A Comprehensive Vulnerability Analysis of LoRaWAN-based Cyber-Physical Systems in the Presence of EMI and PSD Transient Faults

Faezeh Saghaei, Hamid R. Zarandi*, Morteza Tavakkoli

Department of Computer Engineering, Amirkabir University of Technology (Tehran Polytechnic), Tehran, Iran

* Corresponding author:h_zarandi@aut.ac.ir (Hamid R. Zarandi)

Received: ; received in revised: ; accepted:

KEYWORDS

Fault Injection;
LoRaWAN;
Cyber-Physical System;
Electromagnetic Interference;
Power Supply Disturbance

ABSTRACT

This paper presents a comprehensive vulnerability analysis of LoRaWAN networks, focusing on the effects of electromagnetic interference (EMI) and power supply disturbance (PSD) faults on network performance and security. The study begins by outlining the fundamental principles of LoRaWAN, including its architecture, key management, and security features. It then delves into the potential vulnerabilities introduced by EMI and PSD, which can disrupt communication, cause data corruption, and lead to security breaches. Through a series of physical experiments, a developed framework evaluates the impact of these factors on LoRaWAN networks under various conditions. The results reveal that EMI and PSD can significantly degrade the performance of LoRaWAN networks, leading to packet loss, increased latency, and compromised data integrity. The study also highlights the importance of continuous monitoring and adaptive security measures to ensure the resilience of LoRaWAN networks against EMI and PSD. Finally , this comprehensive vulnerability analysis underscores the need for robust security and reliability measures in LoRaWAN networks to safeguard against the adverse effects of EMI and PSD. The findings contribute to the ongoing efforts to enhance the security and performance of IoT networks, ensuring their reliable operation in diverse and challenging environments.

Accepted by Scientia Iranica

1. Introduction

Cyber-Physical Systems (CPS) and Internet of Things (IoT) facilitate intelligent, real-time operations by transmitting sensitive data. These systems have three core components: sensors, aggregators, and actuators, making them indispensable across various sectors, especially in industrial applications [1]. LoRaWAN, a communication protocol tailored for CPS and IoT, enables long-range connectivity with minimal power usage in unlicensed frequency bands. This makes it particularly suitable for environments with numerous connected devices involved in process and environmental monitoring [2][3][4].

LoRaWAN uses Chirp Spread Spectrum (CSS) modulation for long-range communication, supporting distances of up to 15 kilometers in rural areas and several kilometers in urban environments. While on paper, CSS suggests resilience, real-world environments pose challenges. LoRaWAN’s long-range capability is suitable for applications where devices are dispersed and need to communicate with a central gateway. However, maintaining stable connections between end devices and gateways can be difficult due to potential faults like clock glitch, power supply disturbance (PSD), and electromagnetic interference (EMI) [5][6]. Therefore, examining LoRaWAN's performance and reliability is an essential task.

2345-3605 © 2025 Sharif University of Technology. This is an open access article under the CC BY-NC-ND license

Accepted by Scientia Iranica

While analytical modeling and simulation are two potential evaluation methods for the performance of LoRa technology, they often fall short in addressing intricate complexities in real-world scenarios. Although analytical modeling and simulations can offer insights, they fail to replicate all variables encountered in practical scenarios, leading to inaccuracies. In contrast, physical evaluation ensures that our findings are grounded in actual performance data and provides assurance in our assessment of LoRaWAN under such conditions. Previous research has explored the functionality of LoRa technology and its performance in various environments and parameter settings. However, the impact of physical transient faults like EMI and PSD on LoRa performance remains largely uninvestigated due to the challenge of establishing a standardized and reliable fault injection test environment.

This paper aims to assess the vulnerability of LoRaWAN networks to EMI and PSD transient faults. We integrate LoRa modules and gateways, subjecting them to controlled fault injection. A mining-related IoT application crucial for monitoring and accident prevention has served as our workload, highlighting the importance of stable operating conditions in such critical environments [7]. To address critical failure points, we developed a LoRaWAN-based system with sensors to monitor key inputs. A LoRa gateway was deployed to facilitate communication between end devices and the network server. This setup enables data transmission to a separate alarm-equipped end device, triggered under unsafe environmental conditions. In an electromagnetic fault injection lab, the transmitting end device was subjected to electromagnetic waves (80 MHz to 1 GHz, excluding the LoRa operating frequency) with both horizontal and vertical polarizations. Packets of varying content and size were transmitted during this process. For power supply disturbance injection, a dedicated PSD injection circuit was inserted into the LoRa power supply line. The regulator's output voltage was branched to both the LoRa device and the fault injection circuit. Randomly timed glitches with varying durations were introduced, reducing the LoRa's 3.3V operating voltage by up to 30%. This multifaceted approach allows us to comprehensively evaluate the robustness of LoRaWAN in challenging operational environments. The contributions of this paper are as follows:

- A LoRaWAN network has been implemented and a practical application for mine environment monitoring developed.
- This study investigates the vulnerability of LoRaWAN networks to EMI as well as PSD transient faults through controlled fault injection in a standardized testing environment. A comprehensive analysis of the impact on key performance metrics, including packet loss rate, latency, Signal-to-Noise Ratio (SNR), and Received Signal Strength Indicator (RSSI), is presented.
- Extensive analysis demonstrates the robustness of the LoRaWAN network against EMI across the specified range, except at the operating frequency, which exhibits vulnerability and necessitates appropriate shielding.
- The vulnerability of the LoRaWAN network to PSD is investigated using a custom-designed PSD injection circuit. A comprehensive analysis of packet loss rate, SNR, and RSSI is performed.

The rest of this paper is organized as follows: Section 2 is dedicated to reviewing previous work in fault analysis and evaluation methods. Section 3 comprehensively investigates the physical prototype setup used as testbed for fault injection experiments. It also presents workload used as CPS application on top of the developed prototype. Fault injection environment and the method used for injection of EMI and PSD is presented in Section 4. Evaluation of empirical results from EMI and PSD fault injections are shown in Section 5. Finally, Section 6 concludes the paper.

2. Related Work

Several related work focus on the analysis and evaluation of LoRaWAN. For instance, [8] evaluates LoRaWAN coverage in urban and maritime environments with a fixed base station and a mobile end device (mounted on a car or boat) transmitting packets periodically. The resulting data was used to develop a channel attenuation model, potentially useful for network providers in estimating base station density and conducting more detailed LoRa performance analysis. Research in [9] investigates the communication coverage of low-power technologies, including LoRa, across varying distances and placements (ground level, underground, rooftop). Their findings indicate a significant decrease in reliability over long distances. This work also compares the transmission capabilities of LoRaWAN and NB-IoT in challenging environments (underground, underwater, through metal), concluding that NB-IoT performs slightly better on average, although both demonstrate robustness. Furthermore, [10] explores the comparative performance of LoRaWAN and NB-IoT in harsh environments, while [11] assesses LoRa reliability under varying temperatures, showing that increasing temperatures can degrade link quality and reduce RSSI and SNR. Other studies, such as [12] and [13], examine the impact of electromagnetic interference (EMI) on wireless communication systems, demonstrating its detrimental effects on signal quality, error rates, packet loss, and latency in Wi-Fi, Bluetooth, and Zigbee-based IoT systems, respectively.

Several studies have explored voltage-based fault injection attacks against resource-constrained IoT devices. Research done in [14] demonstrates the feasibility of such attacks by briefly reducing the operating voltage of an 8-bit AVR microcontroller to near zero. This research highlights the vulnerability of these devices, particularly when operating near their specified limits. An study in [15] investigates the security implications of voltage manipulation on IoT devices like sensors and actuators used in critical systems such as automotive braking, industrial control, and robotics. By injecting malicious signals through the power supply, it attacks can compromise sensor readings or manipulate actuator behavior, potentially leading to hazardous consequences.

Another related work introduces a novel attack vector using malicious field-replaceable units (FRUs) [16]. The authors integrate a low-cost fault injection circuit within a FRU, which can be placed in proximity to the target device. FRUs, commonly found in devices like routers, mobile phones, printers, and health sensors, are often installed by third-party technicians without rigorous authentication, presenting a significant security risk. This research demonstrates how such a malicious FRU can be used to extract secrets from a privileged system process through a combined hardware-software approach, even when only the attacker's software application is compromised. The low cost of this attack, significantly less than professional fault injection analysis equipment, coupled with the potential for remote execution, underscores the growing threat of fault injection attacks. Considering the advancements in software-only fault injection techniques, the authors argue for broader implementation of fault tolerance mechanisms across various device classes.

3. Physical Prototype Setup and Workload

Our prototype setup, shown in Fig. 1, emulates a typical Cyber-Physical System (CPS) architecture, specifically designed for EMI as well as PSD experiments with a real use case in real-life scenarios where the occurrences of EMI or PSD are high. Also, a full-scale CPS comprises numerous transmitter and receiver nodes communicating through a gateway, our prototype utilizes a single instance of each component to effectively evaluate the impact of fault injection on LoRaWAN communication. This setup, representative of many real-world deployments, consists of a transmitter node equipped with a LoRa chip, a temperature and humidity sensor, and a gas sensor, which are common elements in various CPS applications. The LoRa module is connected to a frequency-matched antenna to ensure reliable transmission. Data from the transmitter is received by an eight-channel LoRaWAN gateway, which acts as a bridge to the network server, forwarding data to the cloud via the internet. This connection facilitates data processing on the application server and enables subsequent actions. Finally, a separate LoRa-enabled receiver node listens for downlink messages, maintaining synchronization with the transmitter and providing status updates. This configuration allows for a comprehensive investigation of fault injection effects across the entire LoRaWAN communication chain.

3.1. CPS Application

Fig. 2 illustrates the implementation of our system within a mining environment, chosen for its challenging communication conditions and critical safety requirements. The deployed sensors monitor environmental parameters, specifically temperature and gas levels, crucial for miner safety. The transmitter node, equipped with these sensors, not only transmits the collected data via LoRaWAN to the gateway but also performs on-device state calculation, triggering local LED alerts based on detected conditions. This calculated state is included in the data transmitted to the gateway.

Upon receiving the sensor data and calculated state, the gateway forwards this information to The Things Network (TTN), a widely adopted open-source LoRaWAN network server. From TTN, data flows to our application server, implemented using Node-RED, a flow-based programming tool ideal for IoT applications. The lightweight and efficient MQTT protocol facilitates communication between TTN and Node-RED. Our custom Node-RED dashboard provides real-time visualization of the mine's environmental conditions, displaying temperature and gas levels using charts and gauges. Crucially, the dashboard incorporates alert functionality based on pre-defined system states. Upon detection of a critical state, such as a gas leak or potential explosion, Node-RED transmits a command back through TTN, initiating a downlink message to a dedicated receiver node within the mine. This receiver node then activates visual and auditory alarms, providing immediate notification of the hazardous condition. This closed-loop system ensures rapid response to critical environmental changes, enhancing safety within the mine.

Accepted by Scientia Iranica

4. Fault Injection Method

This section presents the methodology used to evaluate the robustness of the proposed LoRaWAN-based cyber-physical system against two major types of transient faults: EMI and PSD. It begins by detailing the controlled laboratory environments specifically designed for EMI and PSD injection, including the configuration of hardware components and shielding techniques. Next, the section explains the experimental setup, outlining the defined scenarios, packet configurations, and injection parameters used in both fault types. The final part addresses network-level factors such as congestion and packet timing, which can influence system performance under stress conditions. Together, these subsections form a comprehensive foundation for understanding the empirical results presented later in the paper.

4.1. EMI injection environment

System robustness against electromagnetic interference (EMI) was evaluated within a controlled electromagnetic environment. An electromagnetic compatibility (EMC) laboratory, designed to prevent external EMI and minimize internal reflections (Fig. 3), served as the testing environment. Controlled EMI, generated across a defined frequency spectrum, was emitted using an antenna and signal generator conforming to the IEC 61000-4-3 standard.

4.2. PSD injection environment

Fig. 4 shows a schematic overview of PSD fault injection environment, where fault injection manager is responsible for managing the entire fault injection process. Components include a *voltage regulator*, PSD circuit as a fault injector, LoRa sender module (or transmitter node) along with its microcontroller. The LoRa module is programmed via the connected microcontroller to send network packets through the Wi-Fi antenna. In this process, the input power supply receives its value from the output of the PSD circuit, which experiences a temporary voltage drop (disturbance) when the microcontroller unit present in the PSD circuit commands the transistor gate to inject fault. One of the microcontrollers is responsible for initializing the LoRa module, while the other manages PSD injection (fault occurrence time and its duration). A voltage regulator *LD1117V33* is exploited. This regulator accepts input voltages ranging from 3.3V to 5.0V and provides a stable 3.3V output with a maximum current capacity of 1200mA. The NMOS MOSFET transistor (IRF540) is exploited so that its source is connected to the ground, and its drain is connected to the output node of the voltage regulator.

The gate of this transistor is controlled by a microcontroller (inside PSD circuit in Fig. 4). Following a programmed sequence, the microcontroller selects a random time point between the warm-up period and the end of the transmission phase. At this fault injection time, the microcontroller activates the NMOS transistor's gate, briefly introducing a power supply disturbance at the regulator's output. This injected fault results in a voltage drop at target LoRa Sender (LoRa module) from 3.3V to 2.6V, potentially affecting the LoRa module's operational mode and other parameters.

4.3. Experimental Setup

The CPS application defines three states based on gas level and temperature:

- **Healthy**: Both gas level and temperature are within safe zones.
- **Gas Leak**: The gas level is out of the safe zone, but the temperature is within the safe zone.
- **Possible Explosion**: Both gas level and temperature are out of safe zones.

LoRa transmitter node which plays sender role, transmits these states based on sensed data from the environment.

To evaluate the impact of Electromagnetic Interference (EMI), six experimental scenarios were designed, as summarized in Table 1. These scenarios combined two antenna polarization configurations (vertical and horizontal) with three different payload sizes (two, five, and nine bytes), reflecting a range of data transmission patterns—from minimal system state reporting to more comprehensive sensor data transmission. Each scenario was compared against a baseline measurement taken without EMI present (golden run). This comparative methodology enabled a focused analysis of how specific EMI conditions influence system performance.

Accepted by Scientia Iranica

In our study, the primary focus has been on analyzing the uplink communication, as the chosen CPS scenario—environmental monitoring in a mining application—primarily relies on data flowing from sensor nodes to the gateway. For evaluating the effects of EMI and PSD, we monitored the performance of uplink packets with varying payload sizes and transmission rates, measuring metrics such as packet loss, RSSI, and SNR. This emphasis was intentional, since failures in uplink communication pose more immediate risks in critical applications like gas detection or temperature monitoring.

That said, downlink communication was also implemented in the system—specifically for sending alerts from the server back to an actuator node (e.g., to trigger a local alarm). However, since downlink traffic is much less frequent and less time-critical in our scenario, we did not perform an independent, in-depth statistical analysis on downlink behavior.

For PSD effect evaluation, eleven scenarios, as detailed in Table 2, were defined for all experiments, with each scenario comprising twenty local experiments. In all experiments, ten packets were transmitted, with the first five serving as a warm-up period. Fault injection commenced with the transmission of the sixth packet. The performance under each scenario was compared against a "*golden scenario*" baseline, representing trials conducted without fault injection. *Scenarios 1* through *9* utilized a consistent packet size while varying the fault injection duration. *Scenarios 10* and *11* shared the same fault injection duration as *Scenario 5* but differed in packet size. This structured presentation clarifies the experimental methodology and provides a clear overview of the different scenarios, facilitating a more rigorous analysis of the results within a research context.

As can be seen from tables 1 and 2, number of scenarios are different for EMI and PSD fault injection experiments. This is due to the fact that when applying EMI, controlling fault duration is not possible; however, polarization of injection antenna is possible to change. These scenarios are setup so that it is possible to find effects of each fault injection parameter on packet transmission process.

4.4. Network Congestion

To assess the robustness of our LoRaWAN-based CPS implementation under stress, we conducted experiments simulating network congestion. These tests aimed to evaluate system performance under varying traffic loads, a crucial consideration for real-world deployments. We systematically varied the airtime utilization by adjusting the interval between transmitted packets, effectively simulating different levels of network congestion. This allowed us to determine the maximum throughput achievable within the constraints of our CPS application scenarios. Through these experiments, we determined an optimal inter-packet transmission interval of approximately 20 seconds. This value balances the need for timely data delivery with the limitations imposed by LoRaWAN's duty cycle restrictions and the specific requirements of our defined scenarios and hardware components. This empirically derived interval ensures reliable operation even under high traffic loads, contributing to the overall resilience and practicality of our proposed system.

Regarding buffer size setup in wireless node, the LoRa modules used (e.g., SX1276-based) typically have 64-byte buffers for both transmission and reception. Considered payload sizes (two, five, and nine bytes) were well within this buffer limit, so congestion was not due to buffer overflow, but rather due to increased channel contention and airtime saturation. To ensure that network congestion was indeed occurring, we relied on multiple indicators: 1) Observable packet loss at higher transmission rates, 2) Variations and degradation in RSSI and SNR, 3) Changes in average inter-packet delay, 4) Reduced success rate of transmissions over time. These empirical indicators, combined with controlled variation of traffic load, provide strong evidence that the network experienced congestion-like behavior during the experiments.

4.5. The Effect of LoRa Transmission Distance

Indeed, one of LoRa strength lies in its capability for long-range communication, often spanning several kilometers. In this study, the primary objective was to isolate and evaluate the impact of transient faults—specifically EMI and PSD—on the robustness of LoRaWAN communication. To achieve controlled, repeatable, and focused fault injection experiments, a short-range physical setup was deliberately chosen. This ensured that signal attenuation due to distance did not confound the effects being studied. Therefore, the effects of background noises (due to channel or external conditions) are removed. However, while the experimental distance was limited, the findings are still meaningful for long-range scenarios for several reasons:

1. LoRa's modulation scheme (CSS) is inherently robust against noise and interference, and this robustness is independent of transmission distance but sensitive to signal quality (RSSI, SNR) which was evaluated.

Accepted by Scientia Iranica

2. EMI effects studied here relate to external disturbances at the device level (e.g., coupling to PCB traces or antennas), which can happen regardless of transmission range.
3. PSD faults primarily affect the transmitter’s hardware operation rather than the propagation channel, so their impact would similarly manifest even in long-range scenarios.

5. Evaluation Results and Discussion

Since the fault injection experiments have been conducted physically, controllability and observability have been performed at a level that allows access through designers (or end-users). In other words, in the process of fault injection, efforts have been made to conduct tests with the desired accuracy, and the reports received are influenced by the outputs that the implemented system is capable of reporting. The extractable reports have been obtained through the information from the transmitting device, the gateway interface between the transmitter and receiver, as well as the receiving device. Consequently, the presentation of results is limited to the information that can be extracted from these three devices, which includes packet loss, RSSI, and SNR, as well as checking whether the content of the packets has been received correctly or not. Subsequently, the effects of each of the fault injection will be presented in order.

5.1. Electromagnetic Interference

Since the system's input current can be affected by electromagnetic interference (EMI) in the frequency range of 140 to 380 MHz, a clamp filter was used to protect the system against EMI interruptions. Physical evaluations demonstrated that the filter effectively reduces these disturbances, allowing focus on the effects of EMI on LoRa modules. During the tests, no packet loss was observed, indicating robustness in challenging EMI conditions. The analysis also confirmed that the transmitted data remained unchanged, ensuring data integrity. However, initial tests at the operational frequency of the LoRa module showed clear disturbances, including packet loss and system failure. As the system's current input could be affected by electromagnetic interference (EMI) within the 140 to 380 MHz frequency range, a clamp filter was used to protect the system from EMI interruptions. Physical evaluations revealed that the filter effectively mitigated these disturbances, allowing for a focus on the EMI effects on the LoRa modules. Throughout the experiments, no packet loss was observed, demonstrating robustness under challenging EMI conditions. The analysis also confirmed that the transmitted data remained unaltered, ensuring data integrity. However, initial experiments at the LoRa module's working frequency showed clear disruptions, including packet loss and system failure.

5.1.1. EMI Scenario Comparison Analysis

Fig. 5, Fig. 6, and Fig. 7 show that in the *golden* version, stable RSSI values above -35 dBm indicate stable signal reception without EMI. A consistent trend in all three charts indicates that horizontal EMI has a more significant negative impact compared to vertical EMI. This is evident from the larger deviations from the *golden* references in *scenarios 4, 5,* and *6*, all of which are exposed to horizontal EMI. This suggests that horizontal interference waves may cause more disruption in signal reception. Figures 5 to 7 show that, in the "*golden*" version, consistently strong RSSI values above -35 dBm represent stable signal reception without EMI. A consistent trend across all three graphs is the more significant negative impact of horizontal EMI compared to vertical EMI. This is evident from the larger deviations from the *golden* references in *scenarios 4, 5,* and *6*, all subjected to horizontal EMI. This suggests that horizontal interfering waves may be more likely to disrupt signal reception.

Scenario 1 (vertical EMI, two bytes) demonstrates a lower RSSI compared to *golden 1*, particularly between uplink counts 0-10 and 25-35, indicating a noticeable impact of vertical EMI. In contrast, *scenario 4* (horizontal EMI, two bytes) exhibits a significant RSSI drop compared to both *golden 1* and *scenario 1*. *Scenario 5* (horizontal EMI, five bytes) shows a considerable RSSI decrease compared to *golden 2* throughout the transmission, indicating that horizontal EMI consistently affects signal reception even with moderate payloads. *Scenario 6* (horizontal EMI, nine bytes) shows significant RSSI degradation around uplink counts 45-50 compared to *golden 3*, confirming the overall impact of horizontal EMI, especially with larger payloads. This is most prominently illustrated in *scenario 6*, where the larger nine-byte payload results in a significantly more pronounced RSSI drop compared to other scenarios.

Accepted by Scientia Iranica

Further investigation is needed to gain a comprehensive understanding of the relationship between EMI, payload size, and RSSI. This can be achieved by comparing the lowest possible payload size to the maximum payload size based on modifications and standards. As seen in Fig. 8, Fig. 9 and Fig. 10, the *golden* scenarios, free from EMI, consistently show high SNR values across all measured instances, with median SNR values for the *golden* versions being approximately 11 dB, 11.5 dB, and 12 dB, respectively. This indicates optimal performance of the LoRa module without interference, maintaining strong signal quality. In contrast, scenarios with EMI show noticeably lower median SNR values. The *golden scenario* 1 and *Scenario 4* exhibit higher median values than *Scenario 1*, suggesting that horizontal EMI has a lesser impact on the LoRa module than vertical EMI. *Scenario 1*, the vertical scenario, has the lowest median value. The interquartile range (IQR), representing the spread of the middle 50% of SNR values, is relatively narrow in the *golden scenarios*, indicating consistent signal quality. In contrast, scenarios with EMI display a broader IQR, reflecting greater variability and inconsistency in signal quality. *Scenario 2*, which involves vertical EMI, shows a wider IQR and several outliers, highlighting the significant disruption caused by EMI.

In the *golden scenarios*, the lower percentiles (25th percentile or first quartile Q1) remain high, indicating strong signal quality even at the lower end of the data distribution. However, in EMI scenarios, the lower percentiles drop significantly. For example, *scenario 1* and *scenario 4* show much lower 25th percentile values compared to their *golden* versions, highlighting that a substantial portion of data points in these scenarios suffer from degraded signal quality due to EMI .

When comparing the impact of horizontal versus vertical EMI, vertical EMI appears to have a more pronounced negative effect on the LoRa module's performance. *Scenario 4* generally shows higher median SNR values than *Scenario 1*, suggesting that horizontal EMI is less disruptive than vertical EMI. Similarly, *scenario 5* exhibits a slight improvement in median SNR over *scenario 2*. Despite these differences, all scenarios maintain acceptable SNR medians, with most values within the acceptable range, demonstrating the LoRa module's robustness against EMI.

5.1.2. Average Duration Between Two Consequent Packets

As shown in Fig. 11, Fig. 12 and Fig. 13, for each *golden* version with different payload sizes, the average time difference between uplink packets remains relatively stable compared to the equivalent scenarios with the presence of EMI. Across all payload sizes, whether vertical or horizontal the presence of EMI does not significantly affect the average time difference between uplink packets. The variations observed are minimal and do not establish a consistent pattern.

No clear trend suggests that different payload sizes consistently impact the time difference between uplink packets. The variations due to payload size are minimal and overshadowed by the negligible impact of EMI. This indicates that the average time difference between uplink packets remains relatively stable regardless of payload size and EMI presence.

5.1.3. EMI Comparison Discussion

A research into the impact of EMI on ZigBee technology [17] indicates that for each type of noise, the Packet Error Rate (PER) rises as the Signal-to-Noise Ratio (SNR) decreases. Additionally, the PER increases with the correlation of the modulated monofractal, meaning that correlated noise results in a higher PER compared to uncorrelated noise [17]. Another study examining electromagnetic interference from wireless devices on NB-IoT technology [18] revealed that the most significant harm caused by interference to an NB-IoT device's receiver is errors in the data received from the base station. Such errors can result in delays and inaccuracies in controlling and adjusting NB-IoT devices, which is particularly critical for essential medical devices and high-risk patients. Conversely, the interference caused by NB-IoT devices to 4G/5G mobile stations and Radio Local Area Network (RLAN) access points is generally considered benign, with the worst-case scenario being reduced data rates or brief communication outages.

In an experiment assessing the effects of electromagnetic interference on Wi-Fi within the frequency range of 2460-2480 MHz [19] [20], findings showed a data loss of 32.8% and latency reaching up to 3016 *ms*, rendering the network nearly unusable for most applications. When the wireless network was utilized solely for basic file transfers between two laptops, it failed after less than 30 seconds due to extremely poor performance.

5.2. Power Supply Disturbance

5.2.1. PSD Effect on RSSI

Accepted by Scientia Iranica

Effects of PSD transient faults on *scenarios 1* to *9* is depicted in Fig. 14. The higher the RSSI value, the stronger the received signal, while a lower value indicates a weaker signal. Generally, a signal strength of -30 dBm to -60 dBm is considered very strong, -60 dBm to -70 dBm is strong, -70 dBm to -80 dBm is average, -80 dBm to -90 dBm is weak, and anything below -90 dBm is considered very weak. As seen in Fig. 14, RSSI in all scenarios and the *golden* version falls within the range of -30 dBm to -60 dBm, indicating a very strong received signal. In *scenarios 3, 4, 5,* and *9*, a few packets are in the range of -60 dBm to -70 dBm, which is still within the strong signal range. The slight drop in RSSI in these areas can be attributed to the impact of power supply disturbances on the received signal. Finally, the height of the box represents the Interquartile Range (IQR), indicating that in all scenarios, 50 percent of the data falls within the very strong signal range.

5.2.2. PSD Effect on SNR

Fig. 15 shows PSD effect on SNR in all experiments done in *scenarios 1* to *9*. In the LoRaWAN protocol, considering that the spreading factor (SF) is set to 7, the minimum SNR is 7.5 dBm. According to Fig. 15, a significant amount of data in all scenarios has an SNR higher than 7.5. Since this chart represents the results of packets sent in the presence of injected faults, a small number of data points are below this value, which may be due to the effects of disturbances in the power supply. Finally, the height of the box represents the Interquartile Range (IQR), indicating that in all scenarios, 50 percent of the data fall within the normal range.

5.2.2.1. PSD Effect on Mean Values of RSSI and SNR

The average RSSI and SNR values obtained from all the experiments conducted for each scenario are shown in Fig. 16. In this figure, two independent curves displaying RSSI and SNR are presented. Considering the local variations that occurred in each scenario compared to other scenarios, and that these changes are within the acceptable and normal range for the LoRaWAN protocol, it can be observed that there were no significant changes in the presence of PSD. Particularly, as shown in Fig. 16, average SNR in all scenarios is close to each other and within the normal range, with no significant changes observed. The average RSSI is also in the very strong range across all scenarios. It can be inferred that the mentioned protocol exhibits good resilience regarding PSD transient faults.

5.2.3. Analysis of PSD Duration Effect on Packet Loss

Considering that a total of twenty experiments were conducted in each scenario, resulting in 200 packets sent, some packets were lost during the experiments due to injected faults in the power supply, which caused a voltage drop, preventing LoRa from sending packets. A notable point about LoRa is that if a voltage drop leads to data loss, two types of failures occur. In the first category, after the injection of faults, some packets are lost, but the device restarts and attempts to send other packets. In the second category, LoRa completely fails and stops sending packets, requiring a restart.

As shown in Fig. 17, in *scenarios 1* to *4*, where the duration of fault injection is less than or equal to one second, approximately 10 to 15 packets were not sent, representing about 7.5% of all 200 packets. In *scenarios 5* to *9*, where the duration of fault injection is *two*, *three*, *five*, *seven*, and *ten* seconds, respectively, the number of lost packets starts at *21* and can reach up to *53* during longer times, indicating that over 20% of the data is lost. It can be concluded that the longer the fault injection time, the more data is lost.

5.2.4. Analysis of PSD Effects on Different Payload Size

Scenarios 5, *10*, and *11* share a common fault injection duration of two seconds; however, the packets are sent with different sizes in each scenario. As shown in Fig. 18, in *scenario 5* with a size of two bytes, 21 packets were lost; in *scenario 10* with a size of five bytes, 29 packets were lost; and in *scenario 11* with a size of nine bytes, 39 packets were lost. It can be concluded that since larger packets require more time for transmission, the likelihood of faults occurring during the transmission of these packets increases. Consequently, the probability of losing sent packets also increases.

5.3. Discussion on Bit Error Rate and Throughput

The performance evaluation of the LoRaWAN network in this study has been carried out with a focus on parameters such as Packet Loss Rate, RSSI, and SNR. During the experiments, transmitted packets were thoroughly examined using the

Accepted by Scientia Iranica

inherent mechanisms of the LoRaWAN network, and only those packets that were not completely received were considered as lost. Given this structure—and the fact that the analyses were conducted at the packet level rather than the bit level—it was not feasible to directly calculate the Bit Error Rate (BER) in this study. This is because BER requires a precise comparison of transmitted and received bits in successfully received communications. In scenarios where a packet was received correctly, it is assumed that the content was error-free at the bit level; otherwise, the packet was categorized as lost and included in the packet loss analysis.

In this study, the primary focus has been on analyzing the effects of EMI and PSD on packet-level performance indicators such as Packet Loss, RSSI, and SNR, in order to assess the stability and resilience of LoRaWAN-based communications under fault-injection conditions. Although throughput was not explicitly measured or reported in the initial version of the paper, we fully recognize its importance—particularly in applications that require frequent or rapid data transmission. However, in our experiments, the data transmission rate was deliberately kept low (e.g., one packet every 20 seconds) to comply with the LoRaWAN network's duty cycle limitations. Therefore, the resulting throughput is intentionally low and is not considered a limiting factor.

Considering the data transmission rate in the experiments (approximately one packet every 20 seconds) and the size of the transmitted packets (e.g., five bytes), an estimate of the throughput can be given as follows:

Throughput ≈ (Packet Size × 8) / Interval
For a packet size of 5 bytes:
Throughput ≈ (5 × 8) / 20 = 2 bits per second (bps)

Therefore, this value is very low and aligns with the characteristics of LoRaWAN networks, which are designed for low power and low data rates. The purpose of these experiments was to examine the impact of error injections (EMI/PSD) on reliability, not to increase data capacity.

It is worthy to mention that we are limited to report those performance indicators that can be accessible from the physical system. Since the experimental setup is done at physical level, we included those parameters that were possible to get by the reports given by the sender node, the gateway and the receiver node.

5.4. A solution to mitigate the effects of PSD

Based on the results of previous studies, a potential solution to enhance the performance of LoRaWAN networks under PSD conditions can be achieved. *Class A* devices in the LoRaWAN architecture are designed to spend most of their time in sleep mode and only wake up when data needs to be transmitted. This feature can be utilized to design a control mechanism that prevents data transmission under unfavorable conditions.

In one possible solution, by continuously monitoring the power supply voltage, a decision can be made whether the device should remain in sleep mode or initiate transmission. Specifically, during each transmission cycle, the power supply voltage can be measured through its analog input, and if a voltage drop beyond a certain threshold is detected, the next transmission will be delayed. This delay will keep the device in sleep mode and prevent transmission under unstable conditions. To implement this idea, parameters such as *TX-Interval* and *RX-delay* in the LoRa library of Arduino can be modified so that these settings are dynamically adjusted according to online conditions, without altering the underlying LoRaWAN protocol structure. Such a solution could potentially reduce energy consumption and improve the communication stability of the network due to increasing sender time in sleep mode.

6. Conclusion and future work

This paper examined the vulnerability of the LoRaWAN protocol in the presence of two significant issues: 1) EMI and 2) PSD. In the targeted network, commonly found in cyber-physical systems, a LoRa gateway is utilized. After conducting numerous physical fault injection experiments on LoRa sender module, we concluded that this protocol exhibits considerable robustness in the presence of EMI issues, particularly at frequencies outside its operational range. Additionally, the contribution of polarization may vary based on the experimental results. It is worthy to mention that EMI with horizontal polarity of antenna has negative impacts more than that of vertical one. In the presence of PSD, an increase in the duration of disturbances from the power source leads to a higher packet loss rate; however, the packets received at the gateway maintain a good signal quality, with appropriate RSSI and SNR values. The similar effects where observed when payload size of packets increases. The larger the payload size of a packet, the higher the probability of packet loss. In other words, PSD issues result in packet loss, which is particularly dangerous for safety-critical applications such as mining, necessitating

Accepted by Scientia Iranica

appropriate measures to be taken at either the application level or system level to ensure resilience against these issues.

The robustness of LoRaWAN networks presents numerous opportunities for future research and development. Some of the key areas for further exploration include: 1) To integrate with other communication technologies: Future research can explore the integration of LoRa with complementary technologies such as NB-IoT or 5G. Such hybrid networks can provide improved coverage, lower latency, and enhanced robustness by leveraging the strengths of different communication paradigms in complementary ways. 2) To investigate longer range and higher data rates: Exploring novel hardware solutions and software modifications to enhance LoRa's range and data rates while maintaining energy efficiency is an exciting research frontier. 3) To secure LoRaWAN: With growing concerns about security in IoT, the development of robust security protocols tailored for LoRaWAN is another promising research avenue. Enhancing encryption methods, authentication mechanisms, and anti-jamming techniques will ensure that LoRa-based networks remain secure as they scale.

References

[1] Yaccoub, J. P. A., Salman, O., Noura, H. N., et al, "Cyber-physical systems security: Limitations, issues and future trends," *Elsevier Journal of Microprocessors and Microsystems (MICPRO)*, **77**(1), pp. 103201 (2020), DOI:10.1016/j.micpro.2020.103201.

[2] Bonilla, V., Campoverde, B., and Yoo, S. G., "A Systematic literature review of LoRaWAN: Sensors and applications," *Sensors*, **23**(20), pp. 8440, (2023), DOI:10.3390/s23208440.

[3] Kwasme, H. and Ekin, S., "RSSI-based localization using LoRaWAN technology," *IEEE Access*, **7**(1), pp. 99856-99866, (2019), DOI: 10.1109/ACCESS.2019.2929212.

[4] Jouhari, M., Saeed, N., Alouini, M. S., et al., "A survey on scalable LoRaWAN for massive IoT: Recent advances, potentials, and challenges," *IEEE Communications Surveys & Tutorials*, **25**(3), pp. 1841-1876, (2023), DOI: 10.1109/COMST.2023.3274934.

[5] Centenaro, M., Vangelista, L., Zanella, A., et al., "Long-range communications in unlicensed bands: The rising stars in the IoT and smart city scenarios," *IEEE Wireless Communications*, **23**(5), pp. 60-67, (2016), DOI: 10.1109/MWC.2016.7721743.

[6] Gangolli A., Mahmoud Q. H., and Azim A., "A systematic review of fault injection attacks on IoT systems," *Electronics*, **11**(13), pp. 2023-2023, (2022), DOI: 10.3390/electronics11132023.

[7] Musonda, K., Ndiaye, M., Libati, M., et al., "Reliability of LoRaWAN communications in mining environments: A survey on challenges and design requirements," *Journal of Sensor and Actuator Networks*, **13**(1), pp. 16 (2024), DOI: 10.3390/jsan13010016.

[8] Petajajarvi, J., Mikhaylov, K., Roivainen, A., et al., "On the coverage of LPWANs: Range evaluation and channel attenuation model for LoRa technology," *International Conference on ITS Telecommunications (ITST)*, pp. 55-59 (2015), DOI:10.1109/ITST.2015.7377400.

[9] Kartakis, S., Choudhari, B. D., Gluhak, A. D., et al., "Demystifying low-power wide-area communications for city IoT applications," *10th ACM International Workshop on Wireless Network Testbeds, Experimental Evaluation, and Characterization*, pp. 2-8 (2016), DOI:10.1145/2980159.2980162.

[10] Lombardo, A., Parrino, S., Peruzzi, G., et al., "LoRaWAN versus NB-IoT: Transmission performance analysis within critical environments," *IEEE Journal of Internet of Things*, **9**(2), pp. 1068- 1081 (2022), DOI: 10.1109/JIOT.2021.3079567.

[11] Boano, C. A., Marco, C. and Kay, R., "Impact of temperature variations on the reliability of LoRa," *7th International Conference of Sensor Network*, pp. 39-50 (2018), DOI: 10.5220/0006605600390050

[12] Malisuwan, S., Santiyanon, J. and Sivaraks, J., "The performance of bluetoothtm transmissions in electromagnetic interference environment," *International journal of the computer, the internet and management*, **11**(2), pp. 1-14 (2003), DOI: 10.1109/ICSMC2.2003.1429163.

[13] Mandal, A., De, S., "Analysis of wireless communication over electromagnetic impulse noise channel" *IEEE Transactions on Wireless Communications*, **22**, 1187-1200 (2023), DOI: 10.1109/TWC.2022.3203039.

[14] Adelantado F., Vilajosana X., Peiro P. T., et al., "Understanding the limits of LoRaWAN," *IEEE Communications magazine*, **55**(9), pp. 34-40, (2017), DOI: 10.1109/MCOM.2017.1600613.

[15] Ruminot N., Estevez C., Montejo-Sánchez, S., "A novel approach of a low-cost voltage fault injection method for resource-constrained IoT devices: design and analysis," *Sensors journal*, **23**(16), pp. 7180 (2023), DOI: 10.3390/s23167180.

[16] Wang, K., Xiao, S., Ji, X., et al., "Volttack: Control IoT devices by manipulating power supply voltage," *IEEE Symposium on Security and Privacy (SP)*, pp. 1771-1788 (2023), DOI: 10.1109/SP46215.2023.10179340.

[17] Delarea S., Oren Y., "Practical, low-cost fault injection attacks on personal smart devices," *Journal of Applied Sciences*, **12**(1), pp. 417 (2022) DOI: 10.3390/app12010417.

[18] Ferens, K., Woo, L. and Kinsner, W., "Performance of ZIGBEE networks in the presence of broadband electromagnetic noise," *Canadian Conference on Electrical and Computer Engineering*, pp. 407-410, (2009) DOI: 10.1109/CCECE.2009.5090164.

Accepted by Scientia Iranica

[19] Svistunou, A., Mordachev, V., Sinkevich, E., et al., “Analysis of EMC between equipment of wireless systems and medical NB IoT devices,” *International Symposium on Electromagnetic Compatibility–EMC Europe*, pp. 1-6 (2023), DOI: 10.1109/EMCEurope57790.2023.10274259.

[20] Muratovic, J., Josic, K. and Papic, S., “Analysis of the impact of electromagneticinterference on the performance of a household wireless network,” *44th International Convention on Information, Communication and Electronic Technology (MIPRO)*, pp. 519-522 (2021), DOI: 10.23919/MIPRO52101.2021.9597120.

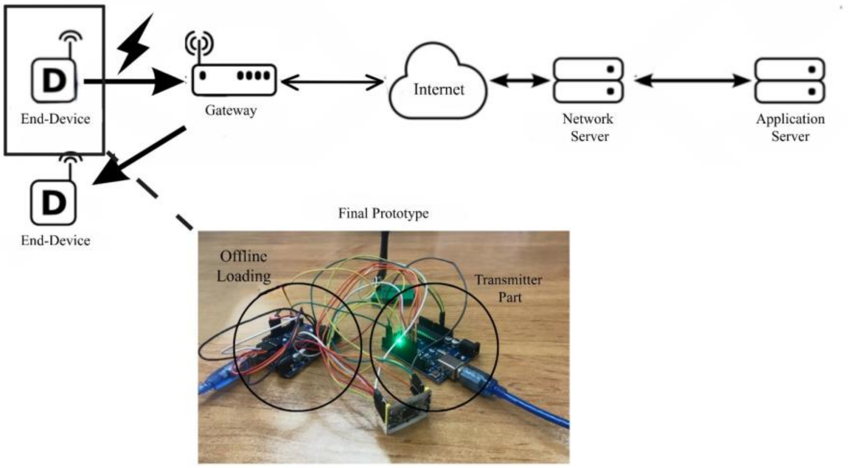


Fig. 1.

Acc Scientia Iranica

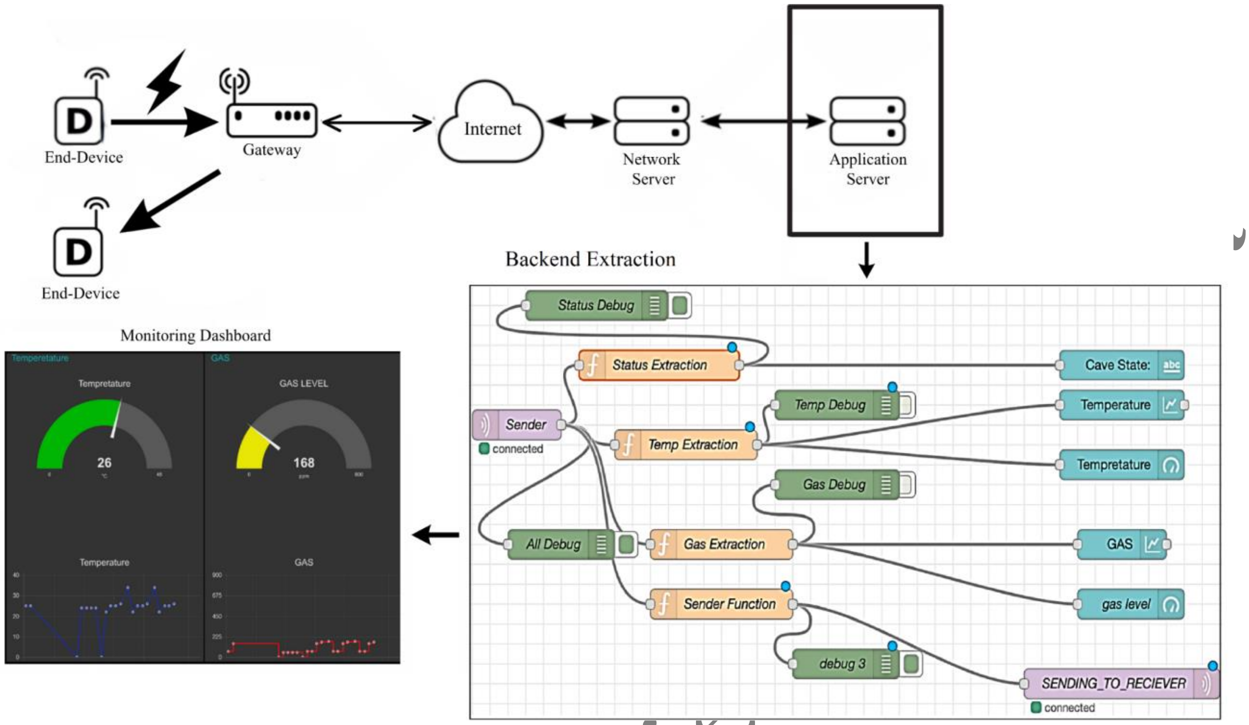


Fig. 2.

Acce Scie

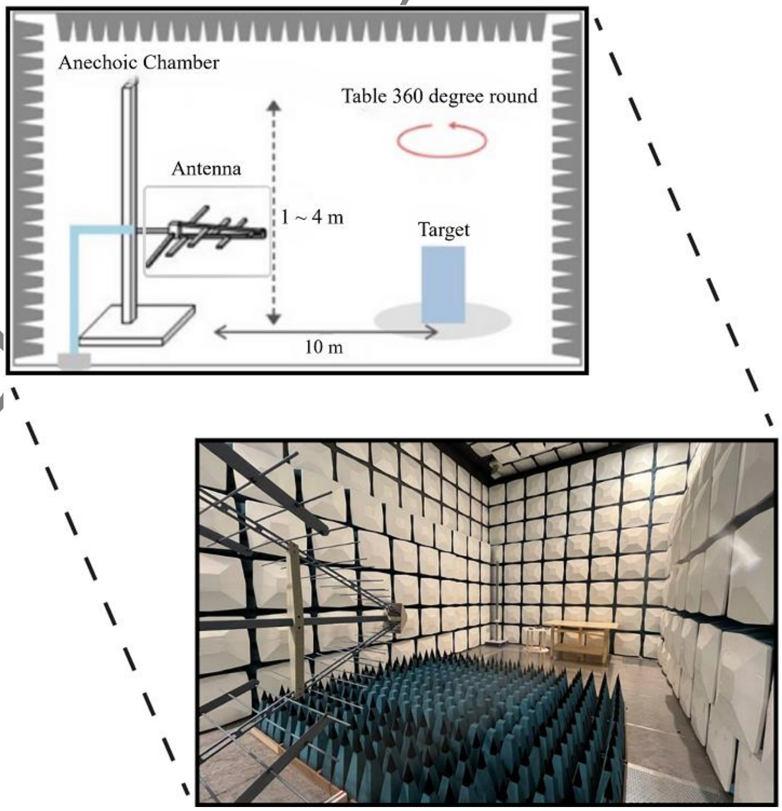


Fig. 3.

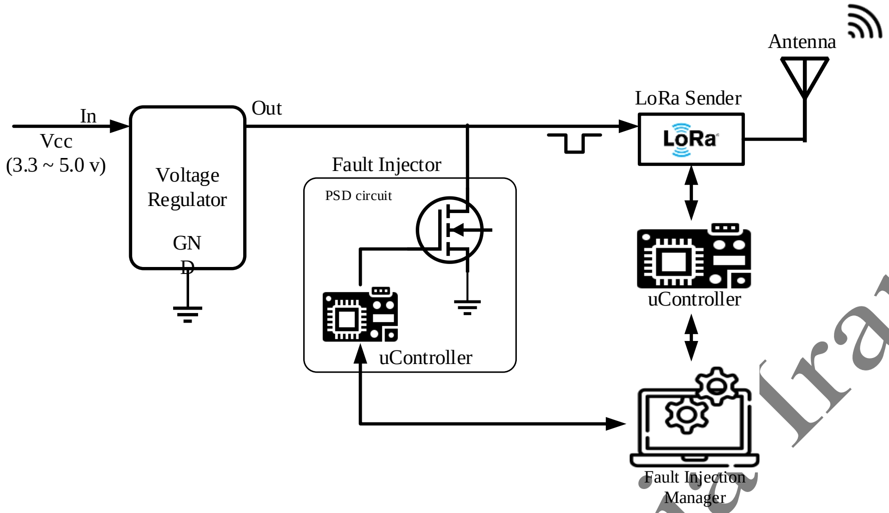


Fig. 4.

Accepted by Scientia Iranica

Table 1.

Scenario Number	Packet Size (Byte)	Antenna Polarization
1	2	Vertical
2	5	Vertical
3	9	Vertical
4	2	Horizontal
5	5	Horizontal
6	9	Horizontal

Table 2.

Scenario Number	Total Experiments	Fault Duration (ms)	Packet Size (bytes)
1	20	100	2
2	20	200	
3	20	500	
4	20	1000	
5	20	2000	
6	20	3000	
7	20	5000	
8	20	7000	
9	20	10000	
10	20	2000	5
11	20	2000	9

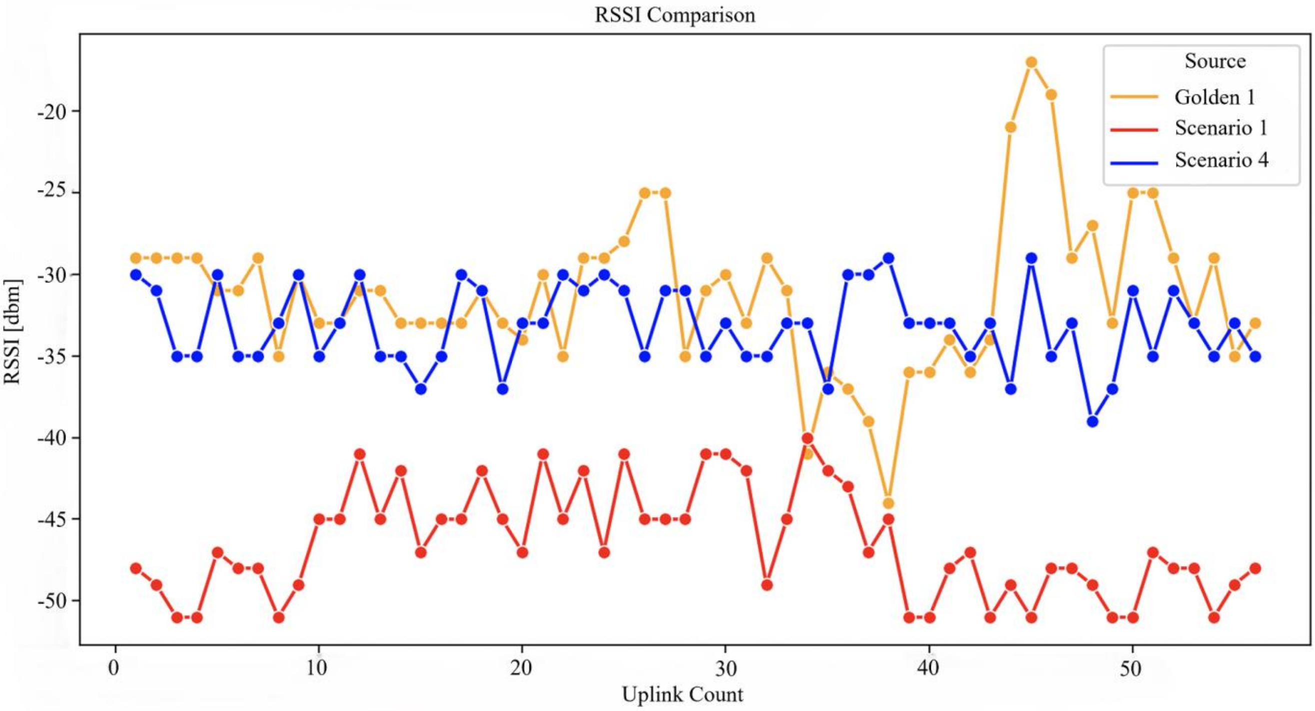

RSSI Comparison
RSSI [dbm]
-20
-25
-30
-35
-40
-45
-50
Uplink Count
0
10
20
30
40
50
Source
Golden 1
Scenario 1
Scenario 4

Fig. 5.

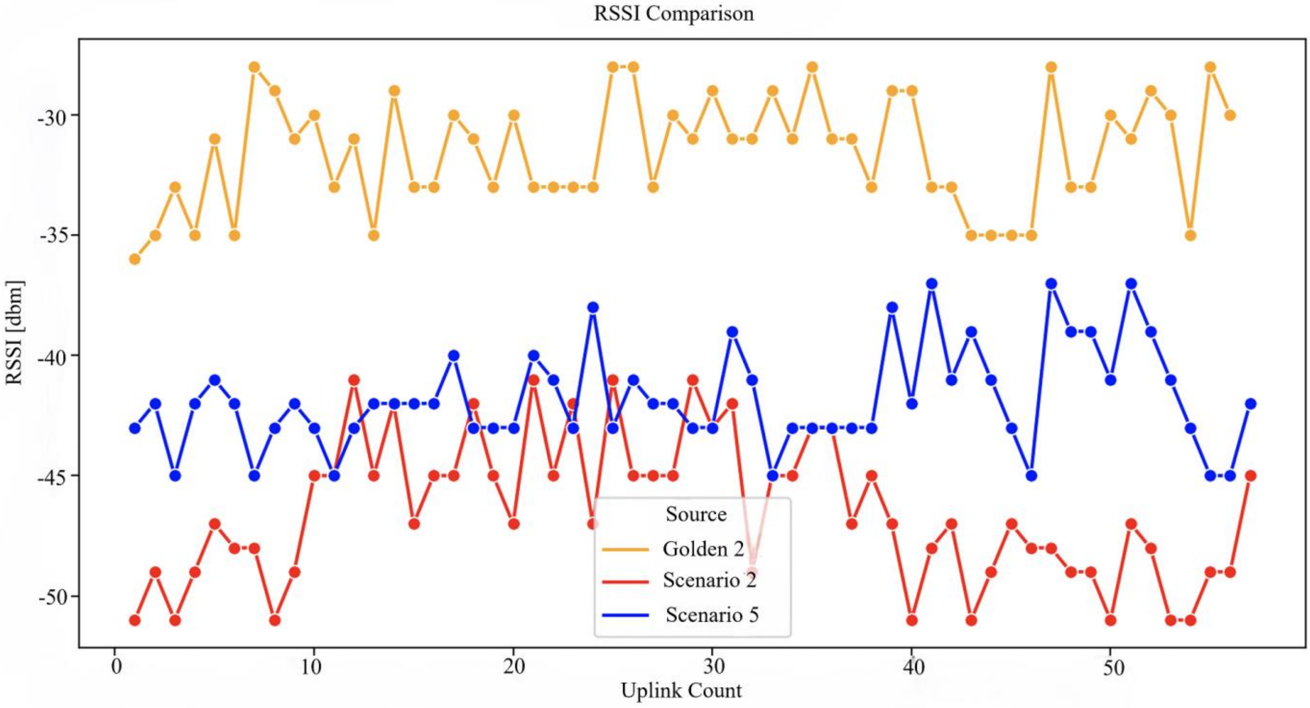

RSSI Comparison
RSSI [dbm]
-30
-35
-40
-45
-50
Uplink Count
0
10
20
30
40
50
Source
Golden 2
Scenario 2
Scenario 5

Fig. 6.

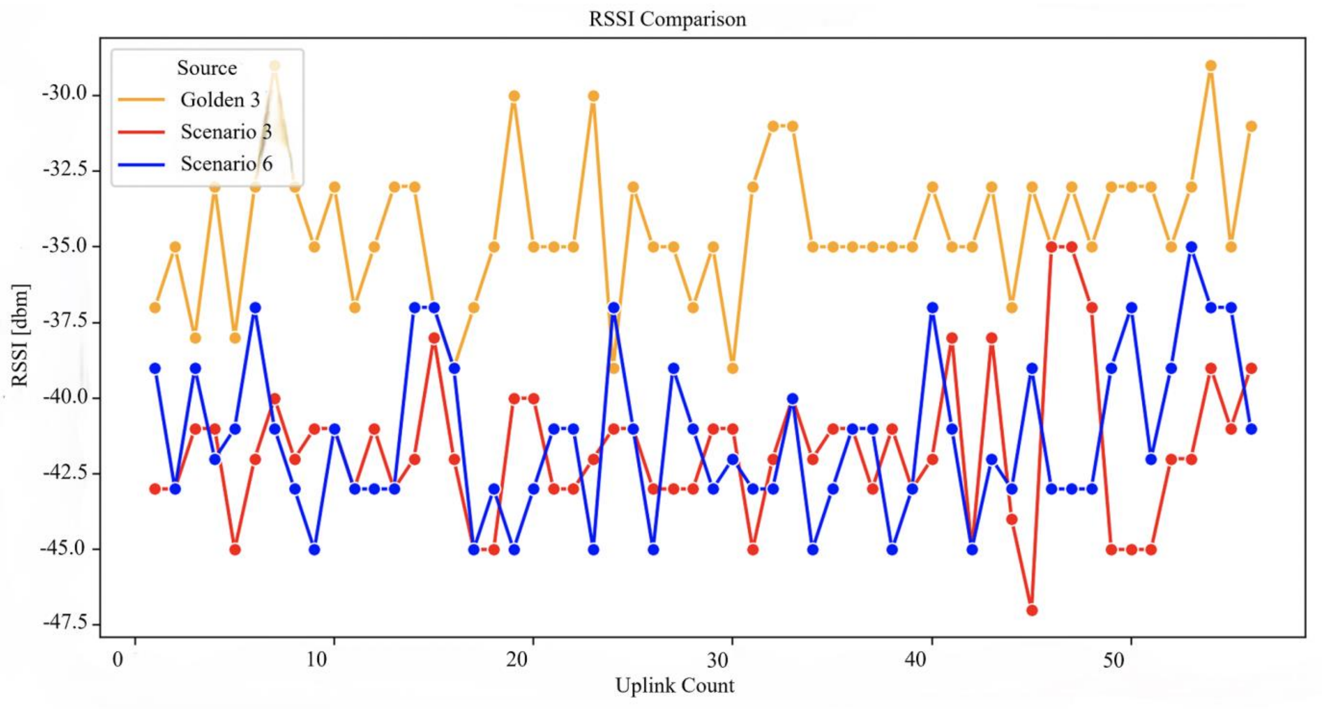


Fig. 7.

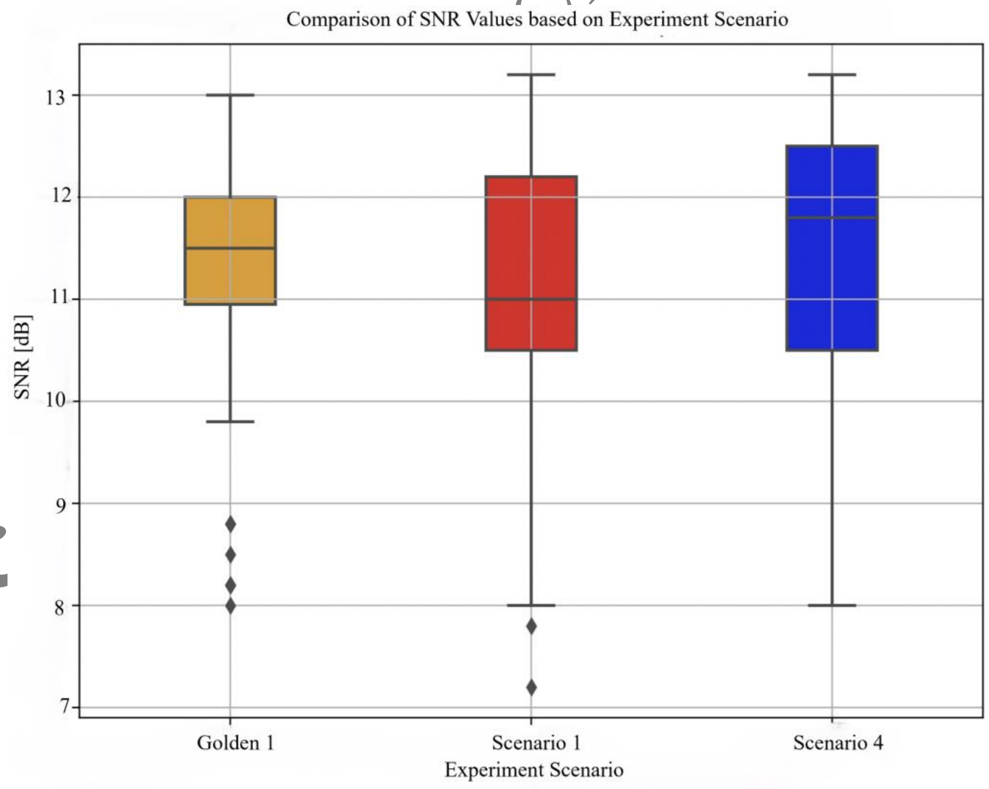


Fig. 8.

Ac cie

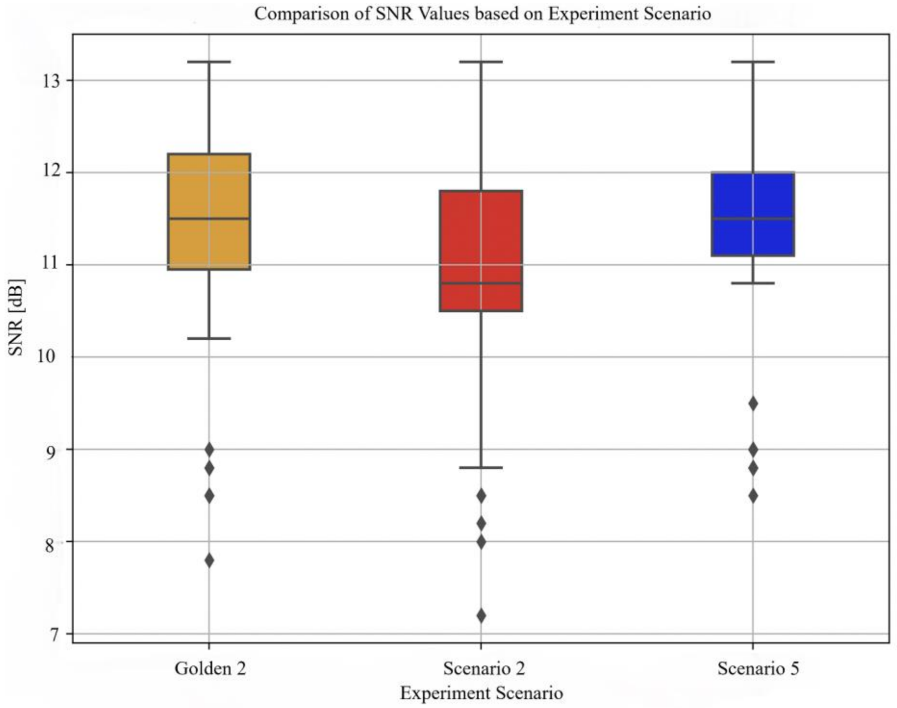


Fig. 9.

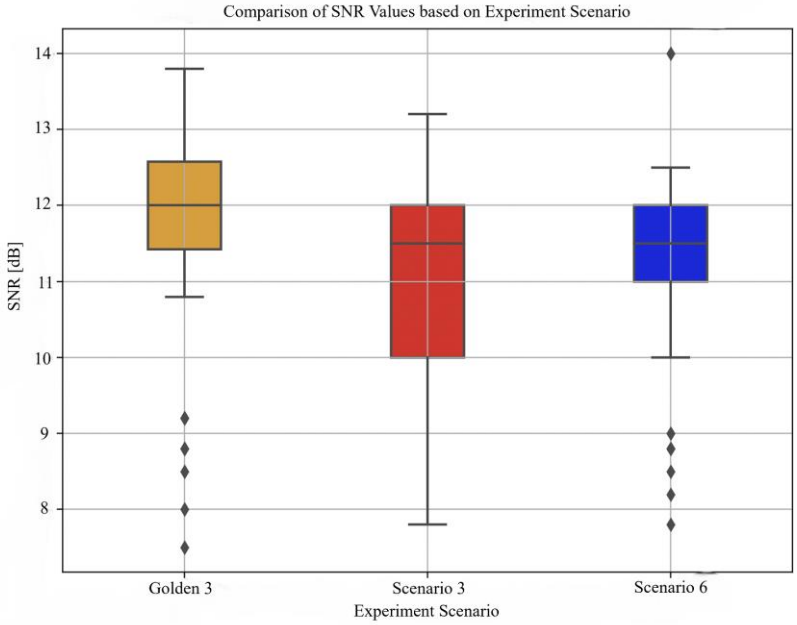


Fig. 10.

Accepted Scientia Iranica

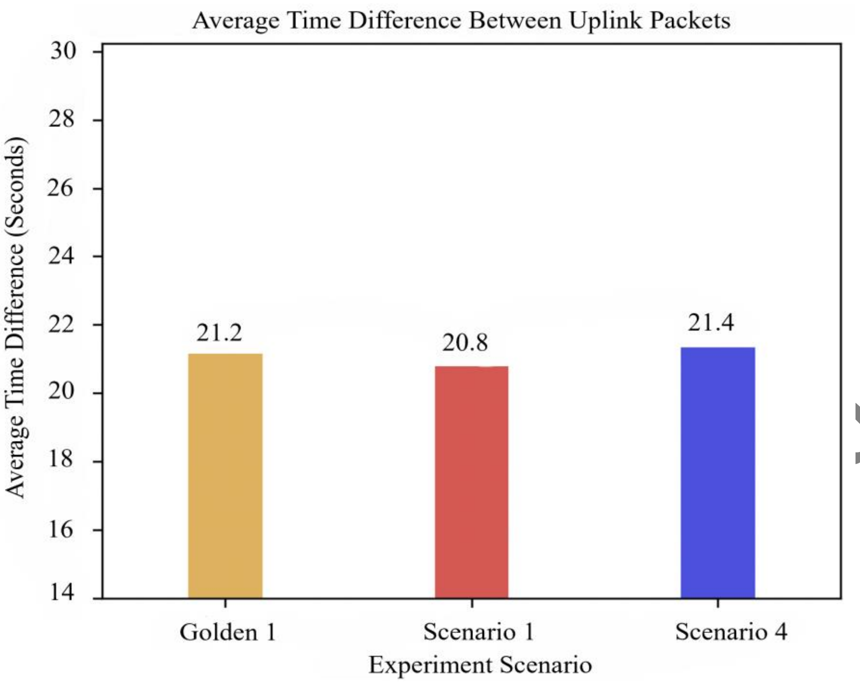


Fig. 11.

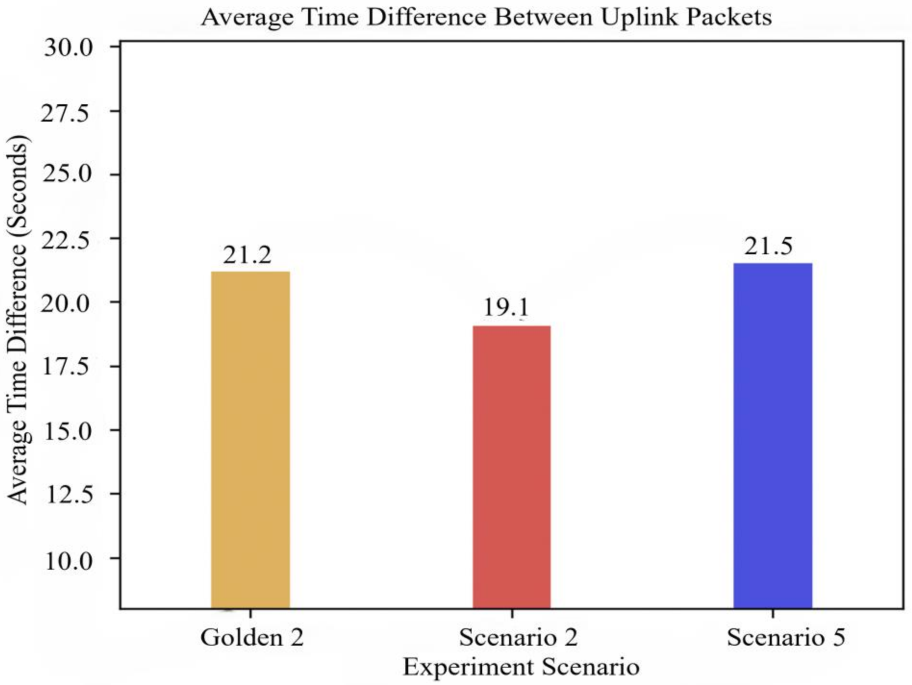


Fig. 12.

Accepted in Scientia Iranica

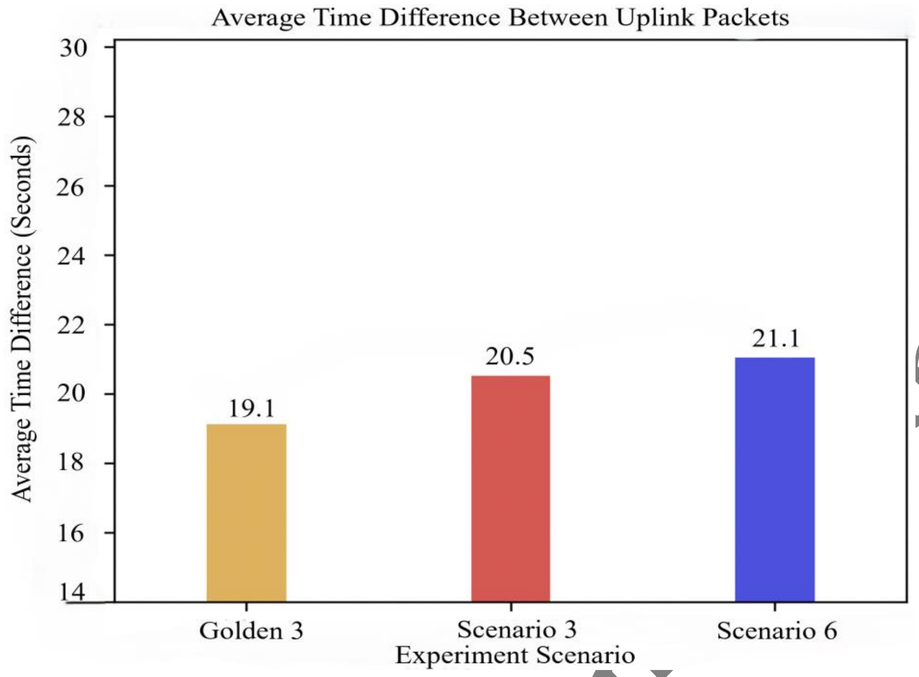


Fig. 13.

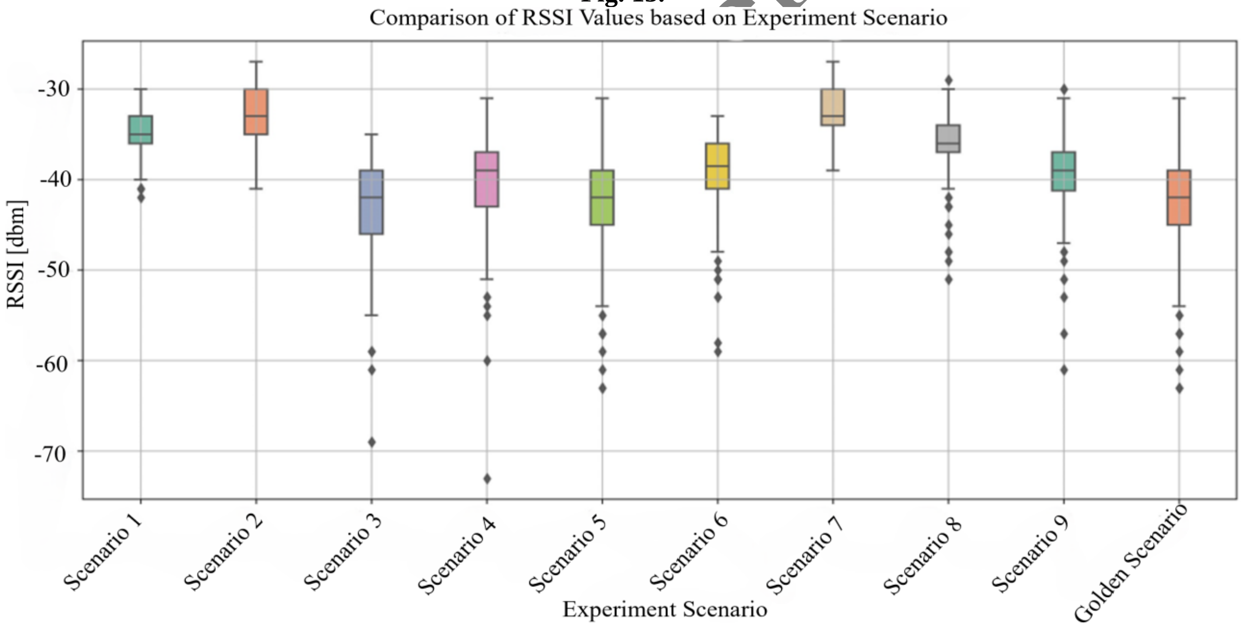


Fig. 14.

Accepted Scientia Iranica

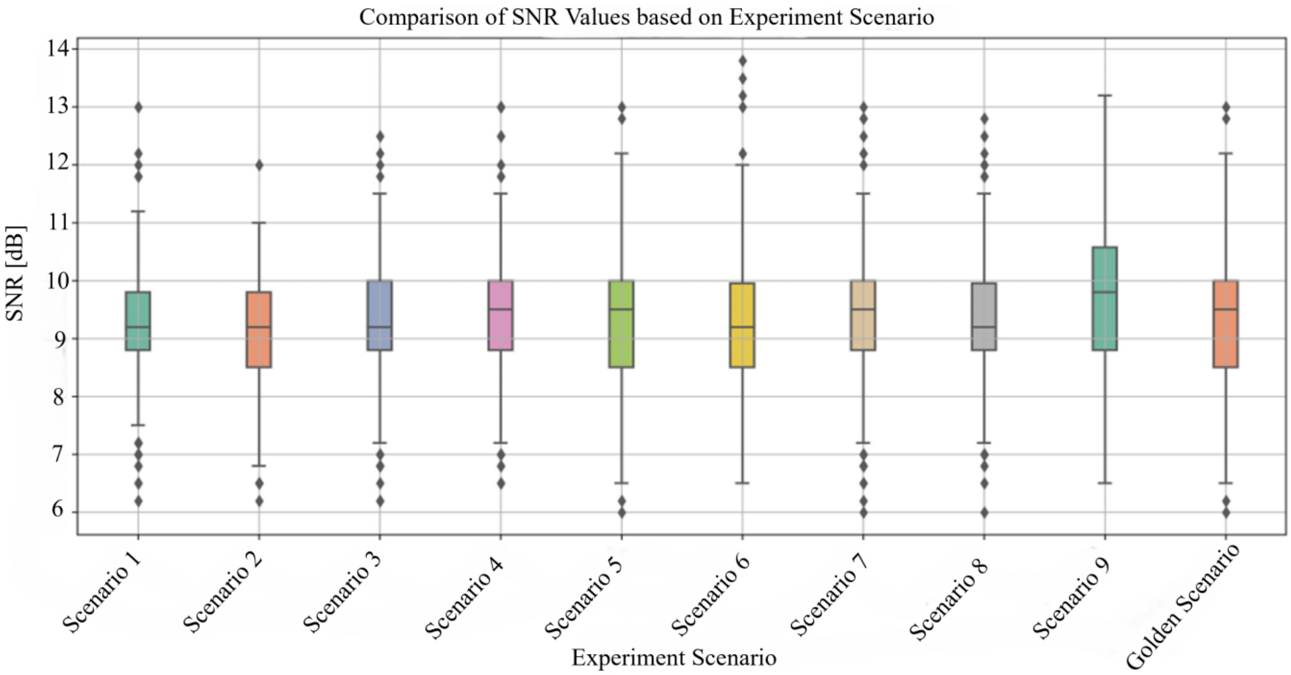
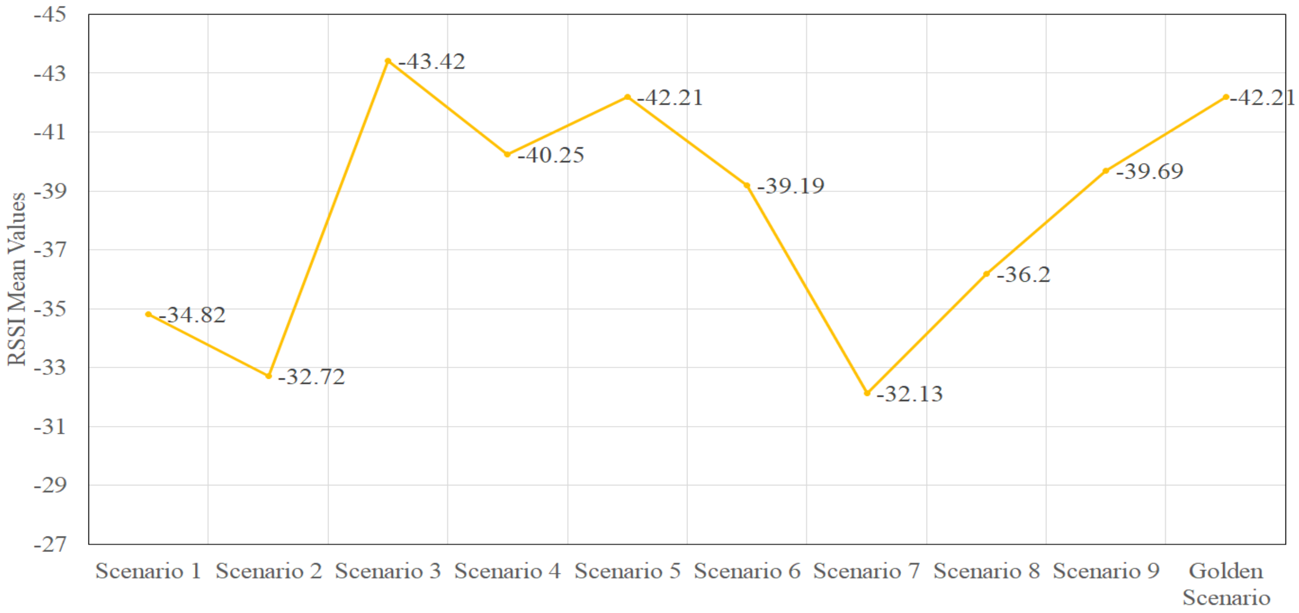
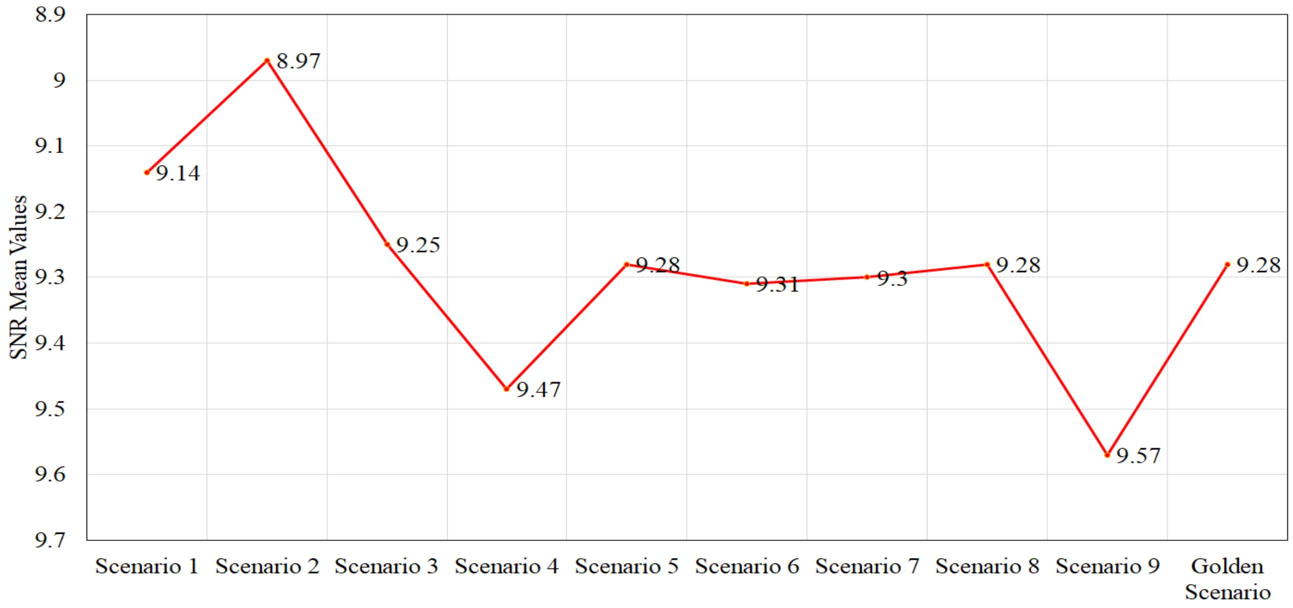


Fig. 15.



(a) Comparison of RSSI mean values



(b) Comparison of SNR mean values

Fig. 16.

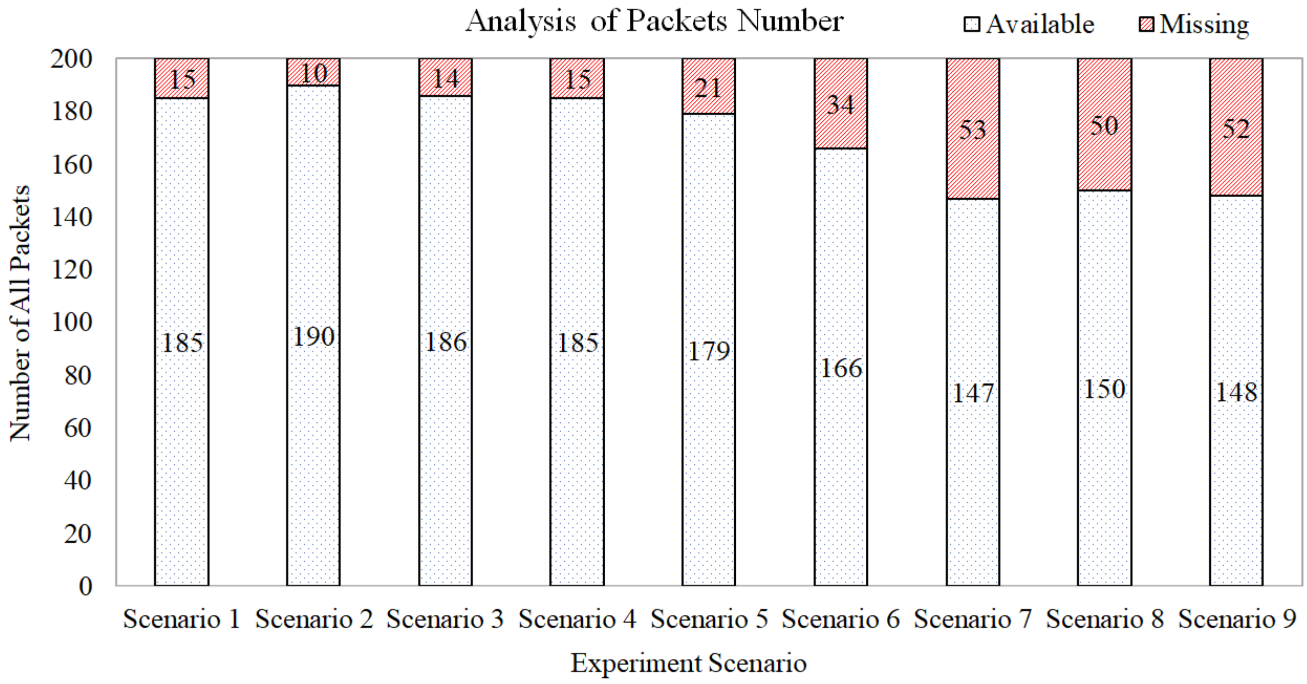


Fig. 17.

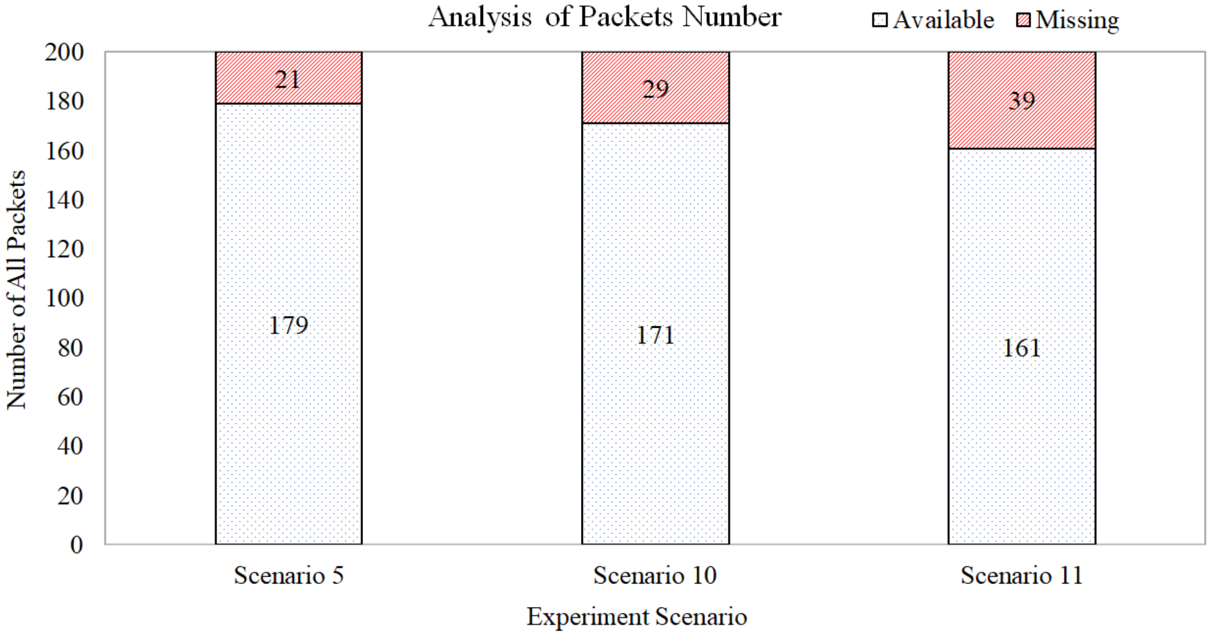


Fig. 18.

Biographies

Faezeh Saghaei received her MSc degree from the Department of Computer Engineering, Amirkabir University of Technology (Tehran Polytechnic) in 2025. Her research interests are fault injection, Internet-of-Things, wireless communication, cyber-physical system, and physical dependability evaluation.

Hamid Reza Zarandi received the BSc, MSc, and PhD degrees all from the Department of Computer Engineering at the Sharif University of Technology, Iran, in 2000, 2002, and 2007, respectively. He is currently an associate professor with the Department of Computer Engineering at Amirkabir University of Technology (Tehran Polytechnic). His research interests include dependability evaluation using fault injection techniques, fault-tolerant computing, dependable computer architecture, and high-performance computing, on which he has published more than 100 referred conferences and journal papers. He established the "Design and Analysis of Dependable Systems (DADS)" laboratory at Amirkabir University, in 2007.

Morteza Tavakkoli received the BSc degree from the Department of Computer Engineering, Amirkabir University of Technology (Tehran Polytechnic) in 2023. He is now MSc student in Ontario Tech University, Canada. His research interests include Internet-of-Things, wireless communication, machine learning methods, data mining, embedded IoT solutions and vehicular automation.

Accepted by Scientia