




Case Study

Performance analysis of a fail-safe wireless communication architecture for IoT based fire alarm control panels

Song Qiu¹  · Robert Allan² · Rajagopal Nilavalan¹ · Jeff Ivey² · Steven Butterfield² · Maozhen Li¹

Received: 28 October 2020 / Accepted: 17 February 2021 / Published online: 25 February 2021
© The Author(s) 2021 

Abstract

This study presents a fail-safe wireless communication architecture for Internet of Things based fire alarm control panels. In fire safety industry, one of the most important issues is to ensure the key information be delivered. A radio frequency wireless communication link is considered for enabling the fail-safe feature when the primary Internet of Things link is failed. In this paper, the design of the wireless communication architecture is proposed, and the system hardware based on customised micro-controller and wireless communication processors is implemented. In order to examine the performance of the proposed wireless communication architecture, a long-term evaluation is designed and conducted in an industrial warehouse, to demonstrate the information latency with parameter of round-trip time, and system reliability with parameter of probability failure rate. The experimental results show that the proposed wireless communication architecture could achieve the low latency and high reliability requirements and reduce the chance of key information loss. With the multi-disciplinary findings discovered, the proposed wireless communication architecture is feasible to be considered to use in future Internet of Things based fire safety products.

Keywords Fail-safe · Wireless communication · Internet of Things · Latency · Reliability

1 Introduction

Nowadays, the Internet of Things (IoT) has been rapidly advancing the way of daily life and work. With the availability of affordable processors and effective wireless communication means, it becomes possible to connect a number of physical objects globally to the internet for collecting, receiving, sharing and even analyzing different kinds of data [1], thus to reveal endless new applications based on this technology. With the commercial utilization of IoT, it has found its way into massive industrial scenarios [2] in recent years.

However, although it is possible to create novel and exciting IoT solutions for existing commercialized wireless fire alarm systems to achieve the next level, it is still highly limited for massive applications due to the critical

requirements of the fire safety industry. The limitations, that hold back IoT enabled fire alarm system (FAS) to bloom, are mainly focusing on (1) system reliability that prevents fire events message (i.e., information) loss by wireless communication link [3]; (2) information latency that needs to be the lowest, or requires fastest internet access and response if IoT based [4], and (3) lack of specific industrial standards for IoT enabled FAS or perfection of current standards [5] related to IoT based FAS. Therefore, as FAS requires high reliability and low latency with the fact that every failure of FAS may cause significant casualties or property loss, the limitations of IoT based FAS must be carefully considered for the design and implementation.

✉ Song Qiu, Song.Qiu@brunel.ac.uk | ¹Department of Electronic and Electrical Engineering, College of Engineering, Design and Physical Sciences, Brunel University London, London, UK. ²Haes Technologies Ltd., Unit 3, Horton Industrial Park, West Drayton, Middlesex, UK.



1.1 Review of related work

There are a number of related works for IoT based FAS, most of them focus on the proposal of system architecture and their hardware design for different application scenarios. For example, Mahzan et al. [6] introduced a fundamental architecture of IoT based home fire alarm system by using Arduino micro-controller board and GSM module to realise wireless communication between the system and end user mobile platform. The system was able to detect abnormal temperature caused by fire event and automatically send SMS to the user for alerting. Imteaj et al. [7] proposed an extended architecture of the system for workhouse in factory. In this system, Raspberry Pi 3 micro-controller was selected to control and cooperate multiple Arduino based sub-systems with WiFi modules to enable different type of sensors integrated into the entire system. Moreover, an IoT based fire fighting robot was designed in [8] based on XRL8 micro-controller board, with the assistance of image detection and auto-tracing capabilities, the robot was able to not only detect, but also take actions in fire event, i.e., extinguishing the fire automatically.

The most recent related work were presented in [9, 10]. The IoT-based fire alarm system proposed in [9] was an ad-hoc network that consisted of several microcontroller based nodes, which connected to a number of different type of detectors. The system communicated with other nodes via WiFi connection and utilized cellular communication to deliver notifications to user mobile phones. By using such system, the authors [10] continued applying it for smart city application scenarios and described their proposed system as edge computing-based system to minimise communication latency without giving any statistic analysis. Reliability of their proposed system was attempt to be addressed by removing a node from the system and monitor the message sent to the user for alerting them. They claimed their proposed system was reliable as the message was successfully delivered to user.

Other works [11–14] contributed to IoT based FAS by providing a variety of hardware solutions with proof of their availability. However, none of them provided performance analysis of reliability or latency for their proposed systems. As latency and reliability are the most critical parameters in fire alarm system, without such statistical results presented, it is questionable for their proposed systems to satisfy the critical requirements for the fire safety industry.

Traditional wireless fire alarm system, which utilises radio frequency only, has several disadvantages. For example, it is difficult to predict the spatial cover

of wireless signal in the deployment environment; the transmission quality may vary at different time, and the radio link can be disturbed by other transmitters [15]. In addition, while IoT is enabled, further system related issues must be carefully considered. Firstly, for example, if the internet is failed (e.g., WiFi router is broken down or cellular module signal for internet is dropped), how will such system to recovery for delivering emergency notifications. Secondly, with use of internet, cyber-security needs to be considered. Malfunction of such system by cyber-attack may result to chaotic evacuations, property damage and even loss of human life [16]. Therefore, it is important to take the cyber-vulnerabilities into account while design the IoT based fire alarm system.

In order to understand the metrics used to describe the characteristics of reliability and latency in fire alarm system, and to tackle the critical issue of failed internet link, some further related research are reviewed. Chen [17] carried out a reliability analysis for a commercial wired FAS deployed in a student apartment. The metrics used in the work were probability of failure on demand and probability of failure per hour as the measurement of system's reliability. By recording the total failure times over 2-year period, the risk of relying on such a system was analyzed and the future suitable system configuration could be considered in such environment. Furthermore, a systematic analysis of latency for IPv6 based low power internet standards IoT wireless communication system used in building automation was delivered in [18]. CC2650 micro-controller based blue-tooth module was selected to be the Internet gateway and round trip time was used to evaluate the latency for different test cases. Finally, a fault tolerance and fail safe that is capable for IoT based dual layer control system was proposed in [19]. Similar to the system architecture in [7], the difference between the proposed system was the capability of utilizing a 2.4 GHz Zigbee wireless communication link across the sensors and actuators to ensure continuity of control action in case of internet link failure. System hardware in [19] was designed and tested for its availability, but there was lack of the analysis on reliability or latency, which made the system questionable whether it was suitable for fire safety industry.

1.2 Contributions and organisations

To the best of our knowledge, there is a lack of both theoretical and practical design of the system hardware architecture for emergency situation to ensure the successful delivery of notification message. In addition, the research work on IoT based FAS, which focuses on the statistical analysis of latency or reliability, is significantly limited. Therefore, in order to tackle the limitations that restrains the development of using IoT in FAS, the main

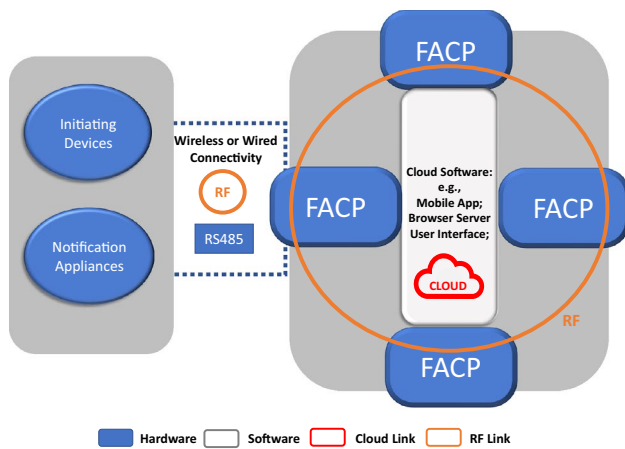


Fig. 1 The system architecture of IoT based FAS

contributions of this case study are: (1) Novel design of system architecture for IoT based FAS with the integration of WiFi for internet access to cloud server, and peer-to-peer RF for information delivery with fail-safe capability available; (2) Statistical analysis of latency and reliability issues: latency analysis of evaluating round-trip times (RTT) with received signal strengths (RSSI), and reliability analysis of evaluating packet loss rate (PLR), packet failure rate (PFR), and probability of failure per hour (PFH).

The rest of the paper organised as follows: In Sect. 2, diverse aspects of the experimental setup, such as the design of the system architecture, the implementation of the hardware with the selection of relevant electronic components and wireless communication modules. In Sect. 3 the experimental procedures including the test environment and evaluation process in details are described. In Sect. 4, the experiment results are presented and analyzed. And finally, the conclusions and future work are included in Sect. 5.

2 Experimental setup

2.1 System architecture

A typical modern FAS consists of a fire alarm control panel (FACP), initiating devices (i.e., detectors or sensors), notification appliance (such as a flashing strobe light, an electromechanical horn or siren or combination of these devices), safety action mechanisms (such as door release, gas valve release, automatic phone call to fire brigade), and power supplies (including backup power supply) [20]. The fundamental of FAS also applies to the IoT based FAS, but as an addition, the devices and FACP are now fully connected with cloud server via internet for unified management.

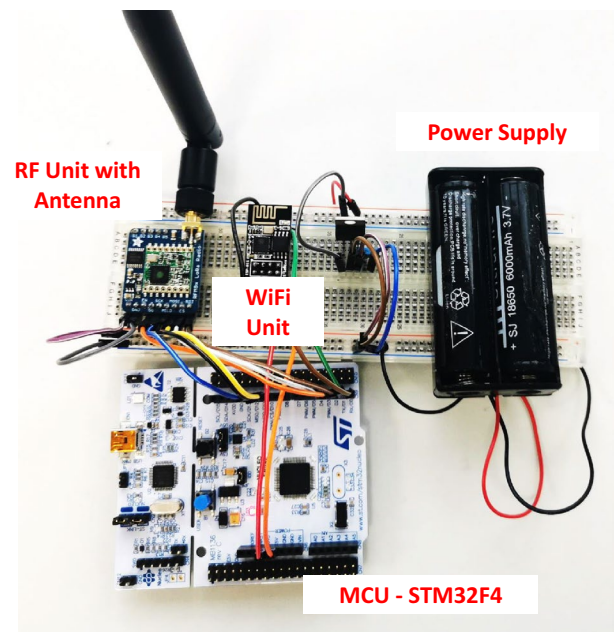


Fig. 2 Prototype hardware of the transceiver

Figure 1 shows the system architecture of our proposed IoT based FAS. Initiating devices are able to collect various type of data, such as environmental temperature, concentration of smoke, etc., then update to FACP via wired or wireless [21] conductivities. The connection between fire safety devices and FACP is well established and widely used commercially. However, the connection between FACP and another FACP remains difficult as the deployment of cable based connection is highly expensive and inflexible for large-scale application scenarios such as industrial park, residential blocks etc., Therefore, the connections between FACP are aimed at in this case study.

By applying IoT technology, an individual FACP operates as an IoT gateway to update the data to a cloud server, exchange important fire event status and send control commands to mechanisms for actions. Particularly, inspired by [19], the RF wireless communication links, are deployed into the FACP to realise simultaneously peer-to-peer key information and commands exchange between each other to prevent fatal consequences caused by information delay or failure of information delivery.

2.2 System prototype

According to the system architecture, a general transceiver for FACP to enable the IoT as well as the fail-safe feature is aimed to be developed. Figure 2 shows the transceiver which has been built to demonstrate the function of the system. The transceiver consists 4 key components: (1)

micro controller unit (MCU), (2) WiFi unit, (3) RF unit, and (4) power supply.

The MCU used is the STM32F4 Nucleo, which is a complete, cost-effective and breadboard-friendly board based on the STM32F401RET6. This board is chosen to mimic the core chipset widely used in commercial FACPs to operate IoT tasks as supplement of other fire alarm functions.

The WiFi unit uses ESP8266EX module to connect the Internet via 802.11n wifi protocol. This module is highly integrated for efficient power usage, compact design and reliable performance for IoT industrial application scenarios [22]. The WiFi module used is to access open source Blynk™ cloud server via customised TCP/IP protocol to achieve cloud computing and controlling. The cloud server user interface can be accessed via a mobile platform (e.g., smart phones or tablets) and PC based applications. By using Blynk™, it is efficient to deliver the key information or commands to destinations and is effective to manage the data received from the sensors or detectors for further analysis and investigation.

The RF unit uses Adafruit RFM95 module based on SX-1276 Long Range (LoRa™) [23] modem, which provides ultra-long range spread spectrum communication and high interference immunity with transmission power of 20 dBm and reception sensitivity of -148 dBm. The frequency is set at 868 MHz, according to the EU legislation that demands this specific radio frequency can only be commercialised used for FAS in the UK [5]. The RF unit connects to an one-quarter of the RF wavelength swivel type dipole antenna with gain of 1 dBi via SMA connector.

A battery packet with 5 V power regulator is used to supply power for the entire transceiver.¹ Table 1 summarises the parameters of the components used in our experimental prototype.

3 Experimental procedures

3.1 Test environment

As the propagation of RF signal can be heavily affected by the communication environment, where the surroundings are typically highly reflective or absorptive, creating significant multi-path effects or electromagnetic resonance [24]. Therefore, in order to prove the feasibility of the prototype system in such complex environment, a typical

¹ It is worth noting that power supply is not a critical concern in design the IoT based FAS as FACP in a typical FAS is required to be connected to mains and a secondary battery power supply unit for emergency power backup, therefore, a battery packet is used here only for the convenience of experiment tests.

Table 1 The experimental prototype and components' parameters

Feature	Parameters and values
MCU	STM32 Nucleo
Micro-controller chip	STM32F401
WiFi unit	ESP8266EX
Transmission band	2.4 GHz
Protocol	802.11n
Transmission power	+ 14 dBm
Receiver sensitivity	-72 dBm
Antenna	PCB trace on ceramic chip
Security	WPA/WPA2
RF units	RFM95
Transmission band	868 MHz
Transmission power	+ 20 dBm
Receiver sensitivity	-148 dBm
Receiver antenna gain	+ 1 dBi

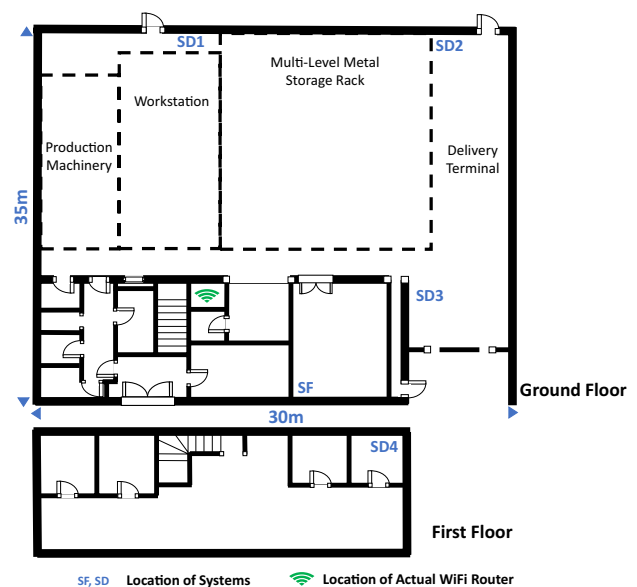


Fig. 3 System deployment locations in floor plan of industrial warehouse

deployment scenario in an industrial estate is considered. The estate shown in Fig. 3 has two area: office and warehouse. The office area has two floors, where both floors are modern styled and well furnished. The warehouse is approx. 850 m² with 7 m in height, which consists of 4 zones, namely, production machinery, workstation, storage with fully loaded multi-level metal rack and delivery terminal.

The experiments were proceeded under the working time of the whole estate to demonstrate the performance of the prototype system in the in situ state. There were 5 proof of concept systems had been prepared for the

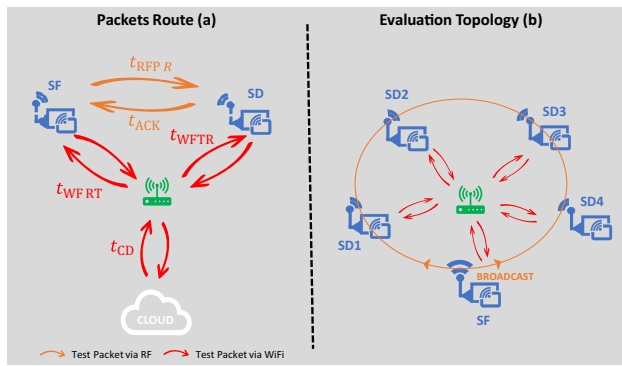


Fig. 4 Illustration of the test topology: packets route during communication (a) and evaluation topology used in the experiment (b)

experiments. One system was placed at the fixed location, which is denoted as SF (i.e., system at fixed location), and another 4 systems deployed at 4 different and numbered (number from 1 to 4) locations² for the experiment, which are denoted as SD1 to SD4 (i.e., system at different numbered location). All the systems were connected to the local WiFi router located in the server room for cloud access.

3.2 Evaluation process

To show the feasibility of the proposed prototype system and to record the packets loss during the testing hours, every packet sent by the proposed system was designed to be recorded. In order to create sufficient results for such analysis, a long-term evaluation was considered. The long-term evaluation was conducted for 1000 h in the test environment to collect round-trip time (RTT) and received signal strength indicator (RSSI) as the metrics for performance analysis. To demonstrate the system reliability, the calculation of packet loss rate (PLR), packet failure rate (PFR), and evaluated the probability of failure per hour (PFH) based on the 1000-h test were processed.

During the long-term evaluation, SF was programmed to broadcast test packets every 3 s to 4 in situ SDs via both wifi and RF link. Once received by SDs, acknowledgment message (ACK) would be sent back to the SF via both WiFi and RF link. SF was able to measure the RTT and RSSI and also record any packet loss (i.e., ACK was not received) for both WiFi link and RF link for later reliability analysis. Figure 4 illustrates the packets routes between SF and SDs

and the test topology for our evaluations. The key evaluation metrics are explained as follows:

3.2.1 RTT and RSSI

- *RTT* RTT is one of the important metrics to indicate the latency of a wireless communication link. The RTT is defined here as the time delay for the successful end-to-end transmission of one test packet. t_{RF} and t_{WF} define the RTT for RF and WiFi cloud link between SF and SDs respectively as follows.

$$RTT_{RF} = t_{PSF} + t_{ACC} + t_{RFP} + t_{PSD} + t_{ACK}, \tag{1}$$

where t_{PSF} and t_{PSD} are the signal processing delay at the transceivers, t_{ACC} is the time cost to access the propagation channel, t_{RFP} is the time for the packet transmission in the air, and t_{ACK} is the time to receive the ACK from SD.

$$RTT_{WF} = t_{PSF} + t_{ACC} + t_{WFTR} + t_{CD} + t_{PSD} + t_{WFRT}, \tag{2}$$

where t_{PSF} , t_{PSD} and t_{ACC} are the same as the definitions in Eq. (1), as the packet transmitted from SF needs to be delivered to one SD via the WiFi router with access to internet, thus, t_{WFTR} denotes the total time for the propagation between SF and the router and t_{WFRT} denotes the total time between router and each SD. t_{CD} is the total time used for exchange the packet between cloud server and the Wifi router.

- *RSSI* RSSI test identified the transmission quality and signal attenuation in the complex warehouse environment. The RSSI measurements were divided into two categories on SF side: (1) RF RSSI, where the RF unit of SF was able to provide RSSI measurements while every ACK received from each SD and then store the RSSI in the MCU for further analysis; and (2) WiFi RSSI, where the wifi module of SD could collect the RSSI with the local wifi router at different location and store the RSSI measurement in cloud server for further analysis.

3.2.2 PLR, PFR and PFH

In order to show the long-term reliability of our prototype, following three metrics, namely PLR, PFR and PFH, were evaluated.

- *PLR* PLR is used to estimate the quality of our proposed prototype with RF or WiFi link, it is defined as the rate of the number N_L of lost packets over the total number N_T of packets sent, given as,

$$PLR = \frac{N_L}{N_T}. \tag{3}$$

² The locations were selected at the place where manual operation is potentially needed or a point to install a FACP or a control interface.

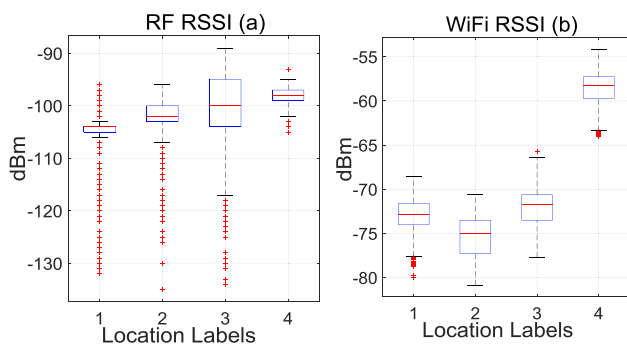


Fig. 5 Statistic boxplot of overall RSSI for RF (a) and WiFi (b) link

- **PFR** Similar to PLR, the communication *failure* is defined as the ACK was not received either via RF or WiFi link from each SD for the same packet sent by SF. The number of failure, denotes as N_F , is able to be recorded and accumulated during the experiment. Therefore, the PFR is given as,

$$PFR = \frac{N_F}{N_T} \tag{4}$$

- **PFH** PFH was used to demonstrate the overall reliability of our proposed prototype and it is given as,

$$PFH = \frac{N_F}{N_{Hours}}, \tag{5}$$

where N_{Hours} denotes the total hours of test, which equals 1000 for each location in our case.

4 Results and analysis

In this section, the robustness of RSSI and RTT performance of the proposed prototype is firstly discussed and compared between RF and WiFi link based on the collected evaluation results during 1000 h. Afterwards, the metrics of PLR, PFR and PFH are analysed for the reliability of the long-term operation of our proposed system.

4.1 Robustness of RSSI and RTT

4.1.1 RSSI analysis

Figure 5 shows the statistic analysis of the entire test packets sent and received at each locations. According to Fig. 5a, it can be observed that the RSSI of location 1 to location 3 fluctuate significantly, due to the RF signal that had to penetrate several walls and warehouse working zones to reach the SDs. While the SD on location 4 was just above the SF, showed a better RSSI than other 3 locations.

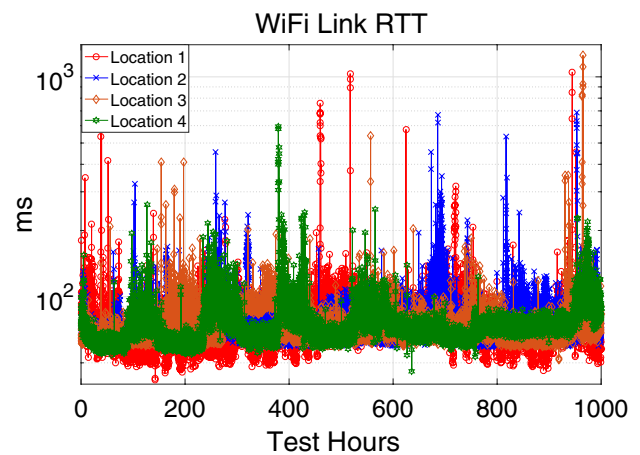


Fig. 6 Preliminary results of WiFi link RTT

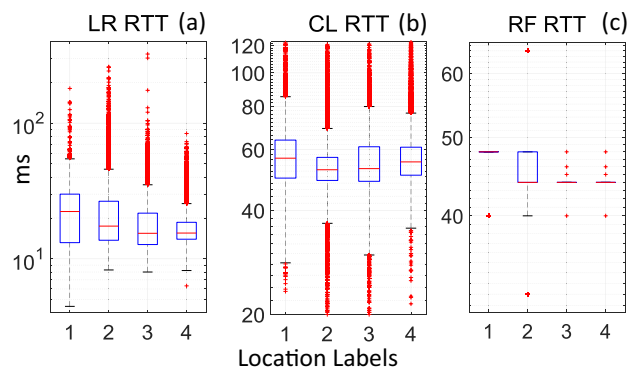


Fig. 7 Statistic boxplot of RTT for local router access (a), cloud link (b) and RF (c)

Figure 5b statistically analyzed the RSSI for the signal connected to the WiFi router. Compared to RF link, overall WiFi RSSI (> -90 dBm) is better than RF RSSI (< -90 dBm) for our specific system hardware setup according to Fig. 5b. It can be observed that location 4 also has a better RSSI than other 3 locations, due to the same reason as RF link, that the WiFi router located in the server room (see Fig. 3) is closer to location 4, where signal only penetrates through office ceilings rather than metal racks or operating machineries.

4.1.2 RTT analysis

Figure 6 shows the preliminary results of WiFi RTT. In order to statistically analyze the preliminary results, a boxplot is presented in Fig. 7. In Fig. 7, the WiFi RTT as the sum of Local Router (LR) RTT (i.e., $t_{PSF} + t_{Acc} + t_{WFTR} + t_{PSD} + t_{WFRT}$), and Cloud Link (CL) RTT (i.e., t_{CD}) is separately analyzed. The RTT of WiFi link was significantly varied due to the time spent on local router access and cloud server access

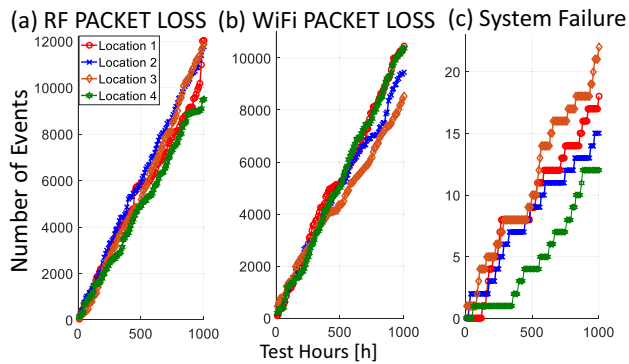


Fig. 8 The cumulative packet loss and the communication failures versus the testing time period with comparison of 4 locations

Table 2 Reliability metrics performance

Location	PLR (RF) (%)	PLR (WiFi) (%)	PFR (System) (%)	PFH (/h)
1	1.000	0.871	1.5×10^{-3}	0.018
2	0.979	0.788	1.3×10^{-3}	0.015
3	0.989	0.711	1.8×10^{-3}	0.022
4	0.793	0.865	1.0×10^{-3}	0.012
Overall	0.940	0.809	1.4×10^{-3}	0.017

according to Fig. 7a, b respectively. However, it is important to note that the mean time of CL RTT is around 55 ms, which is approximate 4 times higher than the mean time of LR RTT. Based on Fig. 7c, RF RTT is varied at around 45 ms despite the location of SDs, and it is also much more stable than the time spent in WiFi link. According to Figs. 5 and 7, it can be concluded that (1) RF signal strength is worse affected by the environment compared to WiFi signal but the RF RTT is more stable than WiFi link; and (2) RTT for both RF and WiFi link is not significantly impacted to the locations of the SDs as long as the wireless communication link existed.

4.2 Reliability of long-term operation

Reliability is one of the most important considerations for FAS. In this section, long-term evaluation for reliability is shown in Fig. 8. The cumulative numbers of packet loss for RF and WiFi link are presented in Fig. 8a, b respectively. It can be observed that both RF and WiFi links suffered from packets loss in all 4 locations and the number of cumulative loss packets approximately increase linearly at similar rate. Figure 8c shows the number of cumulative system failure where both RF and WiFi link failed to deliver the test packet. It is clear that the order of magnitude ($\sim 10^1$) of system failure is significantly less than the order of magnitude ($\sim 10^3$ – 10^4) of packet loss for RF or

WiFi link alone during 1000 h test. The results confirmed the significant risk that current wireless communication used in FAS without a fail-safe solution, could introduce key information loss during the operation of FAS.

In order to analyze the reliability of the proposed system, Table 2 summarized and compared the metrics of PLR, PFR and PFH based on Eqs. (3), (4), and (5). It is worth addressing that, the PFH was defined as the failure of communication for a loss of ACK rather than the failure of the FAS system. the message was considered as lost due to the absence of ACK. However, in reality, according to [5] for commercial wireless communication based FAS, the requirement of message delivery time for fire event status between FACP must be less than 100 s, which means at least 1 out of 33 status data packets must be delivered within 100 s. In this case, it is far more sufficient for our proposed prototype to deliver the message based on our test results. Thus, the results in Table 2 confirmed our proposed prototype was able to significantly reduce the chance of key information loss compared to using RF or WiFi alone, therefore, to provide better reliability performance for IoT based FAS.

5 Conclusions

In this paper, the recent works on IoT based FAS were firstly reviewed. The need to develop a specific system with IoT capabilities, that has high reliability and low latency for the fire safety industry, was pointed out. Inspired by the design found in Sect. 1.1, the system architecture and system prototype to achieve the high reliability and low latency requirements were proposed. In order to prove such achievements, a long-term evaluations in an industrial estate for its robustness of latency and reliability were conducted. It was proved according to the experimental results that the proposed system was able to reduce the chance of key information loss, and satisfy current fire safety standard on wireless information transfer in FAS.

Future work will focus on: (1) reducing the WiFi router accessing time to minimise the overall WiFi link communication RTT; (2) providing multiple internet access options (i.e., ethernet, cellular network, etc.) at the same time to ensure fail-safe internet link; (3) conducting further experiments to evaluate the system performance in an industrial park with multiple infrastructure or a residential zone with estate blocks, to demonstrate the potential deployment of such system for a larger scale, rather than in a single building; and (4) exploring suitable cyber-security means to be applied to the proposed wireless communication architecture.

Acknowledgements The work in this paper is partly supported by the Innovate UK Knowledge Transfer Associate (KTP) Scheme, the Brunel University London, and the Haes Technologies Ltd.

Compliance with ethical standards

Conflict of interest The authors declare that they have no conflict of interest.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>.

References

- Evans D (2011) The internet of things: how the next evolution of the internet is changing everything, Cisco Internet Business Solutions Group (IBSG), Tech. Rep
- Xu L, He W, Li S (2014) Internet of things in industries: a survey. *IEEE Trans Ind Inf* 10(4):2233–2243
- Chagger R (2015) Live investigations of false fire alarms. Building Research Establishment (BRE), Tech. Rep
- Savitha N, Malathi S (2018) A survey on fire safety measures for industry safety using IoT. In: Proceedings of the international conference on communication and electronics systems (ICCES 2018), pp 1199–1205
- British Standard (2012) Fire detection and fire alarm systems part 25: components using radio links. British Standards Institution (BSI), London
- Mahzan N, Enzai N, Zin N, Noh K (2017) Design of an Arduino-based home fire alarm system with GSM module. In: Proceedings of 1st international conference on green and sustainable computing (ICoGeS 2017), pp 1–8
- Imteaj A, Rahman T, Hossain M, Alam M, Rahat S (2017) An IoT based fire alarming and authentication system for workhouse using Raspberry Pi 3. In: Proceedings of international conference on electrical, computer and communication engineering (ECCE 2017), pp 899–904
- Rambabu K, Siriki S, Chupernechitha D, Pooja C (2018) Monitoring and controlling of fire fighting robot using IoT. *Int J Eng Technol Sci Res* 5(3):552–557
- Mahgoub A, Tarrad N, Elsherif R, Al-Ali A, Ismail L (2019) IoT based fire alarm system. In: Proceedings of the third world conference on smart trends in systems security and sustainability (WorldS4 2019), pp 162–166
- Mahgoub A, Tarrad N, Elsherif R, Ismail L, Al-Ali A (2020) Fire alarm system for smart cities using edge computing. In: Proceedings of the IEEE international conference on informatics, IoT, and enabling technologies (ICIOT 2020), pp 597–602
- Li Y, Zhu X, Wang Z, Xu F (2016) Developing a fire monitoring and control system based on IoT. In: Proceedings of the 2nd international conference on artificial intelligence and industrial engineering (AIIE2016), pp 174–178
- Jiang J, Gao Z, Shen H, Wang C (2017) Research on the fire warning program of cotton warehousing based on IoT technology. *Int J Eng Bus Manag* 18(2):121–124
- Seiber C, Nowlin D, Landowski B, Tolentino M (2018) Tracking hazardous aerial plumes using IoT-enabled drone swarms. In: Proceedings of the IEEE 4th world forum on Internet of Things (WF-IoT, 2018), pp 377–382
- Lalwani S, Khurana M, Khandare S, Ansari O, Pokle S (2018) IoT based industrial parameters monitoring and alarming system using Arduino. *Int J Eng Sci Comput* 8(4):17305–17308
- Stockbroeckx B (2017) Wireless interconnections in fire detection and fire alarm systems: points of attention for the installer and the Belgian Application Standard. National Fire Protection Association (NFPA), Tech. Rep
- Shin H, Noh J, Kim D, Kim Y (2020) The system that cried wolf: sensor security analysis of wide-area smoke detectors for critical infrastructure. *ACM Trans Priv Secur* 23(3):1–32
- Chen Y (2011) Reliability analysis of a fire alarm system. In: Proceedings of international conference on advances in engineering (ICAE 2011), pp 731–736
- Zhu H, Pang Z, Xie B, Bag G (2016) IETF IoT based wireless communication for latency-sensitive use cases in building automation. In: Proceedings of IEEE 25th international symposium on industrial electronics (ISIE 2016), pp 1168–1173
- Sharma S, Gupta S, Gupta S, Kotwal S (2018) IoT based innovative dual level control system with fault tolerance and fail safe capability. In: Proceedings of the second international conference on intelligent computing and control systems (ICICCS 2018), pp 307–312
- Jee S, Lee C, Kim S, Lee J, Kim P (2014) Development of a traceable fire alarm system based on the conventional fire alarm system. *Fire Technol* 50(3):805–822
- Jervis V (2010) Short range devices operating in the 863–870 MHz frequency band office of communications (OFCOM) final report. Aegis Systems Ltd., Tech. Rep
- “Esp8266ex datasheet”, Espressif Systems, User Manual, Dec. 2019, rev. 6.2
- 137 to 1020 MHz low power long range transceiver, SEMTECH, User Manual, Mar. 2015, rev. 4
- Candell R, Remley K, Quimby J, Novotny D, Curtin A, Papazian P, Kashef M, Diener J (2017) Industrial wireless systems radio propagation measurements. National Institute of Standards and Technology (NIST), Tech. Rep

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.