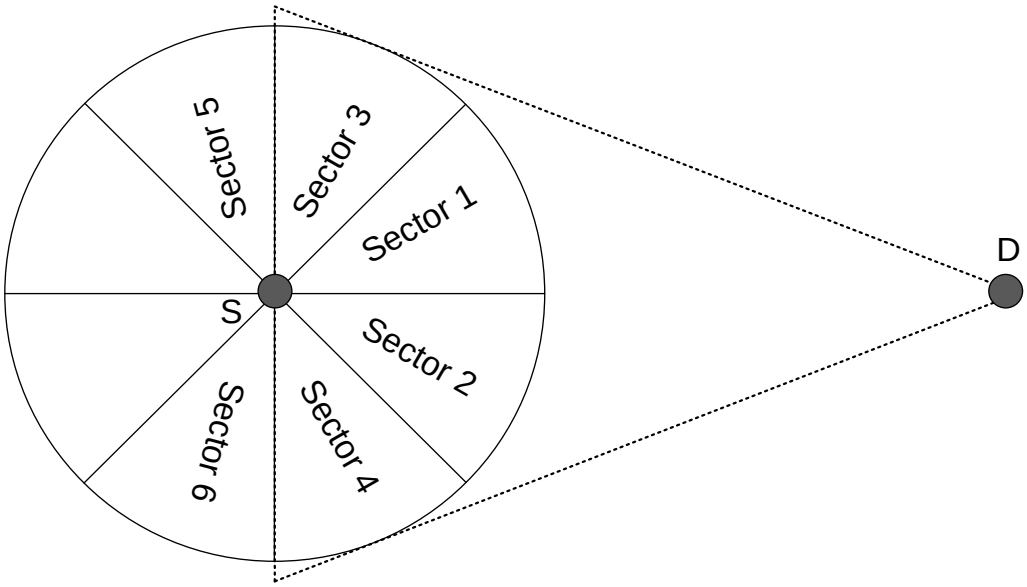

Figure 4- 4: The different sectors used in Pizza forwarding mechanism

In addition, when the packet reaches a local minima or void, the recovery forwarding is applied, according to which the nodes of the recovery area attempt to discover potential candidates in the sender's two hop neighbourhood. The recovery is achieved by sending a SOLICITATION message from each recovery sector. The originator of a SOLICITATION message is called solicitation node. The sender's two-hop neighbours (one-hop neighbours of the solicitation node) compete amongst each other to send a SOLICITATION RESPONSE. Based on the received response messages, the best candidate is selected and sent back to the sender through a SELECTED NEIGHBOUR message.

4.2.2 Suppression techniques

4.2.2.1 Basic suppression

According to the basic suppression scheme [5], the next hop node whose timer expired, re-broadcasts the packet. When another node, whose timer is running, hears the transmission, it cancels its timer and does not forward the packet further. The packet duplication in the basic scheme occurs depending on the density and the location of the neighbouring nodes. The larger the number of nodes within the transmission range of the source, the higher the probability of one or more packet duplications.

4.2.2.2 Area-based suppression

Area-based suppression [5] is proposed in order to avoid the packet duplications from the basic suppression. The scheme proposes to limit the area within the next hop node is selected. Reuleaux triangle[10] is used to divide the radio range of the sending node into three zones as shown in Figure 1. According to the area-based suppression algorithm, the sending node broadcasts the packet. Only nodes contained in the Reuleaux triangle (1) participate in the contention process. That node whose timer runs out first is the next hop to broadcast the packet. All the other nodes within that area will hear the transmission and cancel their timers. If no response or packet retransmission is heard for a maximum response time, the same process is repeated in areas (2) and (3). The order, in which the areas (2) and (3) are selected, is chosen randomly given that no node is located in area (1). Although area-based scheme is an improvement of the basic scheme, it requires three broadcasts for the packet to be successfully forwarded when the worst case scenario is considered, according to which the next hop neighbour is located in area (3). In consequence, this leads to a network load increase, especially when the end-to-end route consists of several hops.

4.2.2.3 Active suppression

Active suppression [5] eliminates packet duplications at the cost of additional control messages. The idea of active suppression is inspired by the Request To Send/Clear To Send (RTS/CTS) concept of CSMA/CA. Accordingly, the sending node broadcasts a Request to Forward (RTF) packet. The RTF packet contains the location of the sending and the final destination nodes. Upon receiving the RTF packet, the receiver sets a reply timer according to the basic suppression scheme. If the timer runs out, a control packet called CTF (Clear To Forward) is transmitted to the sending node, which contains the position of the node sending the CTF. If a node hears a CTF packet, it cancels its own timer and is suppressed. Consequently, the sending node selects the node with the largest progress (if multiple CTFs are received) and transmits the packet using unicast method. Even though active scheme completely eliminates packet

[10] A Reuleaux triangle with a width of r can be constructed by placing three circles with radius r at the corners of an equilateral triangle with an edge length r. The intersection of the circles is the Reuleaux triangle.

duplications, additional delay and overhead are introduced by the exchange of RTF and CTF messages between the sending node and its neighbours.

Finally, the maximum value of the response time 'T', at which the node has to wait before rebroadcasting the packet to zones 2 and 3, is not subject to optimisation in [5] and was assumed to be constant and equal to 45ms. However, optimizing 'T' is highly dependent on the parameters of Media Access Control (MAC) and more specifically on the queuing and contention delay.

4.3 Sender Suppression Algorithm

The distinctive feature of beaconless routing is the elimination of the beaconing effect and its impact on the channel occupancy, energy consumption and network overhead. However, mobile ad-hoc networks are subject to the "Hidden node problem", when two nodes are out of the radio range of each other and attempt to access the wireless channel simultaneously. This impacts the performance of the beaconless routing by introducing packet duplication, meaning that several copies of the same packet are transmitted by the hidden nodes. Therefore, an efficient suppression algorithm is essential in order to improve the routing effectiveness of the beaconless methods.

The current work represents a Sender Suppression Algorithm (SSA) for beaconless routing in mobile ad hoc networks. According to the proposed algorithm, the radio range of the sending node is divided into three forwarding zones, similar to the division proposed in area-based scheme [5], where every zone is constructed based on the concept of the Reuleaux triangle, illustrated in Figure 4-5. The main characteristic of the Reuleaux triangle is that all the nodes within this zone can receive each other's radio signal. Accordingly, when a node broadcasts a packet, all the nodes located within the same Reuleaux triangle zone can hear the transmission, and therefore, suppression is automatically achieved. However, nodes belonging to other Reuleaux triangles may form a hidden node case. Thus, with the advantage of such a partition, we propose the introduction of a time delay to be assigned at every zone, which can turn the timer values uniform within the same zone and multiform amongst the different zones. The

introduced delay is aggregated with the distance function timer to form the total waiting time for the nodes before attempting to forward the packet.

Since the nodes of zone 1 hold the highest priority for forwarding the packets, no delay has been assigned to that zone and the waiting time the node has to defer its transmission consists of the basic timer set according to the contention process. In addition, the delay value of zone 3 should be twice the delay of zone 2, so as to ensure that no simultaneous transmission or packet collision will occur.

Furthermore, we assume a static delay allocation. The highest priority is given to zone 1 as it covers the largest geographical area, and therefore, the probability of a node being in this zone is higher. As for as zone 2 and zone 3 are concerned, zone 2 is assumed to have higher priority and, therefore, the largest zone delay is allocated to zone 3. However, additional work could take place on this, in order to optimise the delay distribution process by designing a dynamic allocation scheme that would introduce the lowest delay to the most appropriate zone, while considering several traffic history parameters formed by the data and control traffic.

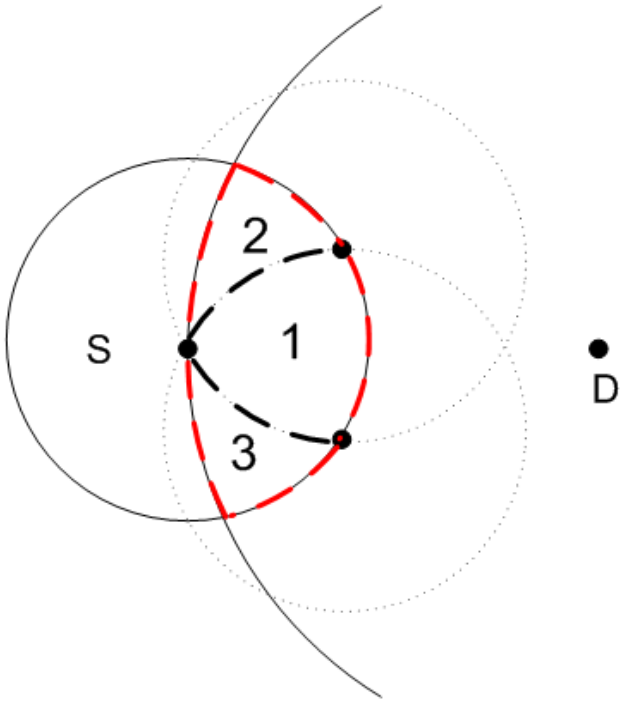

Figure 4- 5: The three Reuleaux triangles of the forwarding area

As proposed in [5], the timer set by a node N_i is based on its progress to the destination and is defined as follows:

$$timer = T * (1 - (dist(S, D) - dist(N_i, D)/R)) \quad (4.4)$$

Where dist(S, D) is the distance from the source to the destination, dist(N_i, D) is the distance from the node N_i to the destination, R is the transmission range and T is the maximum forwarding delay.

Moreover, the delay introduced in the different zones is defined as follows:

$$delay_{zone_1} = 0 \quad (4.5)$$

$$delay_{zone_2} = \partial \quad (4.6)$$

$$delay_{zone_3} = 2 * \partial \quad (4.7)$$

Therefore, the total time delay that a node N_i must wait prior attempting to forward the packet is given by the following equations:

$$N_i \in zone_1 \Rightarrow \quad delay_{N_i} = timer_{N_i} \quad (4.8)$$

$$N_i \in zone_2 \Rightarrow \quad delay_{N_i} = timer_{N_i} + \partial \quad (4.9)$$

$$N_i \in zone_3 \Rightarrow \quad delay_{N_i} = timer_{N_i} + 2 * \partial \quad (4.10)$$

Where ∂ is a delay unit.

To avoid the possibility of a simultaneous access to the channel by nodes of different zones, the delay unit must be greater than a minimum value given by:

$$\partial_{\min} = \max(timer) + TxRx(data) \quad (4.11)$$

The retransmission of the data packet occurring when the timer runs out is detected by the previous sender, which proceeds to suppress the other nodes by broadcasting an Announcement (Acm) packet. The announcement packet contains the address of the new forwarder in addition to its location information as shown in Figure 4-6.

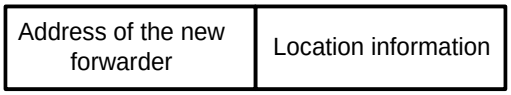

Figure 4- 6: The format of the announcement packet (Acm)

The main operations of the sender suppression algorithm are described as follows:

1. The sending node broadcasts the packet.
2. All the receivers of the packet set a timer according to their progress to the destination as well as to the zone they belong.
3. The node that responds first will forward the packet.
4. Any other node that hears the re-broadcast cancels its timer.
5. Once the sending node hears the re-broadcast of the packet, it will send an announcement packet to all the other nodes that are out of range of the new forwarder.

The main advantage of the proposed scheme is that the suppression is obtained at the cost of low overhead. This additional overhead can be further minimized if the next hop node responding to the transmission remains the forwarding node for a longer period of time, in which case, the sender broadcasts announcement packets its neighbours less frequently reducing, therefore, the number of the suppression packets. In consequence, only one announcement packet is required during that specified time interval.

A general comparison between the area-based, the active selection and the proposed sender suppression algorithm is provided in Table 4-1.

Table 5- 1: A comparison of the different suppression schemes

		Area-based	Active selection	SSA
Number of data transmissions	Zone 1	1	1	1
	Zone 2	2	1	1
	Zone 3	3	1	1
Control messages		No	Yes (RTF/CTF)	Yes (Acm)
Time required for the data packet to be forwarded to the next hop	Zone 1	$Timer_i$	$Timer_i$ + RxTx(RTF) + RxTx(CTF)	$Timer_i$
	Zone 2	$Timer_i$ +T + RxTx(DATA) +	$Timer_i$ + RxTx(RTF) + RxTx(CTF)	$Timer_i$ + Δ
	Zone 3	$Timer_i$ + 2* T + 2*RxTx(DATA)	$Timer_i$ + RxTx(RTF) + RxTx(CTF)	$Timer_i$ + 2*Δ
Overhead		Data	RTF/CTF packets	Acm packet
Data transmission mode		Broadcast	Unicast	Broadcast

$Timer_i$ refers to the timer set by the receiving node that turns to be the forwarder to the next hop. T is the response time that the sending node waits before re-broadcasting the packet.

4.4 Results Analysis

4.4.1 Simulation environment

The proposed Sender Suppression Algorithm (SSA) has been modeled and implemented in OPNET network modeler, version 14.5. In this version of OPNET, a complete implementation of the IEEE 802.11 radio and MAC specifications is available. To evaluate the performance of SSA, a beaconless routing method is needed. We have implemented the Contention-Based Forwarding (CBF) proposed in [5] with the Area-based suppression scheme, referred to as AS-CBF, with which a comparison took place. The complete models of SSA and AS-CBF are provided in Appendix A.

The evaluation has been carried out using two scenarios that cover the possible cases, where the next hop forwarding nodes are located in the second and third Reuleaux triangles, respectively. The simulation environment consists of one pair of wireless stations, communicating through a multi-hop connection formed by a set of intermediate nodes. An instance of one of the scenarios configured is given in Figure 4-3, which illustrates the case

where the forwarding nodes are always located in the third forwarding zone (Reuleaux triangle).

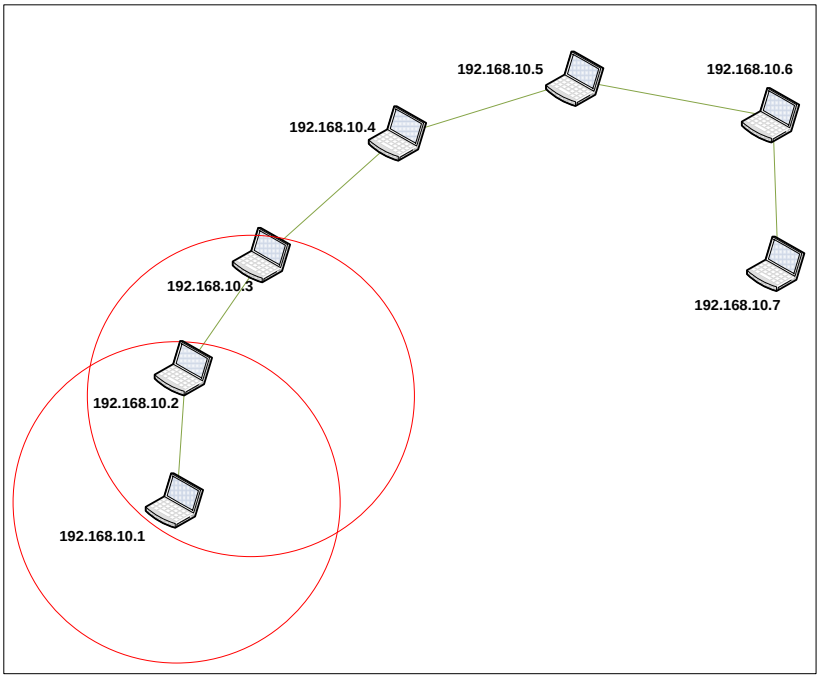

Figure 4- 7: Simulation scenario 1, illustrating the case where the forwarding nodes are always located in the second Reuleaux triangle of the forwarding area.

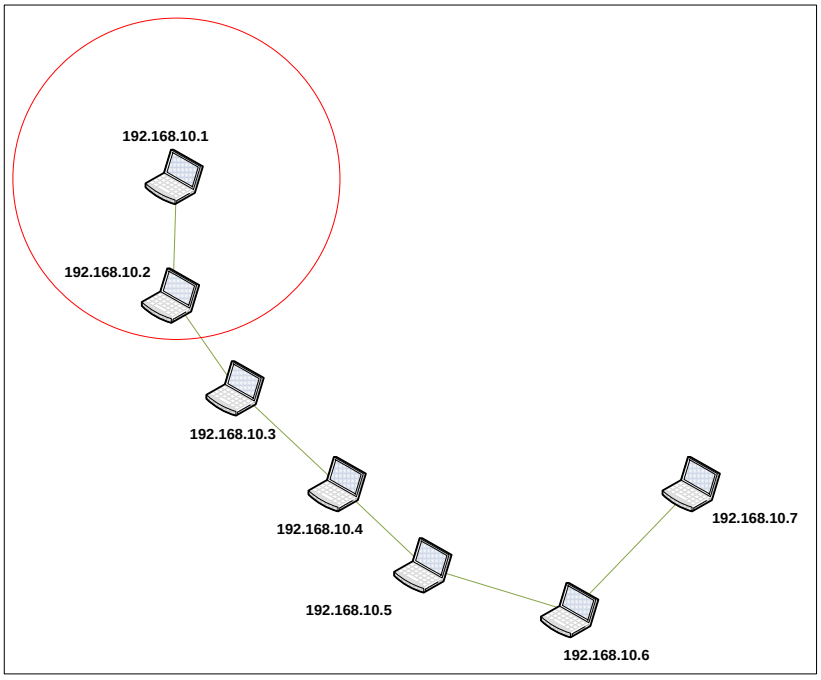

Figure 4- 8: Simulation scenario 2, illustrating the worst case where the forwarding nodes are located in the third Reuleaux triangle of the forwarding area.

The IP addressing scheme is IPv4 and the physical layer is configured to be conformant with the IEEE 802.11g (Extended rate). The number of hops between the source and the destination varies from two to six and the simulation runs for 300s. Table 4-2 presents the simulation parameters configured.

Table 5- 2: Simulation parameters

Network Simulator	**OPNET™ Modeler**	
Radio Range	97*m*	
IP addressing scheme	IPv4	
MAC protocol	IEEE 802.11 g	
Data rate	24 Mbps	
Data traffic	Packet inter-arrival time	1 s
	Packet size	1024 bits
Simulation time	300s	
SSA zone delay 'Δ'	0.0005s	

The evaluation is performed based on the following metrics:

- ***The average network overhead***: it includes the control messages used by the algorithm to perform the suppression, as well as the redundant copies of the data packets transmitted.
- ***The average effective throughput:*** is the ratio of the data traffic received in (bits/sec) by the final destination to the data traffic sent in (bit/sec) by the source and the intermediate nodes.

4.4.1.1 Simulation Scenario 1

In this scenario, the forwarding nodes of the data packet are located in the second zone of the forwarding area. According to the area-based suppression scheme, one redundant data transmission is required at every hop to achieve the suppression, in comparison to one announcement packet per hop by the sender suppression algorithm. Therefore, for every data transmission, one additional packet transmission is required at every hop, leading to the same overhead in terms of packets, as illustrated in the graph of Figure 4-6.

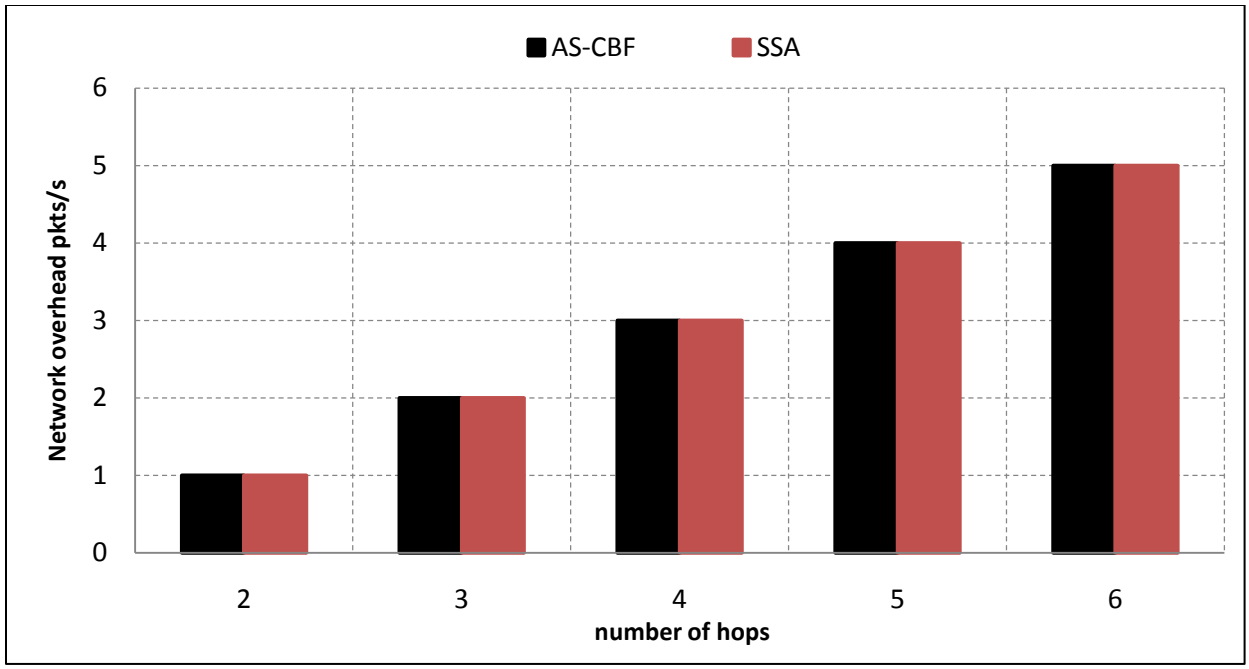

Figure 4- 9: The network overhead in Packets/s of AS=CBF and SSA for different number of hops considering the network scenario 1

However, the size of the additional packet differs in both schemes. For area-based scheme, the transmitted packet consists of the actual data that may have a variable size. Whereas, SSA employs a fixed size announcement packet, which is considerably smaller as compared to the data packet. Figure 4-7 shows the overhead in bits/s introduced by both suppression schemes for a small size data packet (1024 bits). As clearly shown, SSA maintains a low overhead, which consists of the announcement packet (248 bits), as compared to AS-CBF scheme.

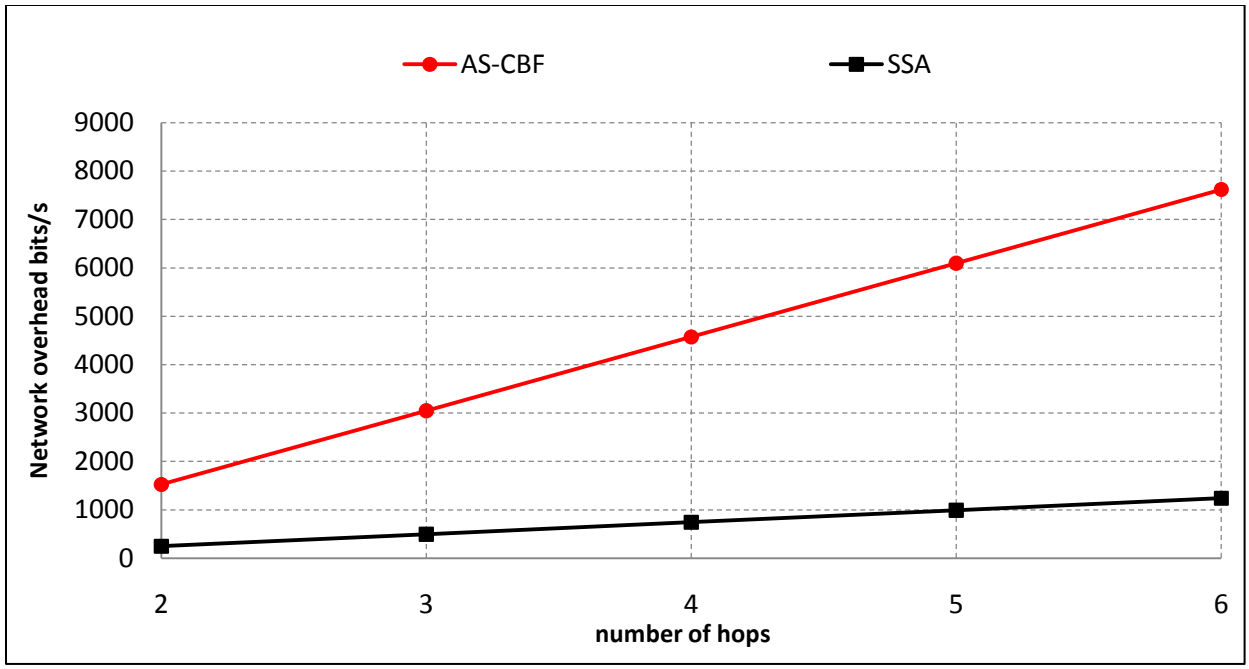

Figure 4- 10: The network overhead in bits/s of AS-CBF and SSA considering network scenario 1

Figure 4-8 presents the effective throughput of the compared schemes. SSA shows higher throughput since one data packet is transmitted at every hop. In contrast, AS-CBF scheme requires two transmissions that lead to an increase in the overall traffic generated by the source and the intermediate nodes.

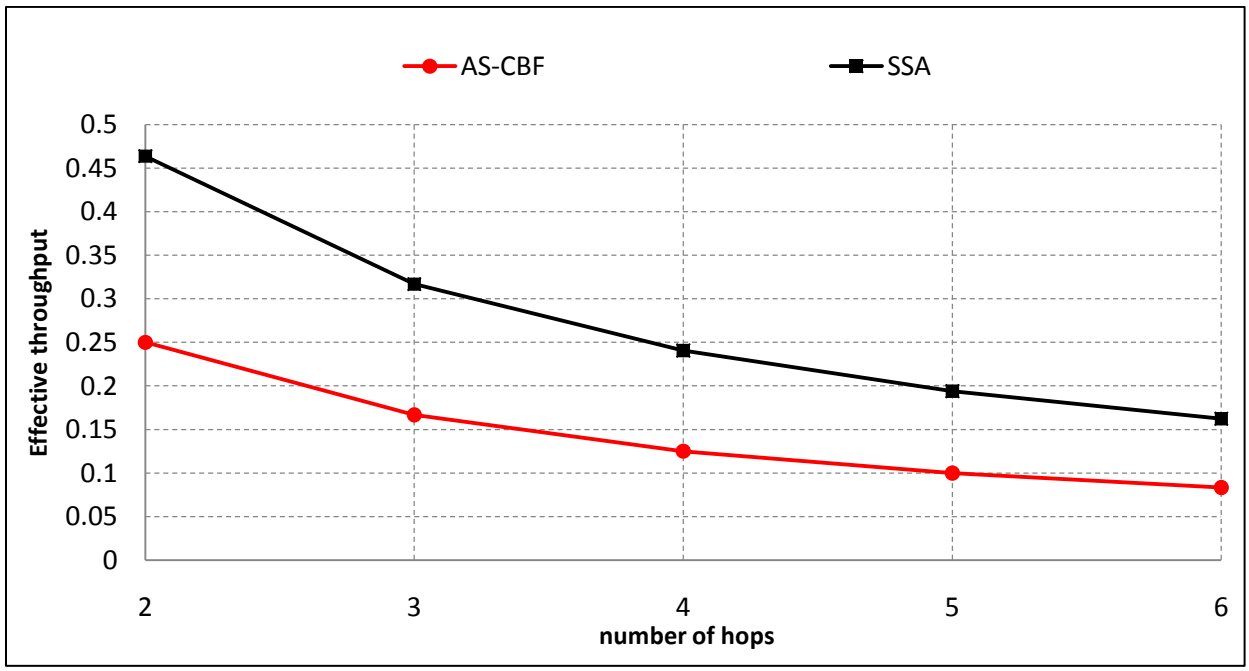

Figure 4- 11: The effective throughput of AS-CBF and SSA considering network scenario 1

4.4.1.2 Simulation Scenario 2

This scenario represents the case, where the nodes forwarding the packet to the destination are located in the third zone of the forwarding area. Accordingly, the area-based suppression scheme will require to broadcast the data packet three times at each hop to be successfully relayed. Figure 4-9 shows the cost of suppression in packets per seconds of the area-based (AS-CBF) and Sender Suppression Algorithm (SSA) schemes. AS-CBF transmits multiple copies of the data in order to isolate the nodes located at different zones (Reuleaux triangles) and, therefore, two redundant packets is the cost of a successful transmission[11]. Whereas, SSA relies on the announcement packet to ensure that one retransmission is taking place, regardless the location of the next forwarding node. From a bandwidth's point of view, the bandwidth required for data transmission is much higher than that needed to transmit an announcement packet, given that is considerably smaller in size than the data packet.

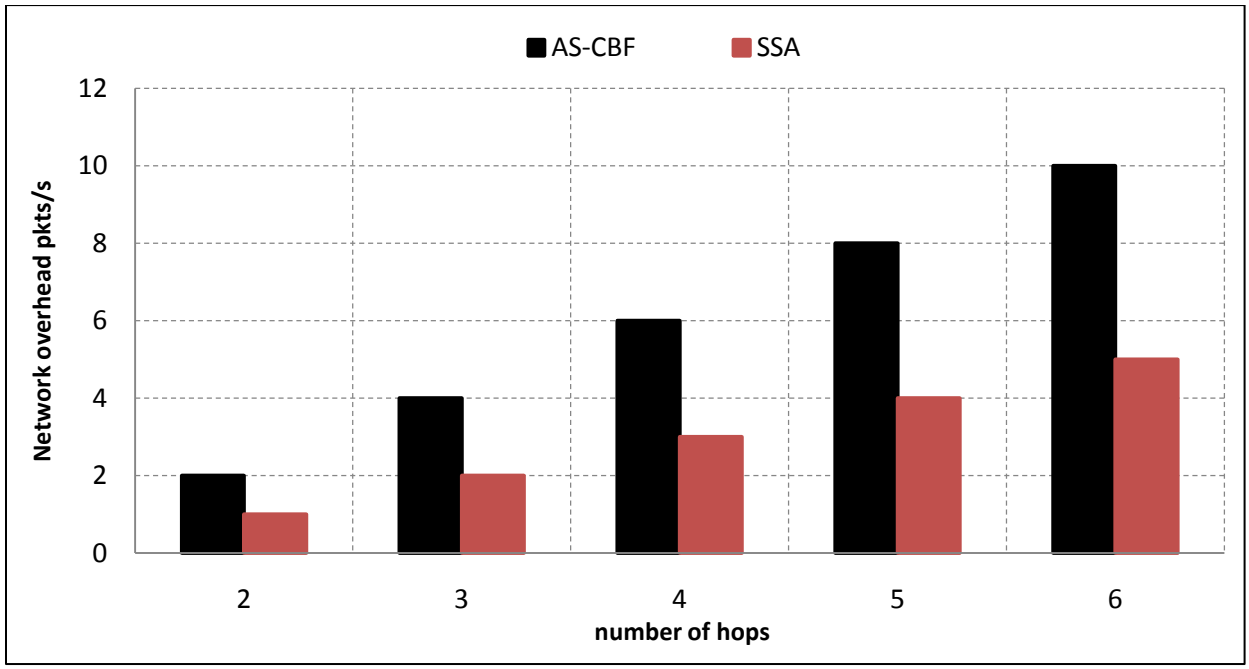

Figure 4- 12: The network overhead in packets/s of AS-CBF and SSA for different number of hops considering the network scenario 2

[11] A transmission is referred to as successful when the transmitted data packet is relayed to the next hop.

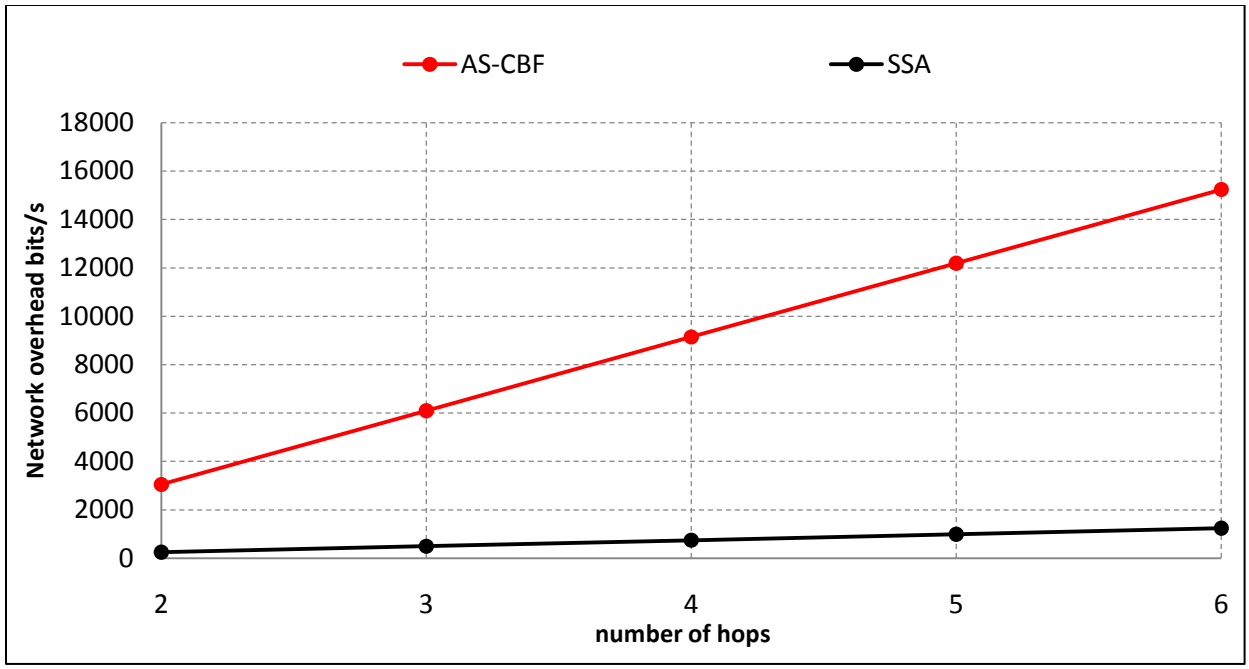

Figure 4- 13: The network overhead in bits/s of AS-CBF and SSA considering network scenario 2

Additionally, the overhead in packets per second may be insufficient to illustrate the actual difference amongst the compared suppression schemes. Figure 4-10 depicts the network overhead of AS-CBF and SSA schemes in bits per second also clearly demonstrated the high overhead maintained by AS-CBF due to the packet size, although a small data packet size is considered (1024 bits).

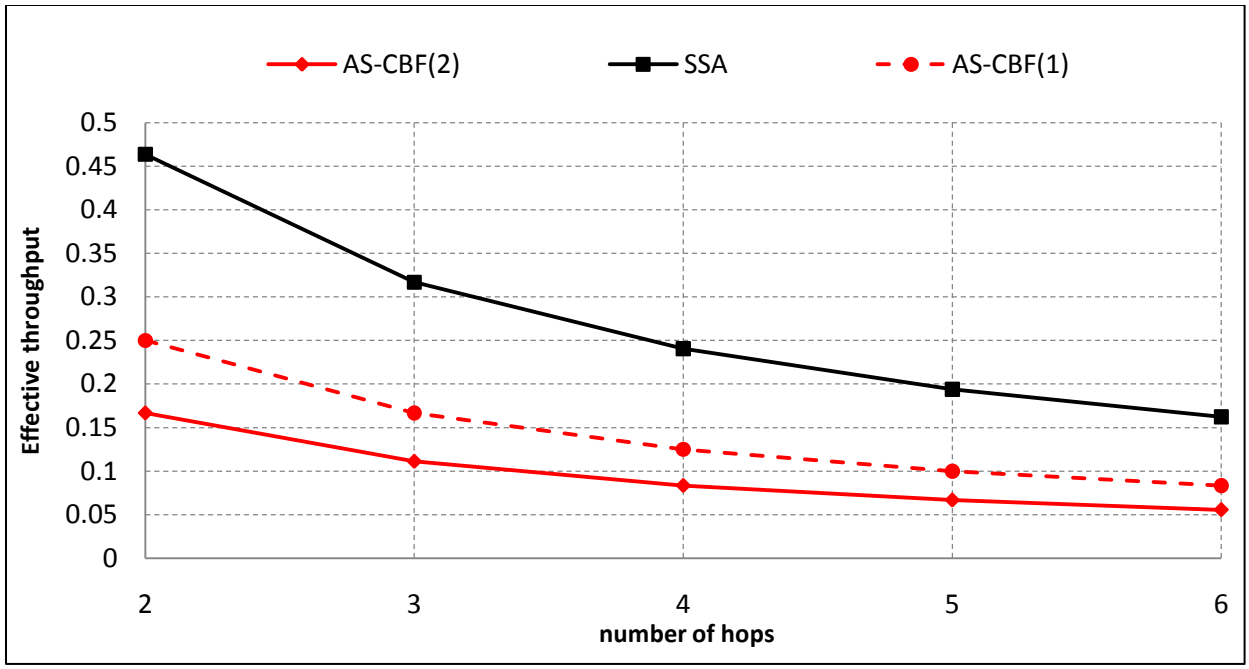

Figure 4- 14: The effective throughput of AS-CBF and SSA considering network scenarios 1 and 2

Figure 4-11 illustrates the effective throughput of the compared suppression schemes in scenarios 1 and 2. While the network overhead of AS-CBF increases, the effective throughput decreases and the SSA throughput remains constant.

4.5 Conclusion

This chapter reviewed the beaconless routing schemes and the mechanism employed to eliminate the packet duplication problem caused by the hidden nodes during the contention process. Sender Suppression Algorithm was then presented and showed to achieve nodes' suppression at low cost. According to SSA, the radio range of the sending node was divided into four zones, with a predefined time delay assigned to each one. The predefined zone delay was added to the contention timer, set by the receiver, to form the total time that it has to wait before responding to the sender's transmission. In addition, SSA involved the sending node in the suppression process, which broadcasted an announcement packet to all its neighbours after hearing the first retransmission. Consequently, all the receivers with active timers that received the announcement packet had to cancel the scheduled transmission. The proposed scheme was integrated with the Contention-Based Forwarding (CBF) and compared to the Area-

based suppression technique. The simulation results demonstrated considerable improvement in terms of network effective throughput.

References

[1] M. Witt and V. Turau, "The Impact of Location Errors on Geographic Routing in Sensor Networks," ICWMC '06, Bucharest, Romania, p. 76, July 2006.

[2] H. Fubler, J. Widmer, M. Kasemann, M. Mauve, and H. Hartenstein, "Contention-based forwarding for mobile ad-hoc networks". Elsevier's Ad-Hoc Networks, Vol. 1, No. 4, pp. 351–369, 2003.

[3] H. Füßler, H. Hartenstein, J. Widmer, M. Mauve and W. Effelsberg, "Contention-based forwarding for street scenarios", 1st International Workshop in Intelligent Transportation (WIT 2004), Hamburg, Gemany, March 2004.

[4] A. Ho, Y. Ho and K. Hua, "A connectionless approach to mobile ad hoc networks in street environments", IEEE IV 2005, Las Vegas, USA, June 2005.

[5] T. Li, Y. Li, J. Liao. "A Contention-Based Routing Protocol for Vehicular Ad Hoc Networks in City Environments", 29th IEEE International Conference on Distributed Computing Systems Workshops (ICDCSW), pp. 482 – 487, 2009.

[6] Pedro M. Ruiz, Victor Cabrera, Juan A. Martinez, Francisco J. Ros, "BRAVE: Beacon-less routing algorithm for vehicular environments", 7th IEEE International Conference on Mobile Adhoc and Sensor Systems (MASS), pp 709 – 714, 2010 .

[7] J. Sanchez, P. Ruiz, and R. Marin-Perez, "Beacon-less geographic routing made partical: Challenges, design guidelines and protocols," IEEE Commun. Mag., vol. 47, no. 8, pp. 85–91, Aug. 2009.

[8] M. Heissenbuttel and T. Braun, "BLR: beacon-less routing algorithm for mobile ad hoc networks", Computer Communications, Vol. 27, No 11, pp. 1076–1086, 2004.

[9] B. Blum, T. He, S. Son, J. Stankovic "IGF: A state-free robust communication protocol for wireless sensor networks". Tech. Rep., Department of Computer Science, University of Virginia, USA, 2003.

[10] N. Meghanathan, “A Beaconless Node Velocity-based Stable Path Routing Protocol for Mobile Ad hoc Networks”, Proceedings of the IEEE Sarnoff Symposium Conference, pp. 1-5, 2009.

[11] C. Dazhi, D. Jing, and P.K. Varshney, “A state-free data delivery protocol for multihop wireless sensor networks”. IEEE Wireless Communications & Networking Conferenc, Vol. 3, pp. 1818- 1823, 2005.

[12] Zorzi M, Rao R. Geographic random forwarding (GeRaF) for ad hoc and sensor networks: Energy and latency performance. IEEE Transactions on Mobile Computing, Vol. 2, No 4, pp. 349-365, 2003.

[13] F.A. Tobagi and L. Kleinrock, “Packet Switching in Radio Channels. II: The Hidden Terminal Problem in Carrier Sense Multiple-Access and the Busy-Tone Solution,” IEEE Transactions on Communications, vol. 23, pp. 1417-1433, Dec. 1975.

[14] M. Witt, V. Turau, “BGR: Blind geographic routing for sensor networks”. Workshop on Intelligent Solutions in Embedded Systems (WISES05), Hamburg, Germany, pp. 51-61, 2005.

[15] J.A. S´anchez, R. Mar´ın-P´ere, and P.M. Ruiz, “BOSS: Beacon-less On Demand Strategy for Geographic Routing in Wireless Sensor Networks”, IEEE MASS, pp. 1-10, 2007.

[16] Chao Huang and Guoli Wang, “Contention-Based Beaconless Real-Time Routing Protocol for Wireless Sensor Networks”, Wireless Sensor Network, Vol. 2 No. 7, pp. 528-537, 2010.

[17] C. Dazhi and P.K. Varshney, “On-demand Geographic Forwarding for data delivery in wireless sensor networks”. Elsevier Computer Communications Vol. 30 No. 14-15 pp. 2954-2967, 2007.

[18] Y. Xu, W-C. Lee, J. Xu, and G. Mitchell, “PSGR: priority-based stateless geo-routing in wireless sensor networks”, IEEE International Conference on Mobile Adhoc and Sensor Systems, pp. 680-687, 2005.

[19] G. Chen, K. Itoh, T. Sato, “Beaconless Location-Based Routing with Signal Strength Assisted for Ad-Hoc Network”. IEEE Vehicular Technology Conference (VTC), pp. 86 - 90 , Oct. 2007.

[20] Xuan Shi and Kai Liu, “A Contention-Based Beaconless Geographic Routing Protocol for Mobile Ad Hoc Networks”, Third International Conference on Communications and Networking (ChinaCom), pp. 840 – 843, 2008.

[21] Haibo Zhang and Hong Shen, “Energy-Efficient Beaconless Geographic Routing in Wireless Sensor Networks”, IEEE Transactions on Parallel and Distributed Systems, Vol. 21, No. 6, pp. 881 – 896, 2010.

[22] M. Chawla, N. Goel, K. Kalaichelvan, A. Nayak, and I. Stojmenovic, “Beaconless position-based routing with guaranteed delivery for wireless ad hoc and sensor networks,” Acta Autom. Sin., Vol. 32, No. 6, pp. 847–855, Nov. 2006.

[23] H. Kalosha, A. Nayak, S. Rührup, and I. Stojmenovic, “Select-and-protest-based beaconless georouting with guaranteed delivery in wireless sensor networks,” IEEE INFOCOM, pp. 346–350, 2008.

[24] S. Rührup, H. Kalosha, A. Nayak and I. Stojmenovic, “Message-Efficient Beaconless Georouting With Guaranteed Delivery in Wireless Sensor, Ad Hoc, and Actuator Networks”, IEEE/ACM Trans. On Networking, Vol. 18, No. 1, pp. 95 – 108, 2010.

[25] I. Amadou, F. Valois, “Pizza Forwarding: A Beaconless Routing Protocol Designed for Realistic Radio Assumptions”, Fourth International Conference on Sensor Technologies and Applications, pp. 495 – 500, 2010.

[26] R. Gabriel and R. R. Sokal, “A new statistical approach to geographic variation analysis,” Syst. Zool., Vol. 18, No. 3, pp. 259–278, 1969.

[27] W. Jaromczyk and G. T. Toussaint, “Relative neighborhood graphs and their relatives,” Proc. IEEE, Vol. 80, No. 9, pp. 1502–1517, 1992.

Chapter 5

Link Lifetime Estimation Method for Greedy Forwarding

5.1 Introduction

The IEEE Mobile Ad-hoc Networks (MANETs) have undergone intensive research attention during the last decade from the academic and the industrial sectors. A MANET consists of mobile hosts spread across a geographical area, connected to each other via wireless links lacking any sort of infrastructure. Moreover, a lot of work has been carried out across all Open Systems Interconnection (OSI) layers from the application to the Medium Access Control (MAC) and the network layer in particular, for which numerous routing algorithms have been proposed to provide end-to-end routes that are reliable and robust against nodes mobility.

Position-based routing protocols for MANETs rely on the knowledge of the nodes' geographical position to forward a packet to the destination. According to some of the existing position-based schemes, the source node establishes an end-to-end route to the final destination, whereas some others apply hop-by-hop routing strategy, in which the main focus lies on selecting the next node to relay the packet. Greedy forwarding (GF) [1], [2], [3] and [4] schemes are examples of the hop-by-hop routing schemes, where the location information of the destination is assumed to be known by the source node in advance. Greedy methods select the next hop node that satisfies specific criteria such as progress, distance and angle. Therefore, the nodes participating in the packet forwarding process are those located in the area that confronts the destination, called progress area. Furthermore, the nodes' mobility is one of the

main characteristics of MANETS that leads to frequent topology changes and to a subsequent increase in the probability of link failures and routes breakage. Consequently, link failures initiate a route maintenance process, which tries to either find alternative links or discover a new route. Such a process wastes bandwidth and battery lifetime resources, and affects the network's performance by introducing additional routing overhead and re-routing delay.

In order to reduce the effect of link failure on the network service and its impact on the routing performance, link and route stability metrics have been introduced at the routing operation by various protocols for selecting the most appropriate route and the next hope relaying node. The route stability constitutes a main challenge for MANETs that help to support real time traffic and multimedia applications, which depends on the stability of the radio links that compose the route. The stability of a link is related to the period of time for which the link is considered available. Several methods have been proposed to estimate the stability or the lifetime of a link. Some of these methods rely on the received signal strength, while some other uses the nodes position information to predict the availability.

The method proposed in [6] estimates the lifetime of a link based on the position, speed and direction of the nodes composing the link. In addition, it represents the time that those nodes remain within the transmission range of each other. However, for greedy forwarding schemes, the link lifetime is practically represented by the time a neighbouring node remains in the progress area of the source node. Therefore, the estimation that is obtained using the conventional method, proposed in [6], does not reflect the precise value that a link is considered available. Given that, the selection process for greedy forwarding schemes is restricted to the nodes within the progress area.

It is important, for the estimation method, to accurately estimate the lifetime of the links between the source node and its neighbours. In this chapter, we propose a novel method to estimate the link lifetime between two nodes for greedy routing schemes. The method considers in addition to the position, the direction and the speed of the nodes forming the link, those of the destination. This assures that the link is considered to be available as long as the receiver is within the progress area of the sender. A Stability-Aware Greedy (SAG) routing is also

introduced, which is employed to evaluate the conventional and the proposed link lifetime estimation methods. SAG' next hop selection criterion is based on a link lifetime metric, according to which the neighbour that maximises the link lifetime with the sender is selected as the next hop relaying node.

The chapter is organized as follows: Section 5.2 presents an overview of the existing link lifetime estimation methods and the stability-based routing protocols in Mobile Ad-hoc Networks. The proposed link lifetime estimation method is presented in section 5.3. Section 5.4 describes the functionality of the stability-based greedy forwarding scheme. The performance analysis and the simulation results are given in section 5.5 and eventually, section 5.6 concludes the chapter.

5.2 Related work

There are several existing methods for link lifetime estimation in MANETs. Some of these methods rely on the received signal's strength, while others use the nodes' position information to predict the link availability. In [7], a method is proposed to predict the Link Available Time using the received signal's strength changing rate. There also exist different approaches that predict the lifetime of a path based on mobility models, [8] being an example. A prediction-based link availability estimation method to quantify the link reliability is introduced in [9]. The basic idea is to predict a continuous time period (Tp) starting from t_0, during which a link is available. The probability of the link remaining available for the duration t_0+Tp is then estimated, considering the possible changes in the mobility speed and direction. In [10] and [11], a probabilistic model measuring the availability of a path being subject to link failure due to mobility, is proposed. Accordingly to those methods, the link availability is defined as the probability that a wireless link between two mobile nodes exists at time t_0+ t, given that a link exists between them at time t_0. In addition, the path selection procedure is based on the probability that the path remains available over a specified interval of time. Moreover, a method to predict the link and the route lifetime based on the nodes' location and movement information has been proposed in [6]. It relies on information about the position,

the speed and the mobility direction of the nodes forming the link that is used to estimate the time the nodes remain within the radio range of each other.

Link and route stability have been integrated to the routing protocols to increase the routing efficiency and reduce the effect of links breakage on the protocol performance. Various stability protocols have been proposed and can be classified based on the method used to measure the link stability. Those routing protocols that measure the link stability based on the received signal's strength are proposed in [12], [13], [14] and [15]. In Associativity-Based Routing (ABR) [12], the wireless links are classified into stable and unstable links, based on accumulated information at the receiving nodes collected through beacon messages. Signal Stability-based Adaptive (SSA) routing [13] is a reactive routing protocol that discovers routes on demand. It uses the signal strength and location stability to select routes with long lifetime to the destination. SSA makes a distinction between strong and weak channels based on the average signal strength at which packets are being exchanged among the hosts. Route-Lifetime Assessment Based Routing (RABR) protocol [14] estimates the residual route lifetime based on an affinity appraisal. It predicts a change in the topology on the basis of signal strength information.

Besides, the protocols that measure the stability using the nodes mobility information are proposed in [15], [16], [17], [18], [19] and [20]. Link Lifetime-Based Segment-by-Segment Routing protocol (LL-SSR) is proposed in [15], where each node maintains a routing table for its k-hop region. Its basic idea is the selection of a stable route, segment by segment, to reduce the routing overhead. The work in [16] introduces three schemes that use mobility information to establish and maintain robust and stable routes to the destination. The concept of using the stability of the links to enhance the hop count routing is studied in [18]. In [19] a stability enhanced routing is proposed, which uses a Link Expiration Time (LET) parameter to establish a stable route.

Moreover, Power Boosting Geographic Routing with link lifetime estimation (PBGR) [20] and Greedy Perimeter Stateless Routing with Lifetime (GPSR-L) [21] are both greedy routing schemes that consider link lifetime in the selection of the next forwarding node. PBGR

proposed in [20] uses two metrics – the distance to the destination and the link lifetime – as next node selection criteria. The closest node to the destination that has a link lifetime longer than a defined link lifetime threshold is selected as the forwarding node. GPSR-L [21] is a variant of the Greedy Perimeter Stateless Routing (GPSR) [21] protocol, while integrating the concept of link lifetime to the routing process. According to GPSR-L, the node holding the packet calculates the lifetime of the link with each of its neighbours, after which a timer is set to obtained value. The timer is introduced to determine the quality of the link. As a result, the closest neighbour to the destination with and non-zero lifetime timer, is selected as the next forwarder of the packet. Link Lifetime-based Backup Routing (LBR) is proposed in [22] with the aim of improve routing stability. LBR determines the shortest path between the source and the destination through a route discovery process, during which local backup paths are determined for each link in the primary route. The local backup paths will be used in case the primary route fails.

Modified versions of the Ad-hoc On Demand distance Vector protocol (AODV) that use the link/route stability estimation in the routing process are presented in [23], [24] and [25]. In [23], a stability estimation method is proposed and link/route stability is applied to an optimized version of AODV protocol to decrease the overhead of the route discovery and route maintenance mechanisms. In the case of link failure, the source node, aware of the stability of the discovered routes, selects another stable route to the destination. Link Stability Based AODV (LSB_AODV) is proposed in [25]. It uses the link stability factor as well as the route stability factor to improve the route selection process, which is based on route stability and hop count. Moreover, LSB_AODV divides the node's transmission range into stable zone and caution zone and initiates the rerouting mechanism when the distance between two neighbouring nodes exceeds the stable zone.

5.3 Proposed link lifetime estimation method

In greedy forwarding, nodes located in the progress area[12], illustrated in Figure 5-1, participate in the selection process, only, since nodes of the other area have lower progress to the destination than the sending node. Generally, lifetime of a link L_{ij} is defined by the time duration the two nodes N_i and N_j remain connected. However, in greedy forwarding schemes, the link should only be available when node N_j remains in the progress area of node N_i, assuming N_i is the sending node. Therefore, two incidents affect the availability of the link: the point at which the neighbouring node moves out of the transmission range of the sending node and when the neighbouring and the sending nodes become equidistant from the destination. Thus, the link lifetime is a function of the position, speed and direction of the sending, the neighbouring as well as the destination nodes.

Considering the case illustrated in Figure 5-1, the link lifetime of neighbouring node A is the time dt required to cover the distance AH. Whereas, in greedy forwarding it is the time required to cover the distance AK, being significantly smaller than dt.

Assuming that (x_S, y_S) are the coordinates of a source node S, and (x_A, y_A) are those of its neighbouring node A and (x_D, y_D) those of the destination node D. We also assume that v_A, θ_A, v_s, θ_S and v_D, θ_D are the speed and the direction of nodes A, S and D respectively. We consider the nodes' speed as constant.

Therefore, the lifetime of the link SA is defined as the duration at which the distance between S and A remains smaller than S's transmission range, and the same time the distance between A and D remains smaller than the distance between S and D.

[12] The progress area is the intersection of circles (C) and (C_1). (C) is the circle of centre the source node and the radius is the transmission range, while (C_1) is the circle of centre the destination node and the radius is the distance from source to the destination.

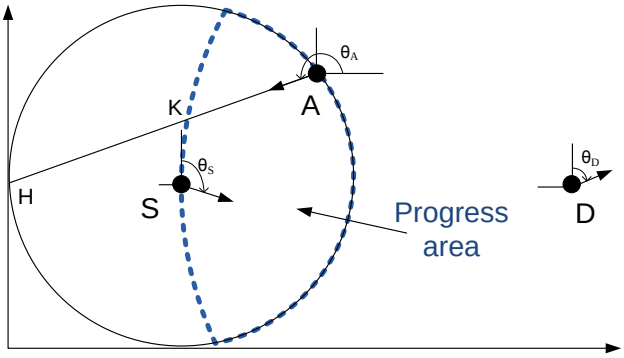

Figure 5- 1: The progress area of node S in respect to the destination D

According to [6], the time the two nodes S and A stay connected, meaning the distance SA is smaller than the transmission range, can be estimated and derived by the following equation:

(5-1)

where r is the transmission range and:

On the other side, the time the distance between the sending node S and the destination node D remains greater than the distance between the neighbouring node A and the destination D is given by:

Assuming that (x_S^*, y_S^*), (x_A^*, y_A^*) and (x_D^*, y_D^*) are the coordinates of nodes S, A and D at the time D is equidistant to S and A, the following equation is derived:

Hence,

Since the distance between two points $S(x_S, y_S)$, and $D(x_D, y_D)$ is given by:

Therefore,

(5-2)

(5-3)

(5-4)

(5-5)

(5-6)

Hence by defining:

we have:

(5-3)
(5-4)
(5-5)
(5-6)

Substituting (5-3), (5-4), (5-5) and (5-6) in the equation (5-2), we obtain the following equation:

(5-7)

The solution of the above equation is given by:

(5-8)

One value of *t* is only used, which is the smallest among the two available solutions.

Accordingly, the time that a neighbouring node A remains in the progress area of a sending node S is the minimum time that the node A needs to reach the edge of the radio range of S, and the time S becomes equidistant to D.

Eventually, the link lifetime Γ is defined as follows:

$$\Gamma = \text{Min}\,(t^*, t). \tag{5-9}$$

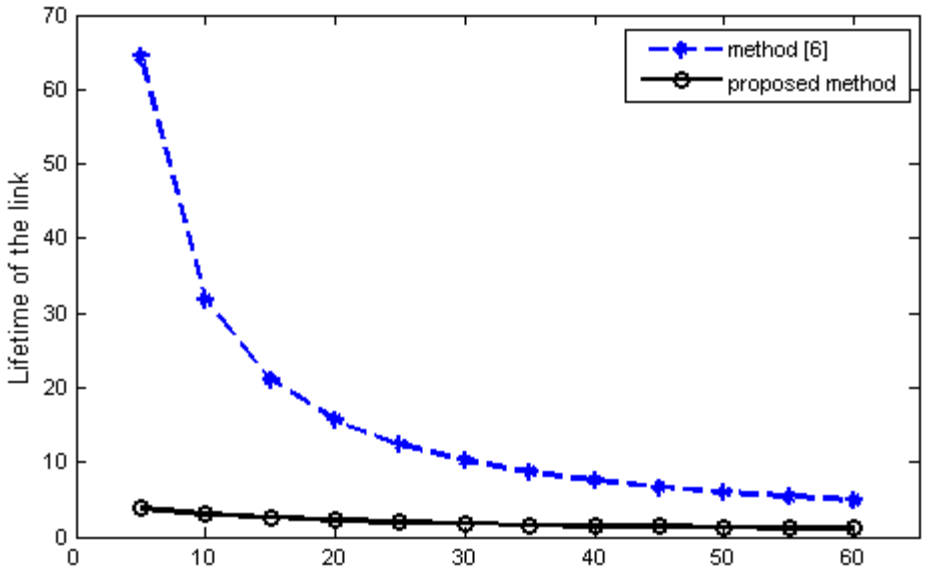

Figure 5- 2: The relation between the mobility direction ($\Delta\theta = \theta - \theta_s$) and the lifetime of the link of two nodes; vs = va=10, xs=ys=10, xa=ya=20, xd=yd=10, θd=0 and R=50

Figure 5-2 depicts the relation between the link lifetime 'Γ' and the difference in the movement Δθ direction of the two nodes forming the link. As it is clearly shown, the link breakages increase while the difference between the movement directions of the nodes, forming the link, increases. Besides, the lifetime of the link estimated using the conventional method [6] is considerably longer when it is estimated by the proposed method.

A longer link lifetime is not always an optimal solution for a routing protocol to consider, as it may incur limitations to the routing process, especially in mobile ad-hoc networks when the sending node is moving at a higher speed than a selected neighbouring node to relay the data traffic. According to the conventional lifetime estimation method, which leads to long-lived links, the connection between the two nodes remains available even when the sending node overpasses the relaying node. This can influence the selection process of the next relaying node and the protocol's overall routing performance.

5.4 Stability-Aware Greedy Routing

In this section, we propose a Stability Aware Greedy (SAG) routing algorithm designed to forward the data packets over stable routes. We assume that every node can obtain the required information such as location, speed and direction. Furthermore, each node maintains a location table to store the location information of the nearby travelling nodes. Updating the table entries is achieved by the use of periodic beacon messages.

The proposed SAG routing protocol is based on greedy forwarding, where the end-to-end route in unknown to the source node. The source node is assigned the task of relaying the packets to the next hop neighbouring node that maximizes the link-lifetime based routing metric. The same process is repeated at every selected forwarding node until the destination is reached. Since link stability is a major issue in mobile networks –specifically in Vehicular Ad-hoc Networks (VANETs), where the nodes' speed is considerably high- we propose a selection metric, which will depend on the stability (link lifetime) of the links amongst moving nodes. The next forwarder of the packet is the node that maintains the highest routing metric, which is a function of the distance progress to the destination and the link lifetime, Γ, of the sending node. The selected node will be responsible of forwarding the packet, as long as the link with the sending node is still available. If the sending node detects through beaconing that the link has failed, the selection process is then triggered to find a new next hop forwarder.

The routing metric for a neighbouring node Ni is defined as follows:

(5-10)

where Di is the distance separating N_i and the destination node, D is the distance between the sender and the destination, and α is the metric coefficient ($0 < \alpha < 1$).

Note that if α is equal to 1, SAG performs the same as distance-based greedy forwarding, according to which the closest neighbour to the destination is selected to be the next relaying node.

An example of SAG routing is given in Figure 5-3, which illustrates the operation of stability-based SAG (coefficient metric α=0). The link {S, 1} has the longest lifetime among the rest of the links with the sending node S, therefore, node 1 is selected as the next hop forwarding node. At the second hop, the same process is applied. Link {1, 2} maintains a longer lifetime than link {1,3} leading to select node 2 as the second hop forwarding node.

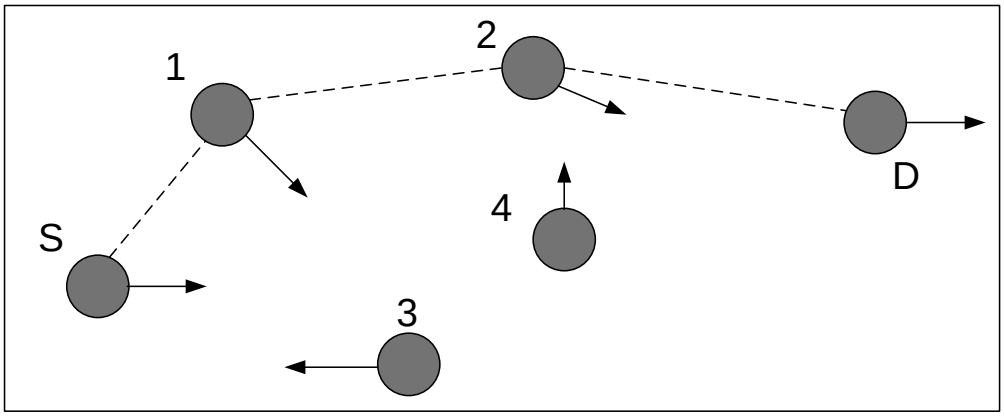

Figure 5- 3: An instance of SAG routing for α=1

Similar concept can be applied in Beaconless routing [25] and [26] by setting the timer value - originally set based on the node's progress to the destination- to be a function of the stability factor Γ.

What follows is an algorithmic description of the ForwardPacket procedure, executed at the node holding a packet to a specific destination.

```
Algorithm    Forward Packet
Constant:    RADIO_RANGE, α;
Input:       NeighbourTable, sender, destination;
Variables:   Max = 0, order = 0, tempNode, d, t1, t2,  Γ;
Output:      M;
1   begin
2      if (NextForwarder ≠ 0)
3                TransmitPacket (NextForwarder);
4      else
5           if (NeighborTable  = 0)
6                     Exit;
7           end if;
8                 d = distance (sender, destination);
9                 foreach i < size (NeighbourTable) do
10                      tempNode = select (NeighbourTable, i);
11                      d = distance (tempNode, sender);
12                      t1 = link_lifetime1 ( );
13                      t2 = link_lifetime2 ( );
14                      Γ = min (t1, t2);
15                      M = α* Γ+ (1-α)* Δ
16                      if (M > Max)
17                            Max = M;
18                            order = i;
19                      end if;
20                end for;
21                NextForwarder = select (NeighbourTable, order);
22                TransmitPacket (NextForwarder);
23     end if;
24  end;
```

We use the following notation:

- *select (NeighbourTable, i)*: a function that returns the i^{th} entry of the list NeighbourTable.
- *distance (N1,N2)*: a function that returns the distance between two nodes N_1 and N_2.
- *link_lifetime1 ( ):* a function that returns time t_1 based on the conventional method proposed in [6].
- *link_lifetime2 ( ):* a function that returns time t_2 based on the proposed link lifetime estimation method.

5.5 Simulation test

The performance of the proposed estimation method was evaluated through simulation using OPNET 14.5 modeler [27]. OPNET 14.5 modeler provides a complete implementation of the IEEE 802.11 radio and MAC specifications. The IP addressing scheme was IPv4 while the PHY was configured to be conformant with the IEEE 802.11g (Extended rate PHY). Moreover, the packet size was set to 1024 bits, the traffic rate to 100 packets/sec and the data rate to 24

Mbps, while the radio transmission radius was kept constant for all the nodes and equal to 97 meters.

The simulation was performed by applying the proposed link lifetime estimation method as well as the one proposed in [6] on stability-aware greedy forwarding (SAG). The evaluated SAG schemes are respectively called SAG-modified and SAG-conventional. The metrics used for evaluation are the average delivery ratio, average end-to-end delay (sec), average link lifetime (sec) and average retransmission attempts (packets). What follows is the definition of the evaluated metrics:

- ***Average packet delivery ratio***: is the ratio of the data bits received by the destination node to the data bits generated by the source.
- ***Link lifetime (sec)***: is the average lifetime, in seconds, of all the links established to forward the data packet from the source to the destination node.
- ***End-to-end delay (sec)***: the end-to-end delay of the packets, throughout the entire network, computed by the time elapsed between the time the packet was generated and the time it got received by the destination node. Therefore, all possible delays caused by queuing, retransmission and propagation are included.
- ***Retransmission attempts (packets)***: the total number of packet retransmission attempts by all WLAN MACs in the network until the packet is either successfully transmitted or it is discarded as a result of reaching the short or long retry limit.

Table 5- 1: Simulation Parameters

Data rate	24 Mbps
Transmission Range	97 m
Packet size	1024 bits
Mac protocol	802.11g
IP addressing scheme	IPv4
Traffic	100 packets/sec
Simulation time	100 sec

5.5.1 Simulation scenarios

In all the scenarios, we have considered a source-destination pair located two hops away from each other, while the intermediate nodes are deployed in one lane (scenario I, scenario II) and two lanes (Scenario III), which provides end-to-end multi-hop connection.

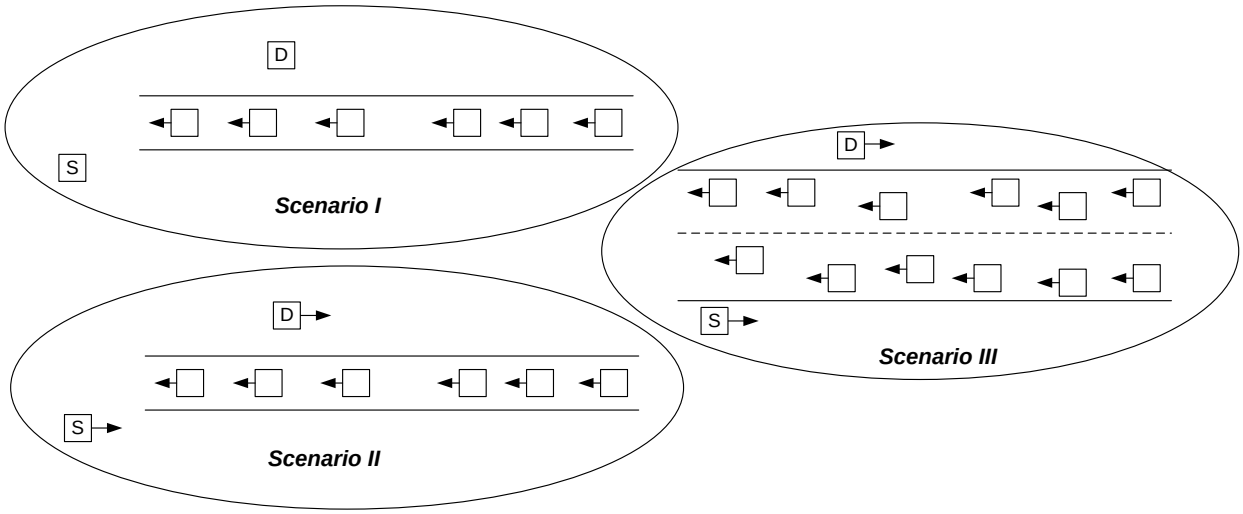

Figure 5- 4: An instance of the simulation scenarios

- ***Scenario I:***

The source and the destination are considered stationary. The intermediate nodes, deployed in a single lane between the source and the destination nodes, travel at a constant speed towards the source as shown in Figure 5-4. Six runs of the scenario were conducted while modifying the speed of the intermediate nodes to 5, 10, 15, 20, 30 and 35m/s.

- ***Scenario II:***

The source, the destination as well as the intermediate nodes move at a constant speed. The source and destination node are moving in opposite direction from the intermediate nodes. Six runs of the scenario were conducted while the speed of the source and destination nodes was modified to 5, 10, 15, 20, 30 and 35m/s.

➢ ***Scenario III:***

The source, the destination as well as the intermediate nodes move at a constant speed. The source and destination nodes are moving in an opposite direction from the intermediate nodes that are deployed in two lanes. The speed of the source and the destination nodes is assumed to be constant and equal to 10m/s. Six runs of the scenario were conducted while the speed of the intermediate nodes was modified to 5, 10, 15, 20, 30 and 35m/s.

5.5.2 Simulation results

Scenario I Simulation results

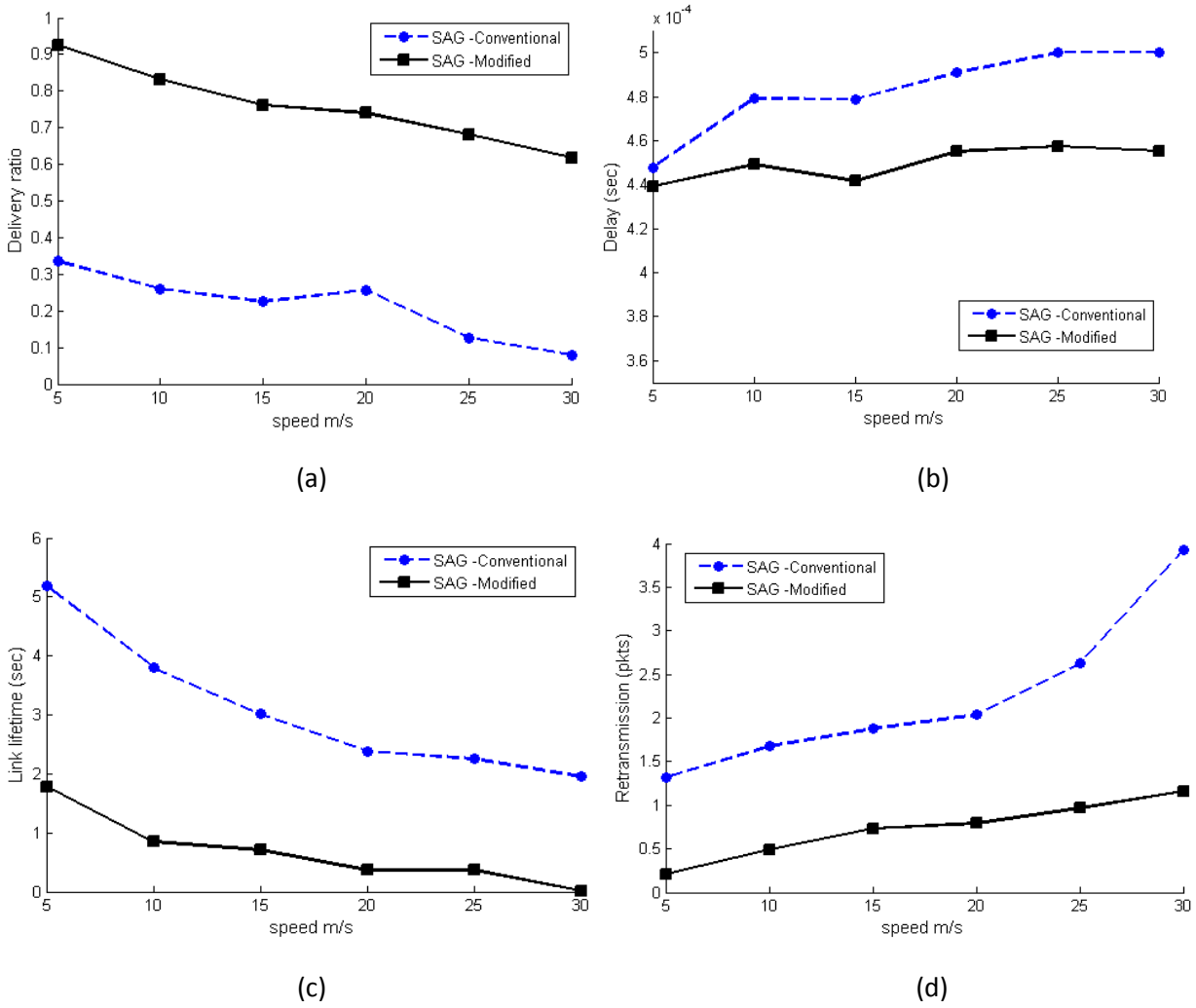

Figure 5- 5: Average delivery ratio, (b): average network delay (sec), (c): average link duration and (d): average retransmission attempts (packets

Scenario II Simulation results

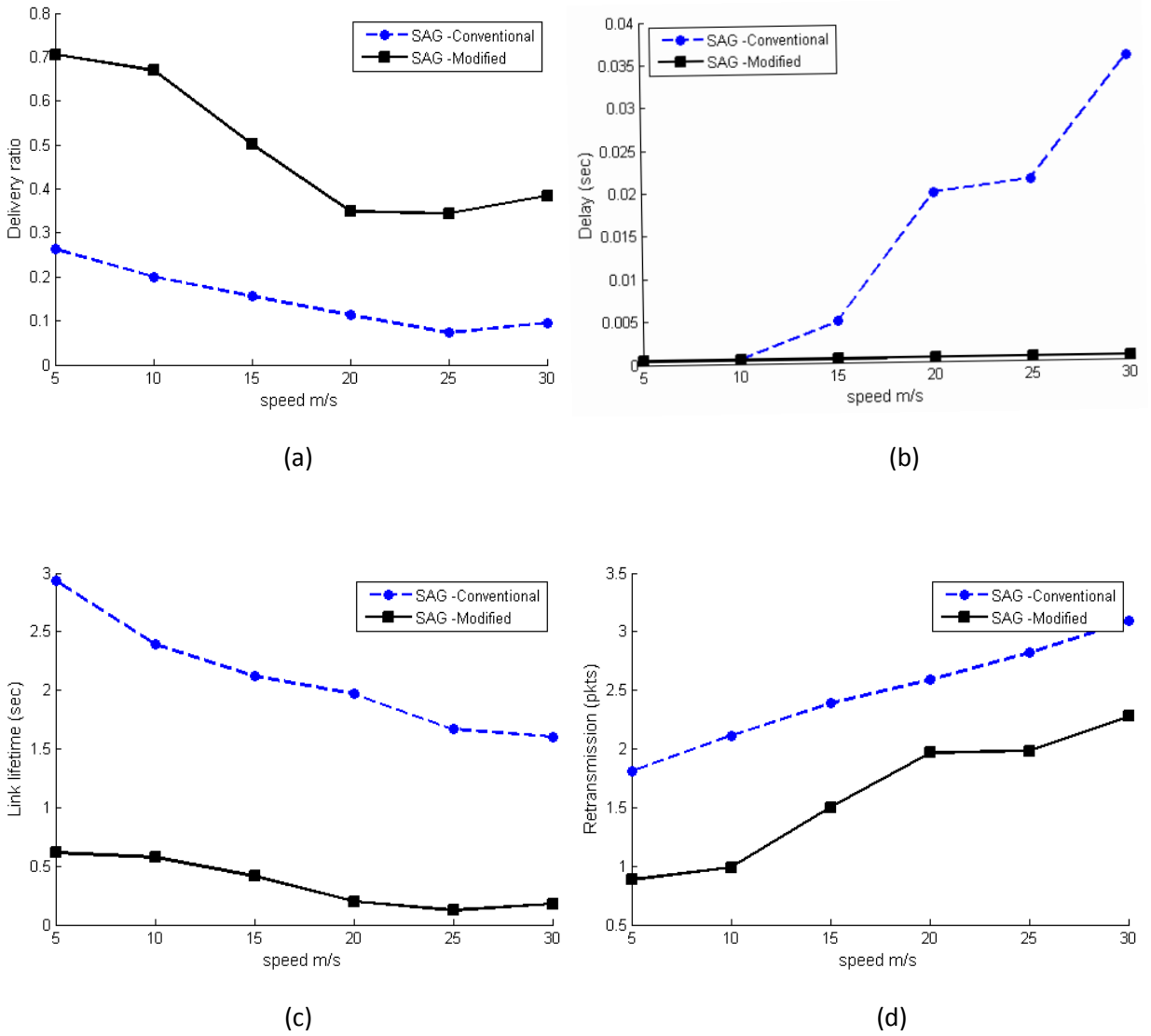

Figure 5- 6: Average delivery ratio, (b): average network delay (sec), (c): average link duration and (d): average retransmission attempts (packets)

Scenario III Simulation results

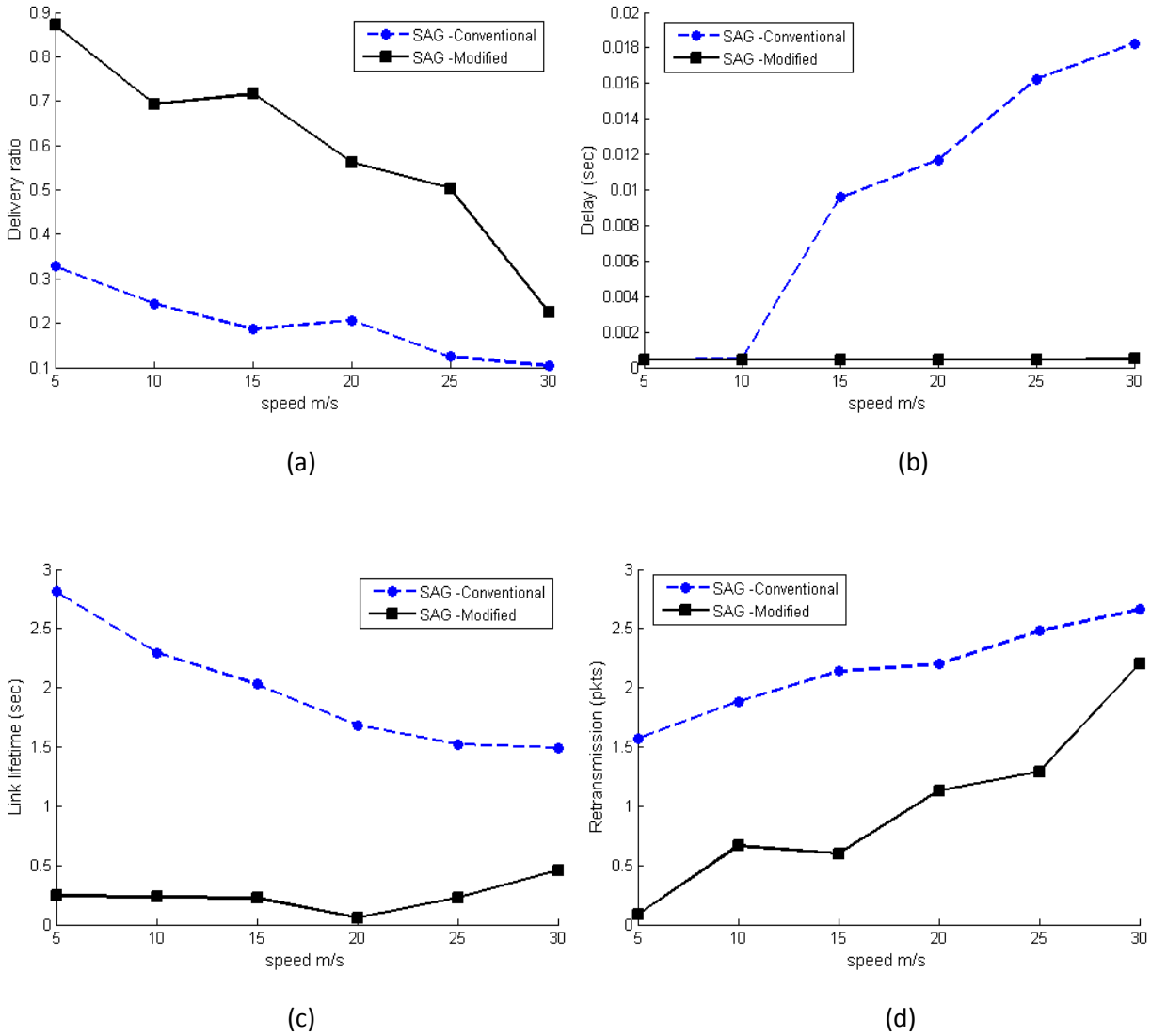

Figure 5- 7: Average delivery ratio, (b): average network delay (sec), (c): average link duration and (d): average retransmission attempts (packets)

5.5.3 Results analysis

We have considered two-hop communication scenarios between the source and the destination, throughout the simulation, to show the impact of the proposed and the conventional methods on the availability of the links formed between the nodes composing the end route to the destination. Figures 5-5a, 5-6a and 5-7a show the delivery ratio achieved by SAG protocol when the conventional [6] and the proposed link lifetime estimation methods are applied. It is clearly illustrated that SAG-modified achieves considerably higher ratio than SAG-conventional that decreases as the nodes move at higher speed. The low ratio achieved by SAG-conventional is related to the impact of selecting the next hop node to forward the packets. As previously mentioned, according to SAG protocol, the selected node remains the next hop relaying node as long as the link between the two nodes stays available. Hence, SAG-conventional applies the selection process less frequently than SAG-modified does due to the longer estimated lifetime of the links. Therefore, when the selected node moves out of the forwarding zone (greedy area), the link is still considered active by SAG-conventional that causes the number of hops to the destination to increases and, more importantly, the chances of selecting a more suitable relaying node to decrease.

Furthermore, the impact of the link estimation method on the routing performance in terms of the network delay is depicted in Figures 5-5b, 5-6b and 5-7b, which show SAG's average delay for the two estimation methods for scenarios I, II and III, respectively. It is clearly illustrated that the SAG-modified maintains lower delay as compared to SAG-conventional. As previously mentioned, the proposed estimation method considers the link between two nodes to be available, as long as the relaying node remains within the progress area of the sending node. Whereas, according to the conventional method, the lifetime of the link is determined by the period the two nodes forming the link remain within the radio range of each other. Therefore, the link lifetime is shorter when SAG-modified modified is applied as it is clearly illustrated in Figures 5-5c, 5-6c and 5-7c. A shorter link lifetime allows the routing protocol for a selection of a better candidate closer to the destination, to relay the packet. Accordingly, in two-hop communication scenario, the two versions of SAG perform in a similar manner when the

selected node is within the progress area. As soon as the node moves out of the progress area while it is still within the radio range of the source node, SAG-modified chooses a new node as the next forwarder and thus, keeping the two hop communication with the destination. Whereas, according to the SAG-conventional, the link is still available as the node remains within the radio range, hence the two-hop communication turns into three hops as the destination becomes unreachable by the selected node. As a result, an increase in the number of hops leads to an increase in the end-to-end delay.

Finally, Figures 5-5d, 5-6d and 5-7d depict the average retransmission attempts of the evaluated SAG schemes. A closer observation shows the high retransmission attempts, experienced by SAG-Conventional, to successfully relay the packet to the next hop. This poor performance is due to the extended lifetime of the link connecting the sender and the relaying node , when the latter remains the selected candidate, even though it may get disconnected from the other nodes that lead to the destination.

5.5.4 Adjusting the metric coefficient α

In the following evaluation, scenario I is considered in order to verify the influence of the metric coefficient α on the delivery ratio and on the link lifetime of the SAG protocol, while considering different node speeds.

Figure 5-8 shows that the delivery ratio is constant as long as the coefficient α has a non-zero value. Therefore, assigning a non-zero value to α does not inflict any variation to SAG's performance and the only parameter that impacts is the nodes' speed. When α is equal to zero, SAG protocol performs the same as the distance-based greedy forwarding [2], according to which the next hop forwarding node is selected based on its distance to the destination, ensuring that the data packets are sent to the closest neighbour to the destination. The delivery ratio achieved by the distance-based greedy forwarding (α = 0) is higher as compared to SAG.

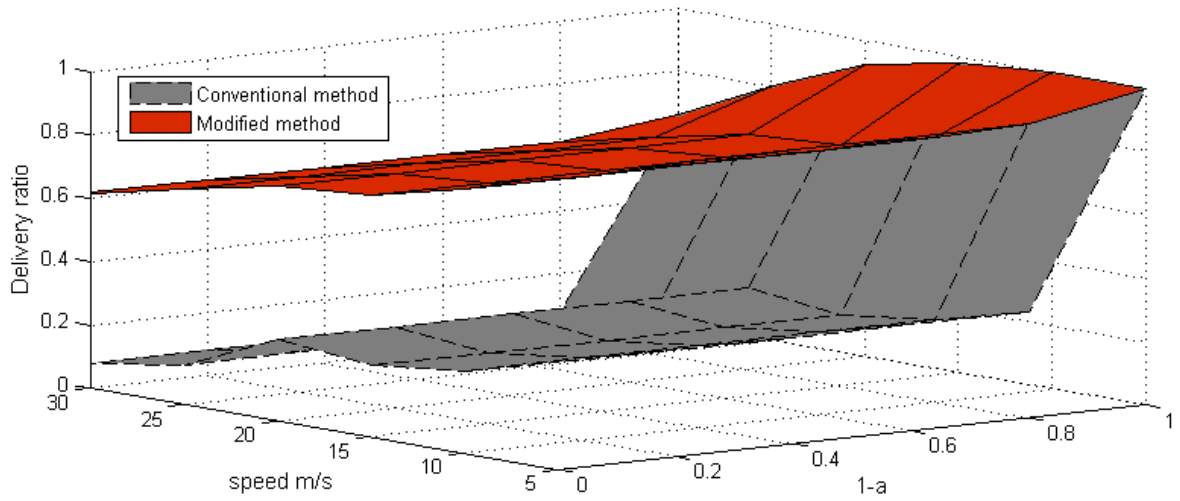

Figure 5- 8: The 3D illustration of the delivery ratio for different speeds and metric coefficient α

In addition, figure 5-9 shows the link lifetime variation in respect to the nodes' speed and the metric coefficient α. We can observe that the link lifetime maintains a constant shape for a non-zero α, while the lifetime tends to be zero when α is equal to 0.

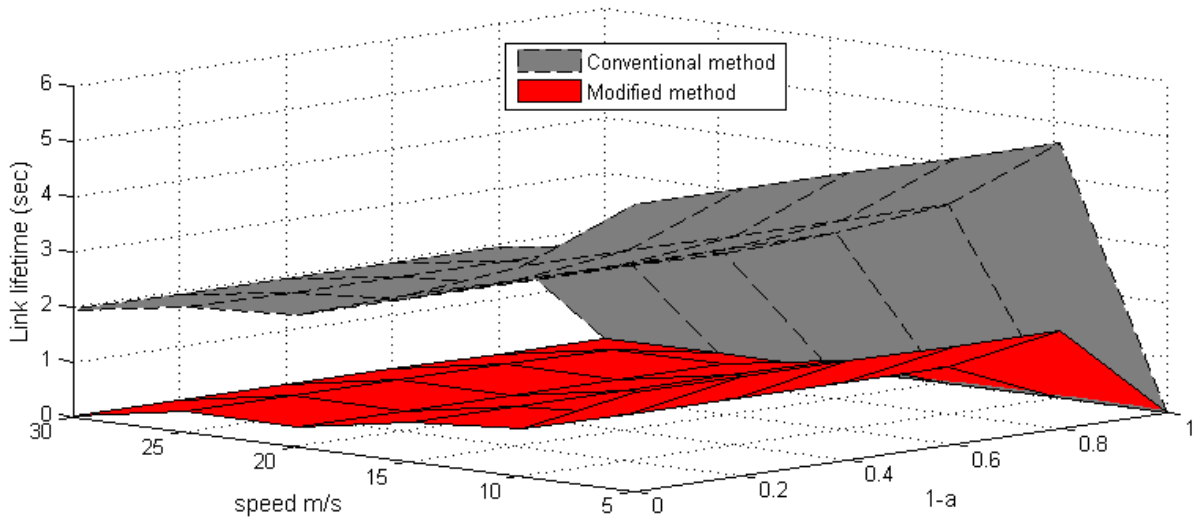

Figure 5- 9: The 3D illustration of the link lifetime for different speeds and metric coefficient α

5.6 Conclusion

This chapter presented a novel method for estimating the link lifetime in greedy forwarding schemes. The proposed method, in contrast to the conventional one, takes into account the position, the speed and the direction of the nodes, forming the link, as well as the destination. Accordingly, given that a source node in active communication with a destination node, the lifetime of a link between the source node and its neighbour is represented by the duration the neighbouring node remains in the forwarding area of the source node in respect to the destination. Besides, a greedy method, called SAG, was also studied, which introduced a link lifetime based metric as the criterion of selecting the next relaying nodes. A stability parameter α was employed to manage the weight of the link lifetime of the metric. For $\alpha = 0$, SAG selects the next hop node that provides the highest link lifetime with the source, while it acts as the typical distance-based greedy scheme when α equals 1. Both conventional and proposed link lifetime estimation methods were applied to SAG to evaluate their impact on the routing performance. The simulations showed that the delivery ratio of the stability-based SAG was significantly higher when the proposed estimation method was applied, in addition to the outperformance achieved in terms of network delay and packet retransmission. Additional simulations were carried out to investigate the impact of the metric coefficient α on the performance of SAG. It was shown that the distance-based greedy scheme achieved higher delivery ratio than the stability-based scheme.

References

[1] H. Takagi and L. Kleinrock, “Optimal transmission ranges for randomly distributed packet radio terminals,” IEEE Transactions on Communications, Vol. 32, No. 3, pp. 246–257, March 1984.

[2] G.G. Finn, “Routing and Addressing Problems in Large Metropolitan-Scale Internetworks”, Research Report ISU/RR-87-180, Inst. For Scientific information, Mar. 1987.

[3] T.-C. Hou V. Li , “Transmission Range Control in Multihop Packet Radio Networks,” IEEE Transactions on Communications, Vol. 34, No. 1, pp. 38- 44, Jan 1986.

[4] E. Kranakis, H. Singh, and J. Urrutia, “Compass routing on geometric networks,” in 11th Canadian Conference on Computation Geometry (CCCG), pp. 51-54,, 1999.

[5] W. Su, S.Lee, and M. Gerla, “Mobility prediction and routing in ad hoc wireless networks,” *in International Journal of Network Management*, Vol. 11, No. 3, John Wiley & Sons, pp. 3-30, 2001.

[6] R. Chang, S. Leu, "Long-lived path routing with received signal strength for ad hoc networks," 1st International Symposium on Wireless Pervasive Computing , Jan. 2006.

[7] Y. Tseng, Y. Li, Y. Chang, "On route lifetime in multihop mobile ad hoc networks," IEEE Transactions on Mobile Computing, Vol.2, No.4, pp. 366-376, 2003.

[8] S. Jiang, D. He, J. Rao, “A prediction-based link availability estimation for routing metrics in MANETs”, IEEE/ACM Transactions on Networking, Vol. 13, pp. 1302 - 1312, Dec 2005.

[9] A. B. McDonald and T. F. Znabi, “A path availability model for wireless ad hoc networks,” in Proc. IEEE WCNC, pp. 35–40, 1999.

[10] A. B. McDonald , T. Znati “A mobility-based framework for adaptive clustering in wireless ad hoc networks,” IEEE J. Sel. Areas Commun., Vol. 17, No. 8, pp. 1466–1487, Aug. 1999.

[11] C.-K. Toh, “Associativity based routing for ad hoc mobile networks,” Wireless Personal Communications Journal, Special Issue on Mobile Networking & Computing Systems, Vol. 4, No. 2, pp. 103-139, Mar. 1997.

[12] R. Dube, C.D. Rais, K.-Y. Wang, and S.K. Tripathi, “Signal Stability-Based Adaptive Routing (SSA) for Ad Hoc Mobile Networks,” IEEE Personal Communications Magazine, Vol. 4, No. 1, pp. 36-45, February. 1997.

[13] S. Agarwal, A. Ahuja, J.P. Singh and R. Shorey, “Route-lifetime assessment based routing (RABR) protocol for mobile ad-hoc networks”, in: Proc. of IEEE International Conference on Communications, ICC 2000, pp. 1697–1701, June 2000.

[14] Y. Chen, G.Wang, S. Peng, “Link Lifetime-Based Segment-by-Segment Routing Protocol in MANETs”, International Symposium on Parallel and Distributed Processing with Applications, pp. 387 – 392, 2008.

[15] M. Al-Akaidi, and M. Alchaita, "Link stability and mobility in ad hoc wireless networks," IET Communications, Vol. 1, pp. 173-178, April 2007.

[16] K. N. Sridhar and C. M. Choon, “Stability and hop-count based approach for route computation in MANET,” in Proc. of ICCCN, pp. 25-31, 2005.

[17] X. Hu, J. Wang, C. Wang, “Stability-enhanced routing for mobile ad hoc networks”, Computer Design and Applications (ICCDA), 2010 International Conference on , pp. 553-556, June 2010.

[18] S. Jung, D. Lee, S, Yoon, J. Shin, Y. Lee, J. Mo, “A geographic routing protocol utilizing link lifetime and power control for mobile ad hoc networks,” proceeding of the 1st ACM international workshop on Foundations of wireless ad hoc and sensor networking and computing, pp. 25-32, May 26, 2008.

[19] Rao, S. A., Pai, M., Boussedjra, M., & Mouzna, J. (2008). GPSR-L: Greedy perimeter stateless routing with lifetime for VANETS. International Conference on ITS Telecommunications (ITST), pp. 299-304, 2008.

[20] B. Karp and H. T. Kung, “GPSR: Greedy perimeter stateless routing for wireless networks”, in ACM/IEEE International Conference on Mobile Computing and Networking, pp. 243–254 ,2000.

[21] W. Yang, W. Yang, W. Yang, W. Yang, "A Stable Backup Routing Protocol Based on Link Lifetime in Mobile Ad hoc Networks ", Third International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies, pp. 202-207, 2009.

[22] M. Zarei, K. Faez, J. Moosavi. "Modified Reverse AODV routing algorithm using route stability in mobile ad hoc networks". International Multitopic Conference. pp. 255-259, 2008.

[23] M. EffatParvar, M.R. EffatParvar, A. Darehshoorzadeh, M. Zarei, N. Yazdani, "Load balancing and route stability in mobile ad hoc networks base on AODV protocol", Intl Conf on Electronic Devices, Systems and Applications (ICEDSA), pp. 258 – 263, April 2010.

[24] J. Sun; Y. Liu; H. Hu; D. Yuan, "Link Stability Based Routing in Mobile Ad hoc Networks", 5th IEEE Conference on Industrial Electronics and Applications (ICIEA), pp. 1821 - 1825, 2010.

[25] H. Füßler, J. Widmger, M. Käsemann, M. Mauve, and H. Hartenstein, "Contention-based forwarding for mobile ad-hoc networks," Ad-Hoc Networks, Vol. 1, No. 4, pp. 351–369, 2003.

[26] M. Heissenbuttel and T. Braun, "BLR: beacon-less routing algorithm for mobile ad hoc networks", Computer Communications, Vol. 27, No 11, pp. 1076–1086, 2004.

[27] OPNET Modeler, OPNET Technologies, Inc ®. Available: http://www.opnet.com

Chapter 6

Location-Aided MAC for Mitigating Hidden Terminal Problem

6.1 Introduction

The IEEE 802.11 standard [1] specifies Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) as the Medium Access Control (MAC) protocol adopted by the wireless stations to share the wireless channel. The basic MAC in 802.11 standard is the Distributed Coordination Function (DCF). This is defined for asynchronous data traffic in the basic service set (BSS), while the optional Point Coordination Function (PCF) is used to support time-bounded traffic with QoS requirements.

CSMA/CA applies listen-before-talk, according to which any node willing to transmit data must sense the wireless channel in order to determine whether another station is transmitting. If the channel is detected as being idle, the station initiates the transmission, otherwise, the transmission is deferred for a random period of time. In addition, CSMA/CA employs an acknowledgment mechanism that makes the receiving station transmit an acknowledgment (ACK) packet back to the sender after a short interval of time, to indicate a successful reception. In case the ACK packet is not received, the data packet is considered lost and a packet retransmission is scheduled.

Any wireless station can detect a wireless signal within its carrier sensing range and therefore, it is able to determine whether the channel is busy. It is commonly assumed, as well as in this work that the carrier sensing range is equal to the transmission range of the wireless

station. Accordingly, wireless networks that utilize CSMA/CA as the MAC protocol are subject to the so-called hidden terminal problem, which may occur when the stations willing to access the wireless channel are not within the carrier sensing range of each other. In consequence, a station may sense that the medium is idle and attempt to access it when another station is already transmitting. This results in radio interference and packet collision at the receivers that can detect the transmission of the hidden stations, alongside a considerable reduction in the network throughput.

In order to reduce the occurrence of hidden terminals, the optional "virtual carrier sensing" mechanism is specified in the IEEE 802.11 standard. It employs the Request-To-Send/Clear-To-Send (RTS/CTS) handshake technique, which aims to prevent wireless stations to access the wireless channel simultaneously. This way, it intends to eliminate the interference caused by the hidden terminals and to decrease the packet collisions and the resultant throughput. RTS/CTS are exchanged prior to the data transmission if the data frame size is larger than the specified RTS threshold [1], so as to reserve the wireless channel for the sending station. The process is initiated by the sending station, which senses the channel and sends an RTS packet if the channel is found idle. The sending station waits for a CTS packet from the receiver in order to start the effective data transmission. Although RTS/CTS technique eliminates the hidden terminal problem, the performance of the network degrades as the number of wireless stations increases. This is due to the additional control traffic sent (RTS/CTS messages), which impacts the network throughput and the message delay, as well as the residual energy of the wireless stations. Additionally, It is demonstrated in [2] through an experimental study, that the RTS/CTS scheme is not useful in network scenarios of 54 Mbps data rate and its effectiveness in improving the network throughput and packet delay is uncertain. Besides, the study in [3] shows that by transmitting RTS/CTS packets at 2Mbps or 11Mbps data rate not only fail to solve the problem, but also further degrades the throughput by introducing additional overhead.

In this chapter, we propose a new technique to mitigate the hidden node problem in 802.11 Wireless LANs, based on the geographical position of the wireless stations. The technique is called Distributed Location-Aided (DLA) algorithm, whose core concept aims to divide the radio

range of the wireless receiver into four zones, according to which a time delay called "zone delay" is introduced. This can be seen as a hybrid MAC combining the carrier sense and the time domain multiple access techniques in one scheme. While every zone is assigned a specific time slot controlled by the zone delay, the stations within a zone compete between each other based on the carrier sense protocol for accessing the wireless medium. Knowing the position of the receiving station, the transmitter can identify the zone in which it is located and determine, accordingly, the correspondent delay that will be added to defer the transmission.

The current chapter is structured as follows: in section 6.2, we review the existing related work. Section 6.3 describes the proposed algorithm in detail. The simulation results and the performance analysis are presented in section 6.4 and eventually, section 6.4 concludes the chapter.

6.2 Related work

Hidden Terminal (HT) is a well-known problem in 802.11 wireless networks that can cause severe performance degradation. It is related to the imperfect operation of the Carrier Sense Multiple Access (CSMA) protocol of the 802.11 MAC that fails to prevent simultaneous access attempts to the wireless channel.

Queuing-based analysis and mathematical model have been presented in [4], [5] and [6] to study the impact of the hidden terminal problem on the network's performance. The authors have also derived an analytical expression of the probability of packet collisions.

Many algorithms and research work have addressed the hidden terminal in wireless networks. Some of the proposed methods were designed to eliminate the problem, while some other to provide with solution for reducing its impact on the network's performance.

6.2.1 Busy-tone based mechanisms

Busy Tone Multiple Access (BTMA) protocol is proposed in [7] to eliminate the hidden terminal problem. It relies on a centralised network operation, where the base station is within the range of all the terminals. BTMA uses the concept of busy-tone channel, according to which the available bandwidth is divided into two channels: a message channel and a busy-tone (BT)

channel. As long as the base station senses a carrier on the message channel, it transmits a busy-tone signal on the busy-tone channel to notify the terminal of the state of the message channel. BTMA access operation is similar to the CSMA's, in the sense that the terminal senses the BT channel before transmitting data. If no signal is detected on the BT channel for a detection time (t_d), the terminal transmits the data packet, otherwise it defers the transmission for a random rescheduling delay.

Modified versions of the BTMA are presented in [8] and [9]. Receiver Initiated Busy Tone Multiple Access (RI-BTMA) scheme [8], divides the packet into a preamble portion and a data portion. The preamble portion of the packet is sent via the data channel by the transmitter after detecting the tone channel as being idle. The receiver acknowledges the successful reception of the preamble by sending a busy-tone signal over the BT channel, allowing the sender to transmit the data portion of the packet and preventing transmission conflict from other nodes. The busy tone is transmitted as long as the receiver is receiving data packets.

Dual Busy Tone Multiple Access (DBTMA) is introduced in [9]. It discusses the use of two busy tones, BT_t (transmit busy tone) and BT_r (receive busy tone) to provide protection from the RTS and data transmission respectively. Following a busy tone signal free channel, the sender transmits an RTS packet after turning on the BT_t. The receiver turns on the BT_r and replies to the sender if the RTS packet was successfully received. The sender will then proceed with the data transmission upon sensing the BT_r signal. An improvement of the RI-BMTA scheme is introduced through the Wireless Collision Detect (WCD) protocol [10] that addresses the hidden node problem by making use of a feedback channel to indicate the receiver state. When a node detects an ongoing data transmission, it sets up the feedback signal before the end of the Receiver Detection Interval (RDI), which is the time needed to determine the destination of the transmission and to assert the feedback channel. After processing the header of the received packet, only the node whose address matches the one in the packet keeps the feedback signal on. The sender continues its transmission after sensing the receiver's feedback signal. In [11] the Asynchronous Wireless Collision Detection with Acknowledgment (AWCD/ACK) for Wireless Mesh Networks is proposed, which deals with the hidden terminal

problem by also making use of a busy tone. The sender transmits the first part of the packet, which includes the destination Address Header (AH), after sensing that the channel is busy tone free. All the receivers within the range of the sender power off their BT, except from the targeted node. The sender will resume the transmission of its data following the acknowledgment that the AH has been received. The work in [12] has pointed the Receiver Busy-Tone Self-Interference (RBTSI) problem, according to which the transmitted busy tone signal of the receiver interferes with its own data. The author has also proposed an approach to get around the RBTSI problem by transmitting the busy tone signal prior to the associated data signal.

6.2.2 Handshake-based mechanisms

The concept of a handshake mechanism between sender and receiver was firstly introduced in [13] that proposed the Split channel Reservation Multiple Access (SRMA) scheme. SRMA is based on the control signal handshake mechanism that splits the control channel into request and answer-to-request channel. The transmitter exchanges control signals over the control channels to determine the time to start the data transmission.

The well-known RTS/CTS scheme was introduced in [14], in which the sender requests channel for data transmission by sending a Request-To-Send (RTS) packet. The receiver replies with a Clear-To-Send (CTS) packet, giving the sender channel access and preventing any collision caused from other possible transmissions. Several improvements of the RTS/CTS scheme were proposed in [15], [16], [17], and [18]. In addition to the new backoff algorithm proposed, the authors of [15] suggest to add to the RTS/CTS handshake two additional control packets: Acknowledgement (ACK) and Data Sending (DS) packets. The ACK is used by the receiver to notify the sender of successful reception of the data. If the sender does not receive the ACK, it schedules a retransmission. DS packet is introduced in order to solve the conflict caused by the exposed node problem and is transmitted by the sender to notify all the nodes within its range if the data transmission. Floor Acquisition Multiple Access (FAMA) scheme is proposed in [16]. FAMA requires that the sending node should gain control over the channel (floor), before attempting to transmit any data packets, to ensure a collision free transmission. Floor

acquisition is achieved using RTS/CTS and carrier sensing. Two variants of FAMA scheme, named FAMA-NPS (Non-persistent Packet Sensing) and FAMA-NCS (Non-Persistent Carrier Sensing) are proposed in [17]. Carrier sensing and longer CTS packet are used in FAMA-NCS. The longer CTS packet is introduced to ensure floor acquisition and collision free data reception. Nodes transmitting, an RTS packet simultaneously, will hear a portion of the CTS and therefore backoff from accessing the channel. The Distributed Coordination Function used by the IEEE 802.11 MAC [18] employs the Carrier Sense Multiple Access (CSMA/CA) [19] and the RTS/CTS scheme. A recent scheme is proposed in [20], combining the busy-tone approach and the RTS/CTS mechanism. To prevent packet collisions, RTS and data packets are transmitted through different channels: control channel and data channel. To eliminate the collisions amongst RTS packets and data packets, the two channels are separated using Frequency and Time Division Multiplexing (FDMA and TDMA). An improvement of MACA scheme, called MACA-RPOLL is presented in [21]. Its concept was inspired by the Point Coordination Function (PCF) of the 802.11 MAC and is applied when the control packets collide. After detecting the collision, the receiver initiates a polling mechanism that polls the wireless nodes one by one.

6.2.3 Carrier sense tuning mechanisms

The key idea behind these types of schemes is to work on the sensitivity threshold of the transceiver to extend its Carrier Sensing (CS) range, where usually the received signal does not get decoded correctly. CS significantly influences the network's performance. By extending the carrier sensing range, the interference and the effect of the hidden terminals may be effectively reduced. However, a larger CS range can reduce the spatial reuse and can significantly affect the throughput as any potential transmitters sensing a busy medium have to defer their transmission. Several studies have discussed CS's impact on the system's performance. One of those is presented in [22], which discusses the effects of carrier sensing range on the MAC layer performance. In [23], the authors proposed an adaptive carrier sensing scheme for mitigating the hidden terminal problem. The basic idea is that each wireless node adaptively selects its Carrier Sense Threshold (CST) based on the periodic transmission of Busy/Idle signal by the Access Point (AP) and the node's BI. Two distributed power control schemes are introduced in

[20], thus minimising the mutual interference amongst links, while avoiding the hidden terminal problem. The transmit power of the transmitter is adjusted based on its connectivity with the receiver as well as the interferences with the surrounding links.

6.2.4 Node grouping mechanisms

The idea of grouping includes grouping the nodes based on their connectivity state and their visibility to each other. Grouping strategy aims to separate the hidden terminals in order to assign different access to the medium, avoiding therefore the occurrence of the hidden terminal problem. Such strategy is more suitable for centralised topologies, such as 802.11 Basic Service Set (BSS) or a Personal Area Network, where the grouping task can be achieved by the Access Point (AP) and the Piconet Coordinator (PNC).

A grouping strategy that avoids the hidden terminal problem in IEEE 802.15.4 Low-Rate WPAN (LR-WPAN) is proposed in [25]. The grouping process is based on the hidden relationship of the nodes and consists of four phases: collision detection, information collection, grouping and bandwidth allocation. It is assumed that the coordinator can distinguish the hidden terminal collision from a normal one based on the time of the occurrence of the collision. Once the collision is detected, the coordinator initiates the polling process by requesting every node to send an acknowledgement (ACK) frame. Each node will then report back to the coordinator that collected the hidden-terminal information, according to which the grouping process is applied and the bandwidth is allocated to each group based on its size. In [26], a clustering algorithm is proposed to resolve the hidden node problem in infrastructure mode IEEE 802.11 wireless LANs. This is achieved by grouping the Stations into clusters, in a way that all the nodes within a cluster can detect each other's transmission signal. The Contention Period (CP) is divided into M Sub-Periods (SP), where M is the number of clusters. Each wireless node within the BSS is required to maintain a list of the nodes whose signals can be detected by the node's physical carrier sensing mechanism. The collected information of the detected carrier will be then sent to the Access Point (AP) during the Contention Free Period (CFP), based on which the AP groups the nodes into clusters. The constant $F_{i,j}$, which indicates whether the $node_j$ can detect the

transmission signal of $node_i$, is introduced for the clustering process. It takes the value of 1 if there is connectivity between $node_i$ and $node_j$ and 0 otherwise.

Recent work is the Hidden Node Avoidance Mechanism (H-NAM) proposed in [27], to avoid the hidden node collision in wireless sensor networks (WSNs). H-NAM is based on a grouping strategy to split each cluster of the WSN into disjoint groups of non-hidden nodes. The process consists of four steps: group join request, neighbour notification, neighbour information report, and group assignment. To avoid the hidden node collision, node N_i sends a group join request message to the Cluster Head (CH) that will acknowledge the reception. Any node that belongs to a group adds N_i address to its neighbour table upon receiving N_i's join request message and is required to sends a notification message. After receiving the ACK packet, N_i waits for the neighbour notification messages to be received, which will be reported to the CH. When the CH receives N_i's neighbour information, the group assignment procedure is initiated, to assign N_i to a given group according to the list of neighbours and available resources. In case no group, whose nodes are Ni's neighbours, is found, the CH checks whether there is available resources for creating a new group.

6.2.5 Interference cancellation mechanisms

The concept of interference cancellation is introduced in order to reduce the packet loss caused by the collisions. It tackles the receiver design to allow the decoding of the collision, as interfering signals, unlike noise, have a structure determined by the data they carry. Several studies have addressed the interference cancellation [28], [29] and [30], where various prototypes and decoding algorithms were developed. The work in [28] and [29] resolve the collisions and recover multiple simultaneous signals by the use of successive interference cancellation and joint decoding. However, it is discussed in [30] that those methods are effective when the senders transmit at a bit rate significantly lower than allowed by their respective Signal-to-Noise Ratios (SNRs) and code redundancy. In [30], an 802.11 receiver design is proposed to limit the effect of the hidden terminals. Assuming that the collisions occur at different offsets, due to random jitter of the 802.11, the access point can identify the interference-free symbols (chunk1) in one of the collisions (collision 1), which will be used to

identify the marred chunk in the other (collision 2). The AP then decodes chunk1, re-encodes the decoded symbols in chunk1 and subtracts them from other collision. The same process is applied on the rest of the chunks until having decoded all the chunks of the colliding packets. The main advantage of this solution is its computability with the 802.11 MAC protocol.

6.3 Distributed Location-Aided (DLA) Algorithm

Hidden terminal problem is very likely to occur in wireless networks utilise carrier sense technique as the multiple access protocol. This is due to the position of the hidden stations that renders the detection of their transmission impossible. The hidden terminals are proven to cause a serious degradation to the network's performance because of the high packet collision experienced. In contrast, the time division multiple access protocol is more robust against this problem, which is because every wireless station is allocated a predefined time slot to access the channel, ensuring that one station is in a transmission state at a time. However, this type of protocol is subject to bandwidth waste and requires a scheduling algorithm that leads to a complicated process in multi-hop communication networks.

In this chapter, we propose the Distributed Location-Aided (DLA) algorithm to be applied to the 802.11 MAC to mitigate the hidden terminal problem and reduce its effects on the network's performance. According to DLA, every station knows its geographical position, which is also shared with its neighbours. Sharing the location information can be achieved by exchanging beacon frames, supported by most of the routing and MAC protocols. The core concept of DLA is to introduce time division into the carrier sense multiple access. This is achieved by dividing the radio range of the receiving wireless station (e.g. access point) into four zones (Figure 6-1), into which a time delay is introduced. Having done that, the time division will be applied to the four zones, while the carrier sense multiple access will be employed by the zones.

The zone delay is allocated by default in the following manner:

$$delay_{zone_1} = 0 \tag{6.1}$$

$$delay_{zone_2} = \partial \tag{6.2}$$

$$delay_{zone_3} = 2 * \partial \tag{6.3}$$

$$delay_{zone_4} = 3 * \partial \tag{6.4}$$

where ∂ is a delay unit.

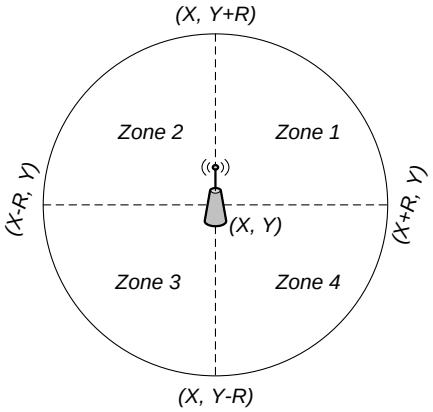

Figure 6- 1: The DLA partitioning concept

The stations within the same zone compete to access the wireless channel, while the stations of the other zones defer their transmission in order to reduce the simultaneous channel access probability. When a node has data to transmit, it defers its transmission by the correspondent zone delay, depending on the zone the station is located in, prior to the conventional carrier sense procedure specified in the IEEE standard. In addition, the zone delay unit must be greater than the time required to complete the transmission of a data frame and its associated ACK plus a SIFS interval.

$$\partial \tag{6.5}$$

Furthermore, DLA algorithm can be integrated into RTS/CTS scheme to further improve the network's performance and reduce the collision probability, especially, in 802.11 WLANs.

The proposed algorithm can also be applied in Wireless Sensor Networks (WSNs). It makes an alternative to the RTS/CTS method that is unsuitable for such networks [**3**], where the data frames are as small as the RTS/CTS packets, leading, therefore, to the same collision probability. Besides, the sensor device is a low power designed entity for which the energy efficiency is an essential factor to be considered. Therefore, by minimizing the transmission of control packets, the WSNs device battery lifetime can be increased.

6.4 Simulation tests and results analysis

DLA algorithm is implemented in OPNET modeller 14.5, which includes the complete implementation of the IEEE 802.11 MAC. We have modified the actual Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) protocol employed by the 802.11 MAC in order to support the Distributed Location-Aided algorithm. The modified MAC, referred as "LA-MAC" checks before accessing the wireless channel whether a zone back-off is required, depending on the position of the transmitting station (STA) in respect to the receiver. The virtual carrier sensing (RTS/CTS) mechanism is, therefore, supported by both CSMA/CA and DLA models.

The performance evaluation of the DLA algorithm is based on the simulation comparison among the CSMA/CA protocol, DLA algorithm, CSMA/CA with RTS/CST enabled and DLA algorithm with RTS/CTS enabled.

The simulation is based on the scenario shown in Figure 6-2. The scenario consists of one receiving node (AP) and a number of wireless stations grouped into four sets and distributed within the radio range of the AP, in a way that form hidden stations amongst the different groups of stations . The number of transmitters was varied from 3 STAs in each zone to 15 STAs. Moreover, the MAC and PHY layers parameters were configured to be conformant with the IEEE 802.11g (Extended rate PHY). The data rate was set to 24Mbps, the packet size to 1024 bytes and the traffic rate to 10 packets per seconds.

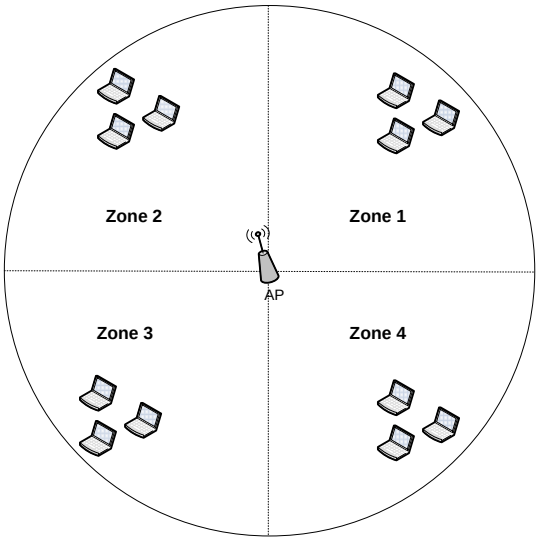

Figure 6- 2: The simulation scenario

A summary of the simulation parameters is given in Table 6-1 below

Table 6- 1: Summary of simulation parameters

Network Simulator	**OPNET^{TM} Modeler**	
Radio Range	97*m*	
MAC protocol	IEEE 802.11 g	
Data rate	24 Mbps	
Data traffic	Packet inter-arrival time	0.1 s
	Packet size	1024 bits
Simulation time	100s	
DLA zone delay 'Δ'	0.0005s	

The evaluation was considered using standard metrics including network throughput, end-to-end delay, retransmission and data drop defined as follows:

- ***Network throughput***: refers to total number of bits (in bits per second) forwarded from the wireless LAN MAC layer to the higher layer in all wireless nodes in the network.
- ***End-to-end delay***: represents the end-to-end delay introduced by all the packets received by the WLAN MACs of all the WLAN nodes in the network and forwarded to the higher layer.

- ***Retransmission***: refers to the total number of retransmission attempts by all WLAN MACs in the network until either the packet is successfully transmitted or is discarded as a result of reaching the short or long retry limit.
- ***The data drop***: refers to the total higher layer data traffic in bits/sec that is dropped by all the WLAN MACs in the network as a result of constant retransmission failure.

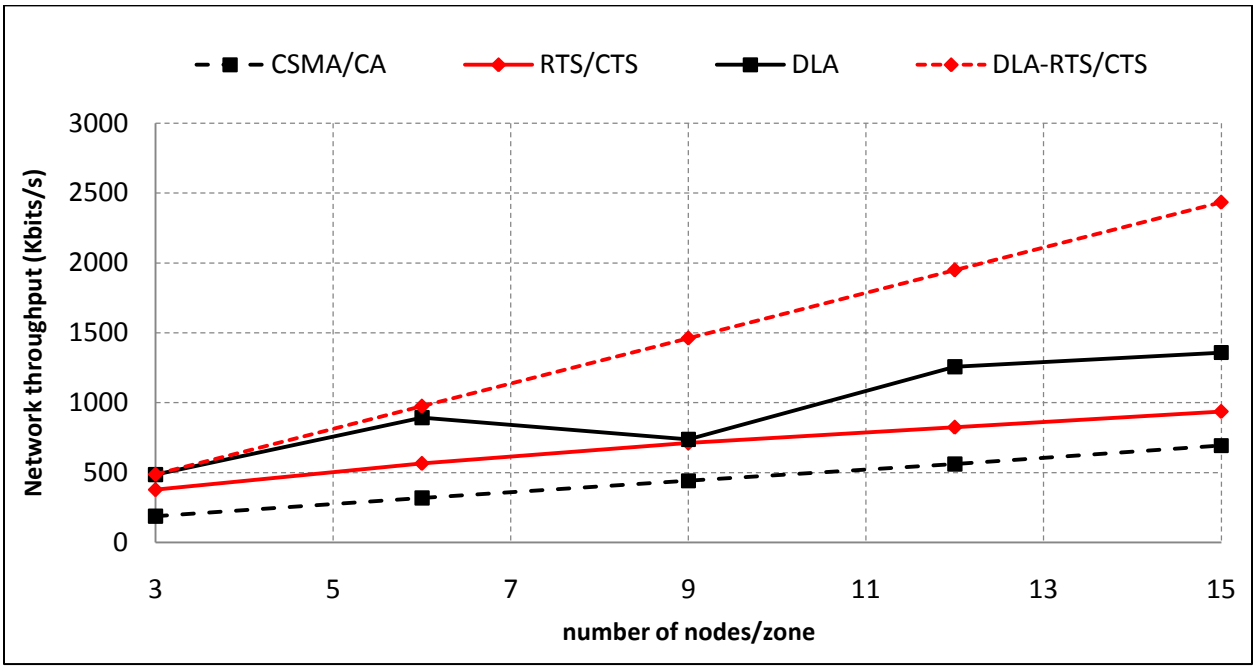

Figure 6- 3: The network throughput of the DLA algorithm and the CSMA/CA protocol

Figure 6-2 shows the network throughput of the evaluated methods. It clearly illustrates that DLA algorithm achieves higher throughput than CSMA/CA and RTS/CTS methods. As the number of nodes per zone increases, the collision probability increases, which in turn, decreases the network throughput. We can also observe that RTS/CTS method by employing an additional handshake process in order to reduce the effect of hidden terminals, fails to maintain the same level of network delivery ratio as the number of stations per zone increases. On the other hand, the standalone DLA algorithm reduces the occurrence of simultaneous data transmissions and consequently the probability of packet collisions, by introducing different time delays to the wireless stations prior to the carrier sensing and to the channel access. Furthermore, the remarkable result of this work is the considerable improvement of the

network's performance in terms of delivery ratio and retransmission attempts, when combining the DLA algorithm and the RTS/CTS handshake mechanism.

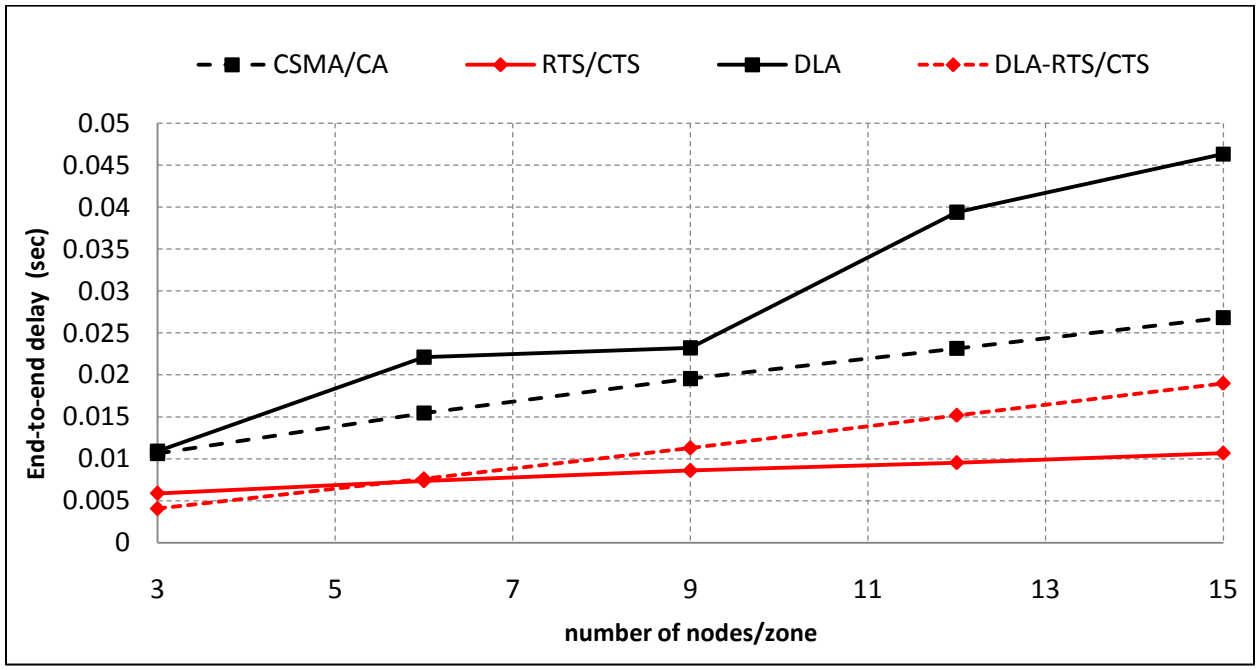

Figure 6- 4: The end-to-end delay of the DLA algorithm and the CSMA/CA protocol

In Figure 6-3, the end-to-end delay is presented, in which the standalone DLA reports the highest level of delay. A fraction of the network delay is explicitly introduced by the algorithm for the sake of enhancing the network's throughput. This increases the MAC's queuing delay of the data packets, which will have to wait in the transmission queue for a predefined time, in addition to the time the carrier sensing process requires. However, the main reason of the high network delay is the packet retransmission, illustrated in Figure 6-4, that occurs after a collision is detected or when the ACK reception timer runs out. Prior to the retransmission attempt, the wireless station sets a back-off timer and proceeds with the carrier sensing process when that runs out, resulting, therefore, to an increase in the end-to-end delay.

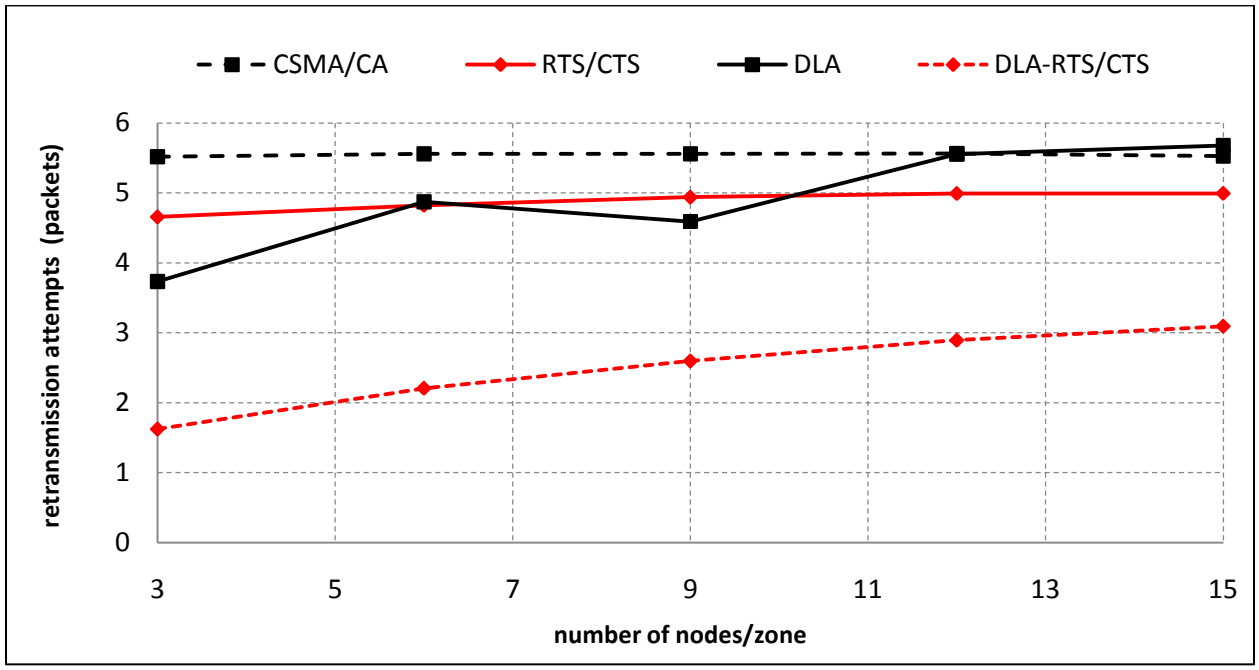

Figure 6- 5: The retransmission attempts of the DLA algorithm and the CSMA/CA protocol

Figure 6-5 shows the data traffic in (Kbits/s) discarded by the MAC layer after exceeding the threshold of transmission attempts. Standalone DLA shows low rate of data drop as compared to those of CSMA/CA and RTS/CTS methods. Moreover, the low rate of the standalone DLA becomes negligible when applying RTS/CTS method as demonstrated in Figure 6-6.

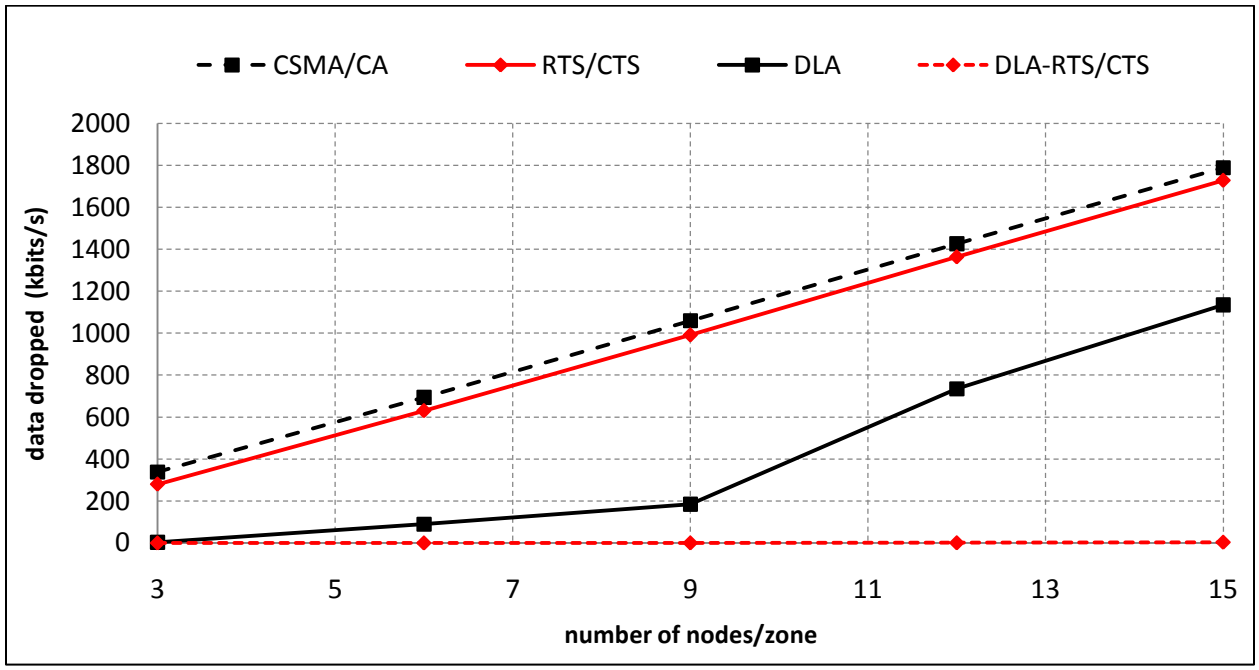

Figure 6- 6: The data dropped by the MAC layer of the DLA algorithm and the CSMA/CA protocol

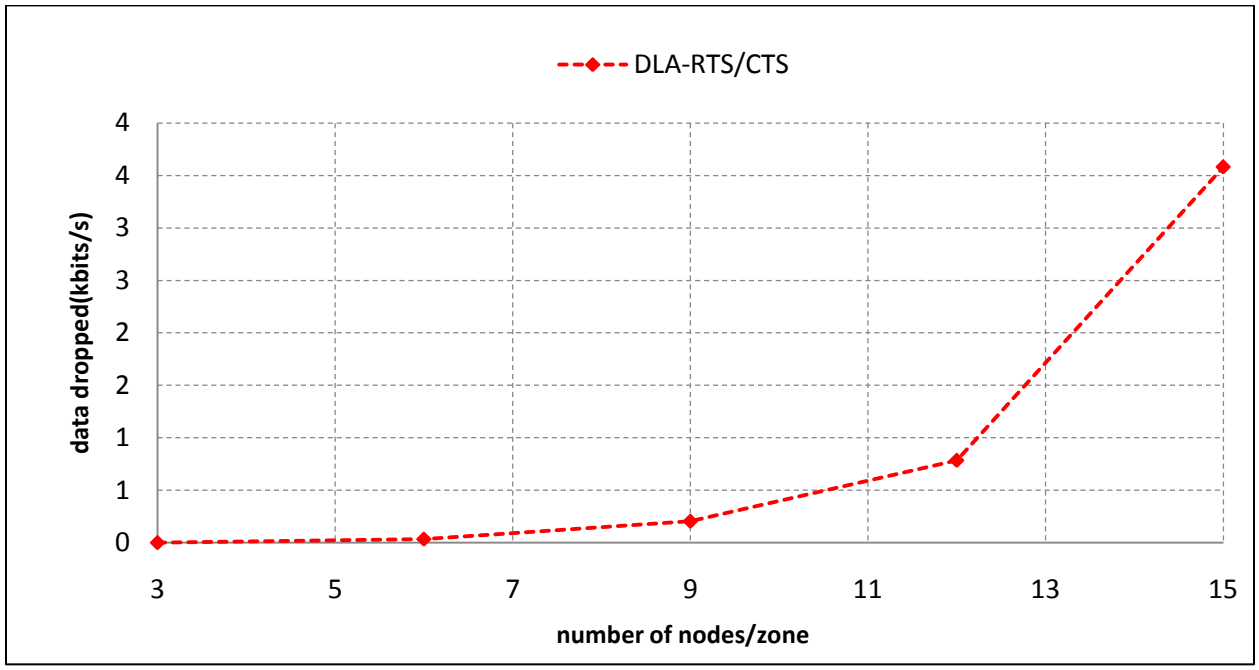

Figure 6- 7: The data dropped by the MAC layer of the DLA algorithm with RTS/CTS enabled

Eventually, DLA algorithm has showcased an important performance and has shown a significant improvement to the network's throughput as compared to the basic CMSA/CA and the RTS/CTS methods. However, the remarkable results came with the integration of the DLA algorithm and the RTS/CTS (DLA-RTS/CTS) that appeared to achieve the best performance and considerably mitigated the effects of the hidden terminal problem.

6.5 Conclusion

This chapter presented a Location-Aided MAC (LA-MAC), which relies on Distributed Location-Aided Algorithm (DLA) to mitigate the effect of hidden terminals. The proposed DLA algorithm made use of the positions of the wireless station and divided the receiver's radio range into four zones, upon which different time delays were assigned. Any station willing to access the wireless channel had to defer its attempt, according to the zone's to which it belonged, prior to the carrier sensing process. The delay allocation and the zone priority were considered to be static. The first zone with the highest priority had no additional delay assigned and, therefore, the basic CSMA/CA was applied. In the rest three zones, different delays were allocated, which were multiples of the zone's delay unit parameter.

The proposed LA-MAC was compared to the basic CSMA/CA and the RTS/CTS mechanisms and the simulation tests showed the improvement to the network's throughput when DLA algorithm was applied. However, the remarkable finding of this work was the important performance, in terms of network throughput and retransmission attempts, achieved by the LA-MAC, when the RTS/CTS mechanism was enabled. Eventually, the integration of DLA algorithm to RTS/CTS mechanism demonstrated its significant reduction of the effects of hidden terminals on the wireless networks' performance.

References

[1] "IEEE Standard for Information technology-Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," IEEE Std 802.11-2007 (Revision of IEEE Std 802.11-1999) ,pp.C1-1184, June 2007.

[2] P. Chatzimisios, A.C. Boucouvalas and V. Vitsas, “Effectiveness of RTS-CTS handshake in IEEE 802.11a Wireless LANs”, Electronics Letters, pp. 915 - 916 , 2004.

[3] P. C. Ng, S. C. Liew, K. C. Sha and W. T. To, “Experimental Study of Hidden-node Problem in IEEE802.11 Wireless Networks”, In Sigcomm Poster, 2005.

[4] S. Ray, D. Starobinski, and J. B. Carruthers, “Performance of wireless networks with hidden nodes: A queuing-theoretic analysis,” Computer Communications, Vol. 28, pp. 1179–1192, 2005.

[5] S. Ray, J. Carruthers, and D. Starobinski, “Evaluation of the masked node problem in ad-hoc wireless LANs,” IEEE Trans. Mobile Computing., Vol. 4, pp. 430–442, 2005.

[6] Li B. Jiang, Soung C. Liew, “Improving Throughput and Fairness by Reducing Exposed and Hidden Nodes in 802.11 Networks “, IEEE Transactions on Mobile Computing, Vol. 7, No. 1, pp. 34-49, 2008.

[7] A. Tobagi and L. Kleinrock, “Packet switching in radio channels: Part II—The hidden terminal problem in carrier sense multiple-access and the busy-tone solution,” IEEE Trans. Commun., Vol. 23, pp. 1417–1433, 1975.

[8] C. S. Wu and V. O. K. Li, “Receiver-initiated busy-tone multiple access in packet radio networks,” in Proc. ACM Workshop on Frontiers in Comput. Commun. Technol., Stowe, Vermont, pp. 336–342, 1987.

[9] Z. J. Haas and J. Deng, “Dual busy tone multiple access (DBTMA)—A multiple access control scheme for ad hoc networks,” IEEE Transactions on Communications, Vol. 50, pp. 975–985, 2002.

[10] Chandra, V. Gummalla, and J. O. Limb, “Wireless collision detect (WCD): Multiple access with receiver initiated feedback and carrier detect signal,” in Proceedings of IEEE International Conference on Communications, pp. 397–401, 2000.

[11] Ji, “Asynchronous wireless collision detection with acknowledgement for wireless mesh networks,” in Proc. IEEE Veh. Technol. Conf., Vol. 2, pp. 700–704, 2005.

[12] H. Yeh, “New Busytone Solutions to Medium Access Control inWireless Mesh, Ad Hoc, and Sensor Networks ”, IEEE International Conference on Communications (ICC '07), pp. 3841 – 3846, 2007.

[13] A. Tobagi and L. Kleinrock, “Packet switching in radio channels: Part III—Polling and (dynamic) split channel reservation multiple access,” IEEE Transactions on Communications, Vol. 24, No. 7, pp. 832–845, 1976.

[14] P. Karn, “MACA—A new channel access method for packet radio,” in Proc. 9th ARRL/CRRL Amateur Radio Comput. Netw. Conf., pp. 134–140, 1990.

[15] V. Bharghavan, A. Demers, S. Shenker, and L. Zhang, “MACAW: A media access protocol for wireless LAN’s,” in Proc. ACM SIGCOMM, London, U.K., pp. 212–225, 1994.

[16] C. L. Fullmer and J. J. Garcia-Luna-Aceves, “Floor acquisition multiple access (FAMA) for packet-radio networks,” in Proc. ACM SIGCOMM, pp. 262–273, 1995.

[17] C. L. Fullmer and J. J. Garcia-Luna-Aceves, “Solutions to hidden terminal problems in wireless networks,” in Proc. ACM SIGCOMM, Cannes, France, pp. 39–49, 1997.

[18] Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, ISO/IEC IEEE-802-11, IEEE Standard for Information Technology, 1999.

[19] Colvin, “CSMA with collision avoidance,” Computer Commun., Vol. 6, No. 5, pp. 227–235, 1983.

[20] Y. Yang, F. Huang, X. Ge, X. Zhang, X. Gu, M. Guizani, and H. Chen, “Double sense multiple access for wireless ad-hoc networks,” Int. J. Comput. Telecomm. Netw., Vol. 51, No. 14, pp. 3978–3988, 2007.

[21] T. Han and W. Lu, “An Improvement of MACA in Alleviating Hidden Terminal Problem in Adhoc Networks”, International Conference on Wireless Communications, Networking and Mobile Computing (WiCom), pp. 1-4, 2009.

[22] [18] l. Deng, B. Liang and P. K. Varshney, “Tuning the Carrier Sensing Range of the IEEE 802.11 MAC”, IEEE Global Telecommunications Conference (GLOBCOM), Vol. 5, pp. 2987-2991, 2004.

[23] E. Haghani, M. N. Krishnan, A. Zakhor, ”Adaptive Carrier-Sensing for Throughput Improvement in IEEE 802.11 Networks”, IEEE Global Telecommunications Conference (GLOBECOM), pp. 1-6, 2010.

[24] A. Ho and S. Liew, “Impact of Power Control On Performance of IEEE 802.11 Wireless Networks”, IEEE Transactions on Mobile Computing, Vol. 6, No. 11, 2007.

[25] L. Hwang, “Grouping strategy for solving hidden node problem in IEEE 802.15.4 LR-WPAN,” in Proc. IEEE 1st Int. Conf. Wireless Internet (WICON’05), Budapest, Hungary, pp. 26–32, 2005.

[26] Woo-Yong Choi, “Clustering Algorithm for Hidden Node Problemin Infrastructure Mode IEEE 802.11 Wireless LANs”, 10th International Conference on Advanced Communication Technology, ICACT, pp. 1335-1338, 2008.

[27] Koubâa, R. Severino, M. Alves, E. Tovar “Improving Quality-of-Service in Wireless Sensor Networks by Mitigating Hidden-Node Collisions”, IEEE Transactions on Industrial Informatics, Vol. 5, No. 3, pp. 299 – 313, 2009.

[28] D. Halperin, J. Ammer, T. Anderson, and D. Wetherall, “Interference cancellation: Better receivers for a new wireless MAC,” in Proc. Hotnets, pp. 339–350, 2007.

[29] D. Halperin, T. Anderson, and D. Wetherall, “Taking the sting out of carrier sense: Interference cancellation for wireless LANs,” in Proc. ACM MobiCom’08, pp. 339–350, 2008.

[30] S. Gollakota and D. Katabi, “Zigzag decoding: Combating hidden terminals in wireless networks,” in Proc. ACM SIGCOMM, pp. 159–170, 2008.

Chapter 7

Conclusions and Future Work

This thesis touched on Mobile Ad-Hoc Networks (MANETs) and IEEE 802.11 MAC, where several challenges and issues were identified for further research. The various routing and MAC approaches and design strategies in the existing literature have been discussed in detail. The impact of the nodes' mobility on the routing performance, mainly in terms of packet deliverability, was a focus of this work, which served as an opportunity to present the model design and specification of our proposed protocol. To widen the scope of the research, we discussed the effects of the Hidden Terminal problem in the network and the MAC layers' performance, which frequently occurs in MANETs. Accordingly, two techniques that rely on the nodes' position were then proposed to improve the routing protocol and the MAC layer's performance in hidden-terminal scenarios. Finally, after various methods of estimating the link lifetime amongst mobile nodes were studied, a link lifetime estimation method that focuses on the characteristics of greedy forwarding is further proposed.

The main challenges addressed in this thesis as well as the proposed solutions are presented in the following sections.

7.1 Design of Routing and MAC protocols

7.1.1 FORTEL

The principal feature of MANETs is mobility support that allows the mobile nodes to move freely within the network geographical area. The nodes' movement varies in speed and

pattern, which causes links and routes disconnections that, in turns, can significantly degrades the employed routing protocol's performance. Furthermore, link information is highly sensitive to the nodes' mobility and requires frequent updates to maintain the connectivity of the active routes. Link information reflects the network topology at a specific time and becomes invalid when any changes occur, in contrast to the outdated location information that can be used to predict a future position.

In this thesis, FORTEL, a new position-based source routing protocol is proposed to increase routing efficiency in mobile scenarios. Each node has a global knowledge of the network by storing the location information of all the nodes in a Location Table. FORTEL uses the nodes' location information to predict the network's topology and compute end-to-end routes between source and destination peers. Its adaptation and robustness to mobility is derived from its forecasting mechanism of predicting the future state of the network's topology and adjusting the route selection mechanism accordingly. The route with the lowest hop count is constructed using a modified version of Dijkstra algorithm, which is designed to obtain the k-possible routes to the desired destination. Two location update schemes were integrated to FORTEL to disseminate the changes throughout the network. The first update is based on changes in the mobility speed and pattern, whereas in the second, the updates are transmitted periodically at a predefined rate. A third update scheme, named window update scheme is also proposed, which combines the two previous schemes to increase the accuracy of the protocol.

The main features of FORTEL can be summarised in the following points:

- Geographical Source routing: the data packets are embedded within the end-to-end route and, therefore, the intermediate nodes will only need to relay the packet following the route.
- Topology forecasting and route construction: FORTEL forecasts the network's topology prior for any attempt of transmitting packets. This practice increases the protocol's efficiency against the link breakages and network disconnections.

- Multiple routes to the destination: FORTEL route computation function determines multiple routes to the desired destination, while the lowest route in terms of hop count, is selected for data transmission. Moreover, changing FORTEL's selection metric to the shortest path or to any other routing metric is a simple process.
- "Hello" messages/location update switching mechanism: "Hello" messages are the base of all routing protocols in MANETs and they periodically transmitted within the single hop neighbourhood. Despite its small size, the frequent transmission of "Hello" messages increases the overhead as well as the delay, consumes power and requires bandwidth that can be allocated for data exchange. The switching mechanism to enable/disable the Hello transmission according to the mobility status of the node.
- The design of FORTEL protocol allows for an easy integration of QoS parameters (such as queuing, transmission, and contention delay and data rate) to the route selection process.

In addition, different versions of FORTEL have been discussed and studied corresponding to the previously mentioned update schemes. The simulation tests have shown that the version FORTEL, which employs the proposed window update scheme, achieves the highest routing performance. Finally, the comparison of FORTEL against AODV, DSR and OLSR protocols demonstrates the effectiveness of FORTEL, in mobile scenarios, in terms of delivery rate, routing overhead and network delay.

7.1.2 Suppression Mechanism for Beaconless Routing

Beaconless routing approach has proven its significance in Mobile Ad-Hoc Networks (MANETs) as well as in Vehicular Ad-Hoc Networks (VANETs). The fundamental of this approach is that it does not require any sort of information for data routing, eliminating therefore, all the consequences in terms of overhead, packets collisions and channel contention. On the other hand, beaconless routing schemes suffer from packet duplication and message redundancy, which are caused by the hidden nodes during the contention process.

In this thesis, a suppression mechanism was presented to eliminate the problem of packet duplication in beaconless routing. According to that, the forwarding zone of the sender is divided into three zones of Reuleaux triangle and a different time delay is assigned to each zone. The advantage of using Reuleaux triangle is that the nodes within that area can hear each other's transmission. Furthermore, the delay assigned to the zone is added to the contention timer, set by the receiver, to form the total time that it has to wait before responding to the sender's transmission. Following the first transmission, the sender will then interfere by broadcasting an announcement packet to force the nodes with active timers to cancel their scheduled transmission. The proposed scheme was integrated with the Contention-Based Forwarding (CBF) and compared to the Area-based suppression technique. The simulation results have shown considerable improvement in terms of the network effective throughput.

7.1.3 Design of a Link Lifetime Estimation Method

There are several methods for estimating the lifetime of a link between two nodes, which differ in the information utilised to perform the estimation. One of those methods makes use of the location information such as position, speed and movement direction, of the nodes composing the link to estimate the link lifetime. Besides, greedy forwarding approach follows the concept of delivering the packet to the closest neighbour to the destination. Thus, only a set of nodes that are located within a specific area, called "greedy area", will participate in the selection process of the next hop forwarder. The conventional estimation method that uses the location information does not consider the special characteristics of the greedy schemes and assumes that the link is active as long as the nodes are within the radio range of each other.

In this thesis we presented a novel link lifetime estimation method, specifically designed for greedy forwarding. The proposed method estimates the link lifetime based on the location information the nodes composing the link as well as that of the destination node. Accordingly, the link is considered to be available as long as the neighbour is within the greedy area of the sender. A Stability-Aware Greedy (SAG) scheme is then proposed that employs a combined link lifetime and distance metric to select the appropriate neighbour that will forward the packet towards the destination. Both the conventional and proposed link lifetime estimation methods

are applied on SAG to evaluate their impact on the routing performance. The simulations have shown that the delivery ratio of SAG is significantly higher when the proposed estimation method is applied, in addition to the outperformance achieved in terms of network delay and packet retransmission.

7.1.4 Design of a Location-Aided MAC protocol

Hidden terminal problem is reported to significantly degrade the network's throughput and increase the packet retransmission in 802.11 wireless networks. The hidden terminals are not able to detect each other's transmissions, so they attempt to access the wireless channel even if a transmission is taking place. This phenomenon leads to packet collisions, after which the nodes have to go through a backoff process to schedule a retransmission. RTS/CTS mechanism was proposed to solve the earlier mentioned problem by exchanging control packets prior to data transmission. However, this mechanism fails to eliminate the hidden terminals and can further degrade the network's performance by introducing additional overhead.

In the current thesis, a Location-Aided MAC (LA-MAC) protocol was presented, which is based on the Distributed Location-Aided Algorithm (DLA), proposed to mitigate the effect of hidden terminals. DLA makes use of the nodes' positions, according to which the receiver's radio range is partitioned into four zones. Static delays have been allocated to the zones, which define the period that a node has to wait before sensing the wireless channel. The delay allocation and the zone priority are considered to be static. The first zone with the highest priority has no additional delay assigned, and therefore, the basic CSMA/CA is applied. In the rest three other zones, different delays are allocated, which are multiple of a predefined zone delay unit parameter. LA-MAC can be considered as an integration of the time division multiple access to the carrier sense collision avoidance protocol. While the nodes within the same zone compete among each other to access the medium using the carrier sensing mechanism, the inter-zone access is further controlled by time division. The DLA algorithm has been integrated with the IEEE 802.11 MAC and the simulations have shown its outperformance over both CSMA/CA and RTS/CTS, in terms of throughput. However, the remarkable findings of this thesis came about when the DLA algorithm and the RTS/CTS were combined. The results have shown that DLA

with RTS/CTS have significantly increased the network's performance, in terms of network throughput and retransmission attempts.

7.2 Directions of future work

7.2.1 Thesis' future research

Several issues and unsolved problems in the research of this thesis require further study. The future research is outlined as follows:

7.2.1.1 Improving FORTEL protocol

1. FORTEL's routing, in the current thesis is designed for obstacle-free ad-hoc networks. Therefore, it is assumed that there is some sort of communication between two mobile nodes as long as they are within the transmission range of each other, which is a quit common assumption in MANETs' geographical routing. However, in real scenarios, natural obstacles such as trees, buildings and tunnels may exist and prevent two nearby mobile nodes to communicate, imposing a serious challenge on FORTEL's functionality. Given that, one of the tasks that we are determined to work on in the future is addressing FORTEL's performance in real scenarios. This can be achieved by applying the obstacle detection mechanism that allows FORTEL to identify whether two nearby nodes are able to communicate.
2. FORTEL's route computation algorithm is based on the nodes' positions that are represented by their (X, Y) coordinates. Besides, a principal factor that influences the frequency of the location updates is the variation of the nodes' location information that can be considerably high in mobile scenarios, especially when considering VANETs. Therefore, modifying the route computation algorithm to rely on a region (circle) rather than the nodes' position (point (x, y)) could improve the protocol's efficiency and eliminate the straight line movement constraint. The region is an area, where the node is expected to be at a specific time, represented by a disc centred at the node's position, while the radius is the distance covered during time $\Delta t = t_1 - t_0$, where t_0 is the time at which the position update was received and t_1 is the time to transmit a packet.
3. Hardware implementation of FORTEL and experimental testbed.

7.2.1.2 Developing a stability-based beaconless routing protocol

4. An important challenge that the sender suppression mechanism has to face is to ensure that the sender will broadcast the announcement packet before packet duplications occur. This challenge will be addressed in a future work, by further investigating the delay function used by the receivers to set up their contention timers.
5. According to the proposed sender suppression mechanism, the sender intervenes in the contention process by transmitting an announcement packet to suppress the receivers with active timer. This additional overhead, caused by the announcement packets, could be further reduced by designing a beaconless scheme featured with link stability metric. Accordingly, the receiver that first responds to the sender's transmission will be selected for a period of time, enough to forward a batch of packets.

7.2.1.3 Enhancing the Location-Aided MAC

6. The zone partitioning in the Location-aided MAC could be further investigated. Besides, the fixed delays assigned to the zones may cause channel access fairness and bandwidth waste issues, as it may be the case that one of the sectors does not include wireless stations or one zone is more congested than another. Therefore, a dynamic delay allocation algorithm should be designed to ensure that access to the wireless medium is fairly granted to all the different zones.

7.2.2 Other research work

The research that has not been addressed in this thesis that will be carried out includes the design of a green routing platform for Highly Dense Mobile Ad-Hoc Networks (MANETs) to increase energy efficiency and reduce power consumption. The platform introduces a novel concept of routing based on heterogeneous multi-radio interfaces, where the network traffic is split over different radio interfaces. The routing control traffic is transmitted using low power radio technology (e.g. UWB), while the data packets are sent over the 802.11 interface. Following the analytical analysis, a practical model is planned to be designed, in order to evaluate the performance of the proposed platform using simulation tests as well as testbed experiments if possible.

The design and modelling phase includes the following tasks:

- Definition of the specifications of the proposed platform.
- Design of a virtual layer between the network and the MAC layers to manage the incoming and outgoing traffic to and from the wireless node, according to the platform specifications.
- Modification of a MANET routing protocol to include multi-interface support feature and handle the interaction with the designed virtual layer.
- Implementation of the design in OPNET simulator and evaluation its performance through different network scenarios, while comparing the results with the single radio routing.
- Definition of the testbed specifications and the experiment plan.

Appendix A: FORTEL route computation function

```
List* construct_route_list(PrgT_String_Hash_Table* destination_table, InetT_Address
my_address, InetT_Address destination,  double src_lat, double src_long)
{
int                         index,i,j,s;
InetT_Address*              temp_dest;
InetT_Address*              temp;
List*                       dest_list;
double                      result;
list_struct*                route;
list_struct*                r;
List*                       route_list;
Boolean                     FOUND;
Boolean                     FFOUND;
List*                       table_list;
Fortel_Dest_Info*           node_ptr;
InetT_Address*              tt;
InetT_Address*              ttemp;
int                         level;
List*                       node_list;
int                         counter;
double                      lifetime;

FIN(construct_route_list(<args>));

table_list = prg_list_create();
route_list = prg_list_create();
dest_list= prg_list_create();
node_list = prg_list_create();

table_list = (List*) prg_string_hash_table_values_get (destination_table);

node_list = append_list(destination_table, my_address, destination,src_lat, src_long);

level = 1;
temp_dest = (InetT_Address*)prg_mem_alloc(sizeof (InetT_Address));
*temp_dest = inet_address_copy(destination);
prg_list_insert(dest_list, temp_dest,OPC_LISTPOS_HEAD);
index = 0;
counter = 0;
do
{
if (index == level)
       {
       delete_list(dest_list, node_list, level, prg_list_size(dest_list));
       level = prg_list_size(dest_list);
       }
temp_dest = (InetT_Address*)prg_list_access(dest_list, index);
for(i= 0; i< prg_list_size(node_list);i++)
{
node_ptr = (Fortel_Dest_Info*) op_prg_list_access (node_list, i);
if (inet_address_equal (node_ptr->dest_addr, *temp_dest))
       continue;

if (inet_address_equal(node_ptr->dest_addr,my_address))
       result = alculate_distance_to_src(table_list, *temp_dest, src_lat, src_long);

else
```

```
	result = calculate_distance(table_list, node_ptr->dest_addr,node_ptr-
	>dest_lat,node_ptr->dest_long, *temp_dest);

lifetime =   calculate_link_lifetime (table_list, node_ptr->dest_lat,node_ptr-
>dest_long, node_ptr->dest_speed , node_ptr->dest_direction, *temp_dest);
if(result <= RADIO_RANGE)
	{
	counter ++;
	if(OPC_FALSE == inet_address_equal(node_ptr->dest_addr, my_address))
		{
		FOUND = OPC_FALSE;
		for(s= 0; s< prg_list_size(dest_list);s++)
		{
		tt = (InetT_Address*) op_prg_list_access (dest_list, s);
		if(inet_address_equal(*tt, node_ptr->dest_addr))
			FOUND= OPC_TRUE;
		}

		if(FOUND == OPC_FALSE)
		{
		temp = (InetT_Address*)prg_mem_alloc(sizeof(InetT_Address));
		*temp = node_ptr->dest_addr;
		prg_list_insert(dest_list,temp,OPC_LISTPOS_TAIL);
		}
		}

		temp = (InetT_Address*)prg_mem_alloc(sizeof(InetT_Address));
		*temp = node_ptr->dest_addr;

		if(inet_address_equal(*temp_dest, destination))
			{
			r =(list_struct*)prg_mem_alloc(sizeof (list_struct));
			r->list = prg_list_create();
			r->metric = result;
			r->lifetime = lifetime;
			ttemp = (InetT_Address*)prg_mem_alloc(sizeof(InetT_Address));
			*ttemp = *temp_dest;
			prg_list_insert(r->list, ttemp,OPC_LISTPOS_TAIL);
			prg_list_insert(r->list, temp,OPC_LISTPOS_TAIL);
			prg_list_insert(route_list,r,OPC_LISTPOS_TAIL);
			}
		else
			{
			for(j=0;j<prg_list_size(route_list);j++)
			{
			route = (list_struct*) op_prg_list_access (route_list, j);
		ttemp = (InetT_Address*)prg_list_access(route->list,OPC_LISTPOS_TAIL);

		if(inet_address_equal(*ttemp,*temp_dest))
			{
			FFOUND = OPC_FALSE;
			for(s = 0;s< prg_list_size(route->list);s++)
				{
				tt = (InetT_Address*) op_prg_list_access (route->list, s);
				if(inet_address_equal(*tt,*temp))
					FFOUND= OPC_TRUE;
				}
			if(FFOUND == OPC_FALSE)
				{
				r = (list_struct*)prg_mem_alloc(sizeof (list_struct));
				r->list = prg_list_create();
				copy_list_int(route->list,r->list,0);
			prg_list_insert(r->list, temp ,OPC_LISTPOS_TAIL);
```

```
                        r->metric = route->metric + result;
                        if(lifetime < route->lifetime)
                                r->lifetime = lifetime;
                        else
                                r->lifetime = route->lifetime;

                        prg_list_insert(route_list,r,OPC_LISTPOS_HEAD);
                        j++;
                        }
                      }
                    }
                  }
                }
        delete_routes(*temp_dest, route_list);
        index ++;
        }
        while(index < prg_list_size(dest_list));

        free_list(table_list, node_list, dest_list);

        FRET(route_list);
        }
-------------------------------------------------------------------------------------------

double calculate_distance_to_src(List* node_list, InetT_Address a, double
src_lat,double src_long)
        {
        double          lat1,long1, xres, yres;
        double          result;
        Objid           node_objid;

        FIN(calculate_distance_to_src(<args>));

        for(i = 0;i<prg_list_size(node_list);i++)
                {
                node =(Fortel_Dest_Info*) prg_list_access(node_list,i);
                if(inet_address_equal(node->dest_addr, a))
                        {
                        long1 = node->dest_long;
                        lat1  = node->dest_lat;
                        break;
                        }
                }
        xres = ((lat1 - src_lat) * (lat1 - src_lat));
        yres = ((long1 - src_long) * (long1 - src_long));
        result = sqrt(xres + yres);

        FRET(result);
        }

-------------------------------------------------------------------------------------------

void copy_list(List*a,List*b, int index)
        {
        int             i;
        link_struct*  temp;

        FIN(copy_list(List*a,List*b, int index));

        for(i=index;i<prg_list_size(a);i++)
                {
```

```
		temp = (link_struct*)prg_list_access(a,i);
		prg_list_insert(b,temp,OPC_LISTPOS_TAIL);
		}

	FOUT;
	}

-------------------------------------------------------------------------------

static void copy_list_int(List* list1,List* list2, int index)
	{
	int			i;
	InetT_Address*		temp;
	InetT_Address*		copy_temp;

	FIN(copy_list_int(List* list1,List* list2, int index));

	for(i=index;i<prg_list_size(list1);i++)
		{
		temp = (InetT_Address*)prg_list_access(list1,i);
		copy_temp = (InetT_Address*)prg_mem_alloc(sizeof(InetT_Address));
		*copy_temp = *temp;
		prg_list_insert(list2,copy_temp,OPC_LISTPOS_TAIL);
		}
	inet_address_destroy(*temp);
	inet_address_destroy(*copy_temp);

	FOUT;
	}

-------------------------------------------------------------------------------

List* append_list(PrgT_String_Hash_Table* destination_table, InetT_Address my_address,
InetT_Address destination, double x, double y)
	{
	int			count, num_keys;
	Fortel_Dest_Info*	node_ptr;
	Fortel_Dest_Info*	node;
	List*			list;
	List*			keys_lptr;
	char*			key_ptr;

	FIN(<args>));

	list = prg_list_create();

	node_ptr = (Fortel_Dest_Info*)prg_mem_alloc(sizeof(Fortel_Dest_Info));
	node_ptr->dest_addr = my_address;
	node_ptr->dest_long = y;
	node_ptr->dest_lat  = x;
	prg_list_insert(list,node_ptr,OPC_LISTPOS_HEAD);

	keys_lptr = prg_string_hash_table_keys_get (destination_table);
	num_keys = op_prg_list_size (keys_lptr);

	for (count = 0; count < num_keys; count++)
		{
		key_ptr = (char*) op_prg_list_access (keys_lptr, count);
		node_ptr = (Fortel_Dest_Info*) prg_string_hash_table_item_get
		(destination_table, key_ptr);
		if(OPC_FALSE == inet_address_equal(node_ptr->dest_addr, destination))
			{
```

```
                    node = (Fortel_Dest_Info*)prg_mem_alloc(sizeof(Fortel_Dest_Info));
                    node->dest_addr = node_ptr->dest_addr;
                    node->dest_long = node_ptr->dest_long;
                    node->dest_lat  = node_ptr->dest_lat;
                    prg_list_insert(list,node,OPC_LISTPOS_TAIL);
                    }
             }

      inet_address_destroy (node_ptr->dest_addr);
      op_prg_mem_free (node_ptr);
      FRET(list);
      }

--------------------------------------------------------------------------------

void  delete_routes(InetT_Address adr, List* l)

      {
      int                  i,index;
      list_struct*  r;
      InetT_Address*       intptr;

      FIN(delete_routes(InetT_Address adr, List* l));

      index = 0;
      while (index < prg_list_size(l))
             {
             r =  (list_struct*)prg_list_access(l,index);
             intptr = (InetT_Address*)prg_list_access(r->list,OPC_LISTPOS_TAIL);
             if(inet_address_equal(*intptr, adr))
                    {
                    r =  (list_struct*)prg_list_remove(l,index);
                    for (i = 0; i < prg_list_size(r->list); i++)
                           {
                           intptr = (InetT_Address*)prg_list_remove(r-
                           >list,OPC_LISTPOS_HEAD);
                           inet_address_destroy (*intptr);
                           op_prg_mem_free (intptr);
                           }
                    prg_mem_free(r);
                    }
             else
                    index ++;
             }
      FOUT;
      }

--------------------------------------------------------------------------------
```

Appendix B: LA-MAC Results

In this appendix, the performance of LA-MAC is evaluated while modifying the data traffic parameters. The modified simulation parameters are given in Table B-1.

Table B- 1: Summary of simulation parameters

Network Simulator	**OPNET™ Modeler**	
Radio Range	97*m*	
MAC protocol	IEEE 802.11 g	
Data rate	24 Mbps	
Data traffic	Start time	Uniform [5,15]
	Packet inter-arrival time	Exponential (0.1)
	Packet size	1024 bits
Simulation time	10 minutes	
DLA zone delay 'Δ'	0.0005s	

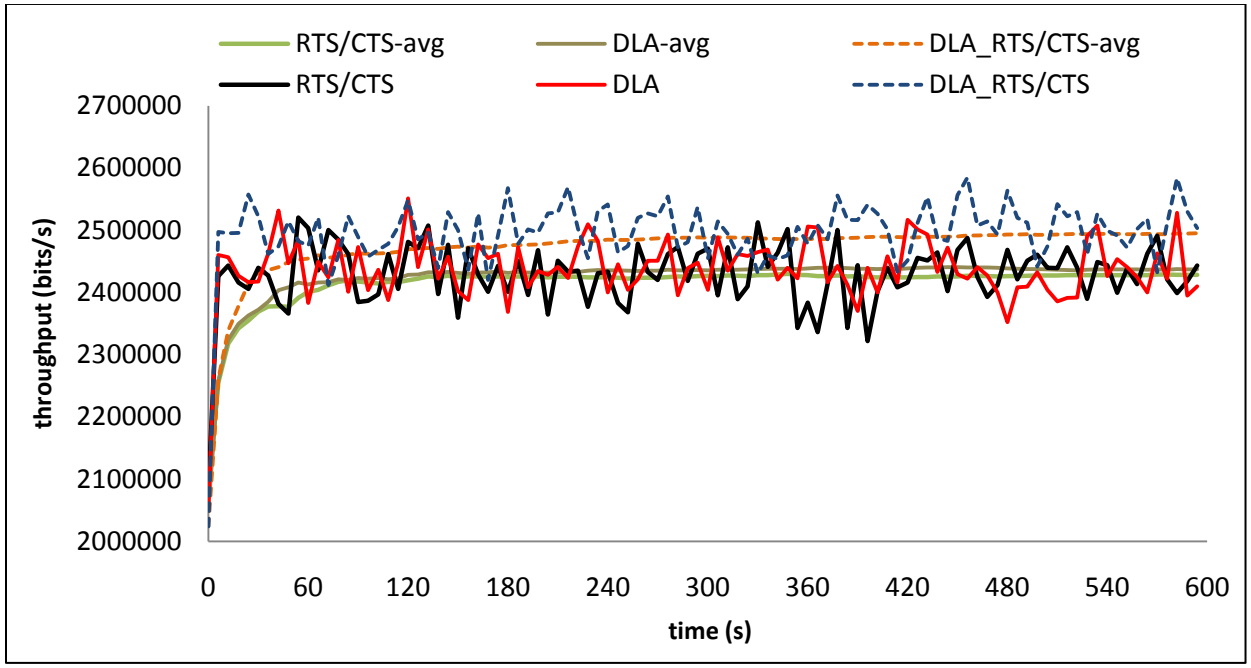

Figure B- 1: The network throughput in bits/s of the DLA algorithm and the CSMA/CA protocol

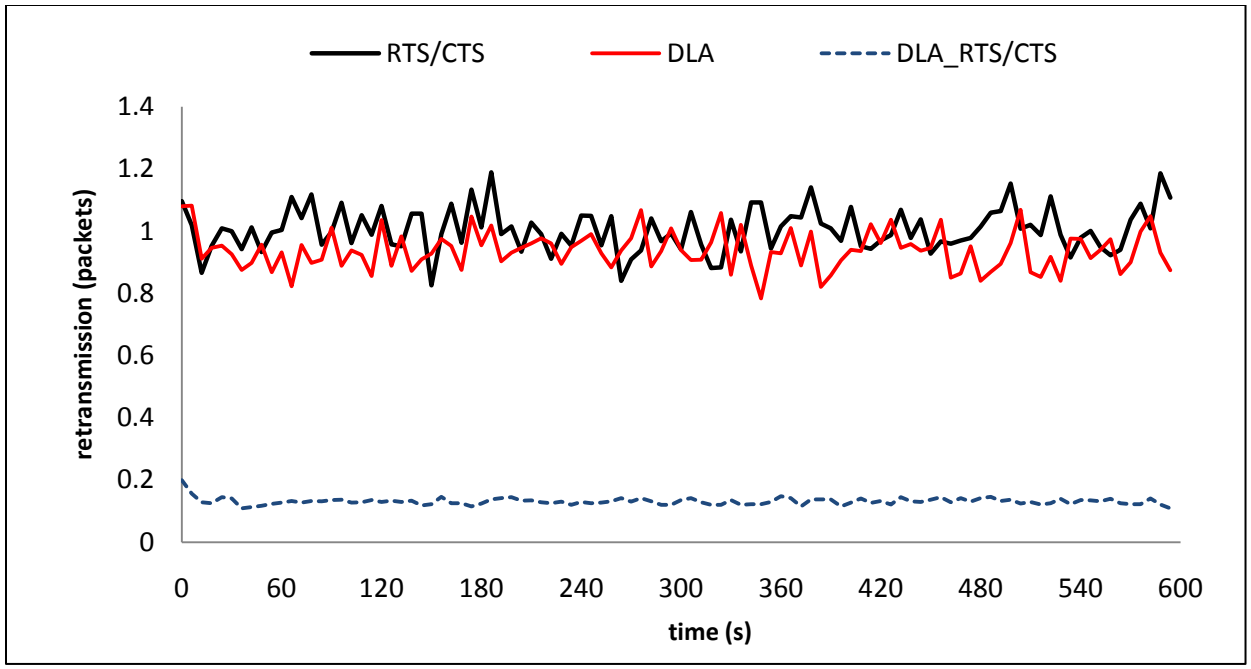

Figure B- 2: The retransmission attempts in packets of the DLA algorithm and the CSMA/CA protocol

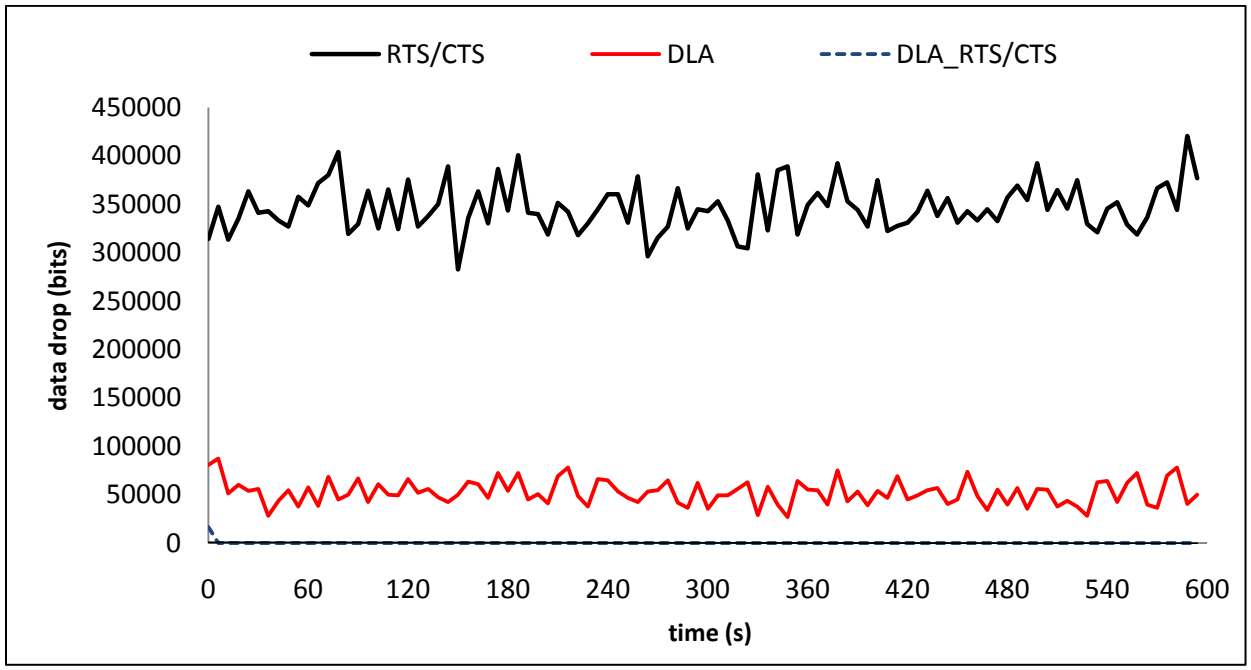

Figure B- 3: data drop in bits of the DLA algorithm and the CSMA/CA protocol

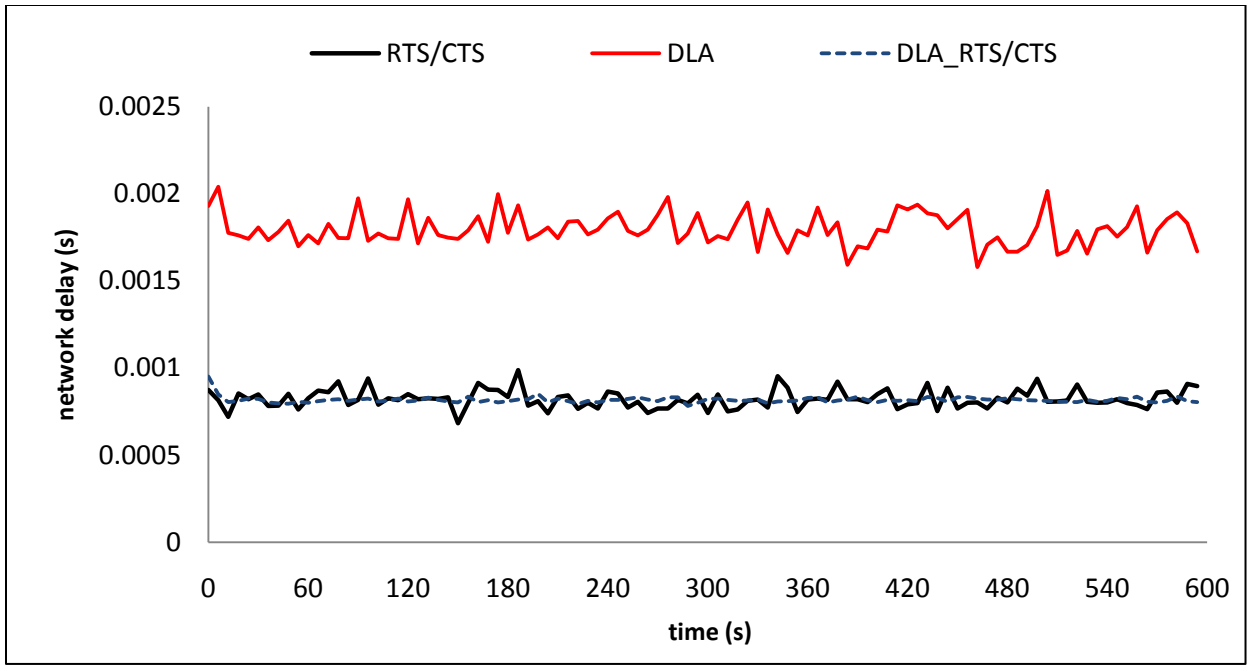

Figure B- 4: The network delay of the DLA algorithm and the CSMA/CA protocol

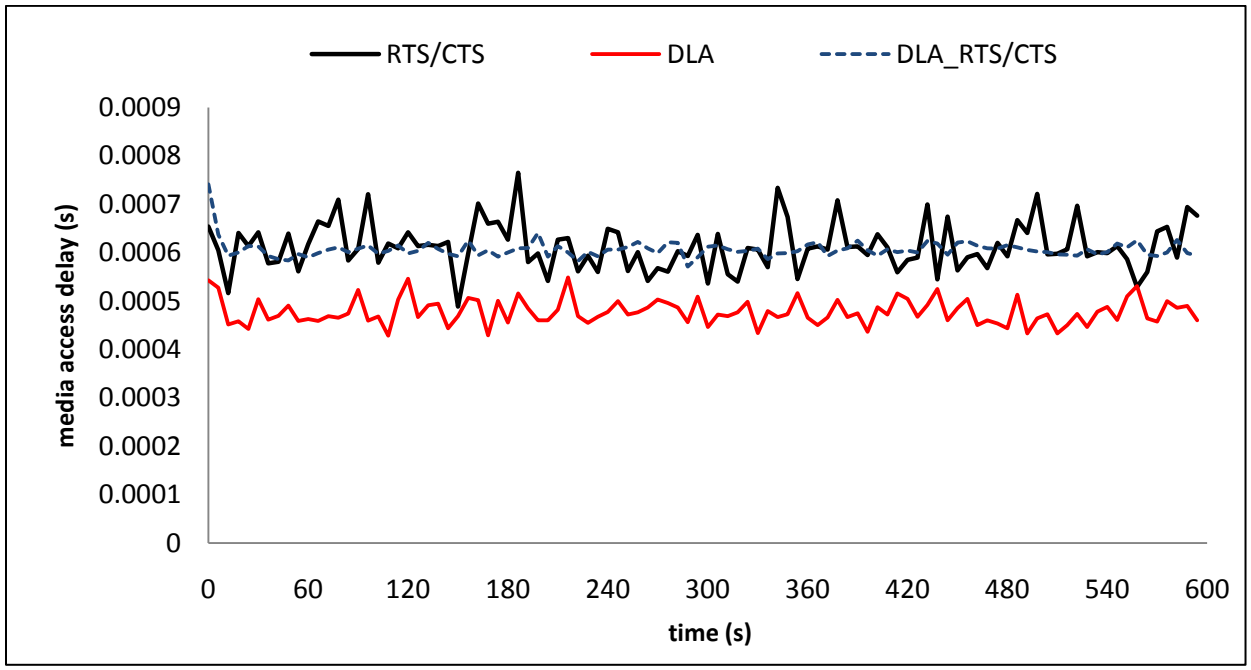

Figure B- 5: The media access delay of the DLA algorithm and the CSMA/CA protocol

List of research papers

Published papers

- Hadi. Noureddine, Hamed. Al-Raweshidy and Qiang. Ni, "FORTEL: Forecasting Routing Technique using Location information for Mobile Ad hoc Networks", IEEE Personal, Indoor and Mobile Radio Communications Workshops (PIMRC Workshops), pp. 473 - 478, 2010.
- Hadi. Noureddine, Qiang. Ni and Hamed. Al-Raweshidy, “SS-CBF: Sender-based Suppression algorithm for contention-based forwarding in Mobile ad-hoc Networks”, IEEE PIMRC, pp. 1810 – 1813, 2010.
- Hadi. Noureddine, Qiang Ni, Geyong Min and Hamed. Al-Raweshidy, ” A New Link Lifetime Prediction Method for Greedy and Contention-based Routing in Mobile Ad Hoc Networks”, IEEE International Conference on Computer and Information Technology (CIT), pp. 2662-2667, 2010.
- Hadi Noureddine and Hamed Al-Raweshidy, “Mitigating the Hidden Terminal Problem in DCF 802.11 WLANs using the Distributed Location-Aided Algorithm”, International Conference on Telecommunications (ICT), pp. 450-453, 2011.
- S. Khan, S. A. Mahmud, H. Noureddine and H. S. Al-Raweshidy, “Rate-adaptation for multi-rate IEEE 802.11 WLANs using mutual feedback between transmitter and receiver”, IEEE PIMRC, pp. 1810 – 1813, 2010.
- Sofian Hamad, Hadi Noureddine, Ibrar Shah and Hamed Al-Raweshidy, “Efficient Flooding Based on Node Position for Mobile Ad hoc Network”, IEEE Innovations, 2011 (to be appeared).

Papers under review

- Hadi Noureddine, Hamed Al-Raweshidy and Qiang Ni, “Geographic/Source Routing Protocol for Mobile Ad-hoc Networks”, IEEE Transactions on Parallel and Distributed Systems.
- Hadi Noureddine, Shahbaz Khan, Seyed Reza Abdollahi and Hamed Al-Raweshidy, “Energy Efficient Routing using Multiple Heterogeneous-Radios in Highly Dense Mobile Ad-hoc Networks“, IEEE Communications Letters (major correction).

- Hadi Noureddine and Hamed Al-Raweshidy, “Survey on Beaconless Routing in MANETs”, IEEE Vehicular Technology Magazine.
- Hadi Noureddine, Qiang Ni, Geyong Min, Hamed Al-Raweshidy, “A New Link Lifetime Estimation Method for Greedy and Contention-based Routing in Mobile Ad Hoc Networks ”, Springer on Telecommunication Systems.
- Hadi Noureddine and Hamed Al-Raweshidy, “ALFA: Advanced Location-Aided Flooding for FORTEL Routing in MANETs”, IEEE Personal Multimedia Communications 2011.
- Sofian Hamad, Hadi Noureddine and Hamed Al-Raweshidy, “LSEA: Link Stability and Energy Aware for reactive routing protocol in Mobile Ad Hoc Network”, IEEE Personal Multimedia Communications 2011.