Computers & Security 140 (2024) 103778

Contents lists available at ScienceDirect

Computers & Security

journal homepage: www.elsevier.com/locate/cose

M-RL: A mobility and impersonation-aware IDS for DDoS UDP flooding attacks in IoT-Fog networks

Saeed Javanmardi [a], Meysam Ghahramani [b], Mohammad Shojafar [c], Mamoun Alazab [d], Antonio M. Caruso [a,*]

[a] *Department of Mathematics and Physics, Salento University, Lecce, Italy*
[b] *Department of Mathematics and Computer Science,Faculty of Basic Sciences, Lorestan University, Iran*
[c] *5G & 6G Innovation Centre (5G/6GIC), Institute for Communication Systems (ICS), University of Surrey, Guildford, United Kingdom*
[d] *Faculty of Science and Technology, Charles Darwin University, NT, Australia*

ARTICLE INFO

MSC:
0000
1111

Keywords:
IoT-Fog networks
Data security
Intrusion Detection System (IDS)
Received Signal Strength (RSS)
Rate Limiting (RL)

ABSTRACT

The Internet of Things (IoT) has recently received a lot of attention from the information and communication technology community. It has turned out to be a crucial development for harnessing the incredible power of wireless media in the real world. The nature of IoT-Fog networks requires the use of defense techniques who are light and mobile-aware. The edge resources in such a distributed environment are open to various safety hazards. DDoS UDP flooding attacks are the most frequent threats to edge resources in IoT-Fog networks. It is crucial for sabotaging fog gateways and can overcome traditional data filtering techniques. This paper introduces M-RL, a lightweight intrusion detection system with mobility awareness that can detect DDoS UDP flooding attacks while taking into account adversarial IoT devices that engage in IP spoofing. To this end, this paper analyzes the malicious behaviors that result in anonymity against Rate Limiting and Received Signal Strength (RSS)-based approaches, combines their advantages, and addresses their vulnerabilities. We test our method in different contexts to achieve that goal, and we find that it may decrease the accuracy of the RL, RSS, and RSS-RL methods to 70%, 48.9%, and 64.3%, respectively. The outcomes demonstrate the proposed approach's resistance to software-based source address forgery, impersonation, and signal modification. It offers more than 99% accuracy and supports node mobility. In this case, the best possible accuracy of the previous methods is 77%.

1. Introduction

The Internet of Things (IoT) is the outcome of a slew of devices linked together in a communicating-actuating network. Fog computing is a leading edge paradigm that provides delay-sensitive services to IoT applications by leveraging near-user edge resources rather than a remote data center on the cloud layer (Laroui et al., 2021; Javanmardi et al., 2021a). Because of the essential nature of the fog paradigm settings in which the applications are deployed, IoT-Fog infrastructure is vulnerable to security threats. Malicious IoT devices employ malware to infect IoT-Fog services and make them inaccessible. As a result, IoT-Fog security is a significant concern in protecting the IoT-Fog system's hardware and services. (Javanmardi et al., 2021b).

IoT-Fog networks are particularly vulnerable to DDoS attacks. These attacks can overload the network's resources and make the devices and services inaccessible to legitimate users. It can result in a loss of revenue, damage to the network's reputation, and potentially even compromise the security of the devices and data within the network. Network administrators can ensure the availability and security of the fog devices' resources by detecting and mitigating DDoS attacks in real-time. It helps to maintain the trust of IoT devices and ensures the success of the IoT-Fog network. Accordingly, it is crucial to devise a lightweight IDS to avoid network downtime, protect users' data, and maintain network performance (Lawal et al., 2021).

DDoS attacks fall into three categories: Application layer attacks, Infrastructure layer attacks, and zero days DDoS attacks; Volum-based and protocol-based attacks are the most common threats in the infrastruc-

* Corresponding author.
E-mail addresses: saeed.javanmardi@unina.it (S. Javanmardi), meysam.ghahramani.cc@gmail.com (M. Ghahramani), m.shojafar@surrey.ac.uk (M. Shojafar), mamoun.alazab@cdu.edu.au (M. Alazab), antonio.caruso@unisalento.it (A.M. Caruso).

https://doi.org/10.1016/j.cose.2024.103778
Received 27 June 2023; Received in revised form 7 January 2024; Accepted 18 February 2024
Available online 22 February 2024

ture layer attacks. Among them, UDP flooding attacks are the common threat as volume-based attacks for the fog layer in IoT. Detecting UDP flooding attacks in IoT-fog networks is essential because they can cause significant disruption to the fog infrastructure and connected fog devices (Sharma et al., 2021). It aims to degrade the availability of edge resources by flooding the links and network nodes with forged requests from hostile IoT devices (Vishwakarma and Jain, 2020). Accordingly, in this paper, we focus on DDoS UDP flooding attacks.

In UDP flooding attacks, malicious IoT devices transmit a large volume of traffic to the fog devices, preventing them from inspecting and allowing approved network traffic. Although Rate Limiting can be used to limit the number of requests received by fog layer servers/brokers to prevent UDP flooding attacks, it lacks the means for verifying the requester. Accordingly, the network is prone to spoofing attacks. Because IP spoofing attacks are more common than MAC spoofing (Fichera et al., 2015; Conti et al., 2019), we only consider IP spoofing in this work. An IP spoofing attack occurs when an IoT device successfully impersonates another device by faking its IP address (Aldabbas and Amin, 2021). Received Signal Strength (RSS) can be utilized to overcome the limitation of Rate Limiting (RL), which determines the distance between the initiator node and the target node. RSS, however, fails when mobile IoT devices are in the network (Ghahramani et al., 2020b).

1.1. Motivation

In recent years, the origin of UDP flooding attacks has migrated to botnets composed of massive infected IoT devices. A large number and weak security protection capabilities characterize IoT devices. These features make IoT-Fog botnets highly flexible and cost-effective as the source of UDP flooding. As a result, UDP flooding is still a complex problem to solve as an ancient attack method (Vishwakarma and Jain, 2020; Kumari and Jain, 2023; Javanmardi et al., 2023a). Researchers mainly focus on two issues: 1) How to apply a programmable network to realize a comprehensive, flexible, and cost-effective defense system; 2) How to optimize the cost of the network-level security defense. Furthermore, most of the UDP flooding defense mechanisms in the literature for IoT-Fog networks are not impersonated and rely on other spoofing detection methods.

Because fog devices have limited processing capability, complicated security methods cannot be employed. As a result, a lightweight IDS is necessary to detect intrusions in the IoT-Fog network while minimizing fog resource usage. Light IDS can analyze network traffic, identify suspicious activities, and alert the resource management system, thereby enhancing the overall security of the IoT-Fog network. Because of the importance of IoT applications in daily life activities and the face of obstacles imposed by inherent IoT features (e.g., computational capacity limitation and price), developing lightweight IoT security approaches has received much attention (Khater et al., 2021). Following the above backdrop, the requirement for a light mobility-aware IDS that takes UDP flooding and spoofing attacks into account inspired us to present M-RL.

1.1.1. The angles of the motivations

The angles of the motivations of this research paper fall into two categories.

UDP flooding detection: Threats using UDP floods, commonly referred to as “bandwidth depletion attacks,” overwhelm the target system’s bandwidth by producing excessive traffic in bits per second. These are the easiest to utilize because they launch the attack using amplification and reflection tactics. According to literature, up to 65% of attacks involve UDP/TCP floods (Vishwakarma and Jain, 2020). This paper presents countermeasures for this threats because UDP flooding is a frequent and straightforward attack on IoT devices.

Rate limitation is an appropriate response to flooding attacks. The effectiveness of rate limitation against UDP flooding attacks is illustrated and explained as a prominent anomaly detection method in the literature (Mehdi et al., 2011; Javanmardi et al., 2021b, 2023b). It does, however, have two significant drawbacks. For starters, it is unable to detect anomalous behavior in the presence of spoofed IP addresses. The second is that it is typically employed in firewalls by setting a specified threshold. The issue is that despite careful engineering to define the threshold number, if the attacker gets access to the threshold and knows the traffic-rate threshold number, it sends slightly less network traffic to the fog layer nodes than the threshold, causing the network to go down.

Spoofing detection: There are several approaches to fending against a UDP flooding attack. Unfortunately, adversaries might conceal their identity and breach intrusion detection systems using malware or malicious software. On the other hand, putting precise plans into practice could be costly and incompatible with the IoT’s goals. As a result, the proposed solution must be accurate while meeting IoT requirements. By estimating the distance to the opponent, one of the lightweight solutions resistant to software forgeries is to use the received signal strength. This concept has two major flaws. To begin with, while this approach is robust to software forgery, it is not resistant to hardware fraud, and attackers who send packets with varied powers remain undetectable. Another downside of this technology is that it only supports static nodes, and packets received from moving nodes are treated as benign data by the RSS-based intrusion detection system (Ghahramani et al., 2020b). As a result, combining the benefits of earlier solutions is critical to creating a lightweight method for detecting UDP flooding attacks that are immune to software and hardware forgery.

1.1.2. The purpose of this research paper

We have discovered that M-RL can improve UDP flooding mechanisms that use spoofed identities. Hence, some questions arise that we aim to address in this study:

- Do methods with 100% accuracy work correctly in all situations, or are there certain situations that adversaries can use to bypass such methods?
- How can alternative techniques be suggested to improve the security of vulnerable methods?
- Is an alternative solution secure against adversaries?
- Can we overcome the limitations of RL and RSS?
- How can we design a mobility-aware attack defense mechanism?
- Can we introduce a robust defense solution tackling the attackers who perform UDP flooding with fake identities?

The rest of the paper delineates the response to these queries.

1.2. Contribution of the paper

M-RL is a lightweight mobility-aware IDS considering UDP flooding employing the *RL method* and spoofing threats using the *RSS method*. It automatically disables IoT devices that begin to participate in harmful activities to secure the IoT-Fog network. The attackers in this paper are assumed to be IoT devices capable of targeting the fog layer nodes. We evaluate and compare M-RL to two well-known anomaly detection algorithms, the RL and RSS algorithms, and a hybrid strategy named RL-RSS. We use RL to detect malicious behaviors based on high submission rates, RSS to detect the changes in IP addresses (spoofing attacks), and combine them with new equitation to detect mobility and signal strength changes to make M-RL able to overcome the limitations of RL and RSS approaches. In terms of accuracy, our proposal outperforms the RL, RSS, and RL-RSS methods, according to the findings. Our main contributions are as follows:

- We present M-RL, a new lightweight approach for detecting anomalies in IoT-Fog networks that considers IoT devices’ mobility.

- The proposed method employs both Rate and RSS simultaneously to detect malicious behavior. Rate is used to detect IP counterfeiting, and RSS calculates distance and supports mobility.
- We employ a lightweight hybrid technique to detect anomalous behaviors that integrate the output of the RL and RSS algorithms and the distance parameter, which solves the disadvantages of the RL and RSS methods.
- We perform experiments to illustrate the M-RL's security metrics in various conditions where the attackers spoof their identities and change their location.

The rest of the paper is structured as follows: Section 2 contains related literature on DDoS attacks on IoT networks. Section 3 provides an overview of the architecture in use and its key components. It also outlines the presented approach, which employs the RL and RSS, and how to overcome their flaws. Section 4 outlines how the performance of this work was evaluated using experimental results. Section 5 examines the issues pertinent to this work. Finally, Section 6 brings the paper to a close by describing some potential future paths.

2. Related works

In this section, we explain DDoS defense approaches in IoT networks. We divide it into subsections that reflect the critical angles of the related works. As the goal of this work is targeting DDoS flooding attacks, we focused on the approaches for flooding attacks. We divided the related work section into non-impersonation-aware and impersonation-aware methods. We explained that most approaches to detect DDoS flooding attacks rely on other approaches to become impersonation aware. Finally, we describe our proposal's critical features with the existing literature. It highlights how the proposed approach can cover some related issues compared to state-of-the-art methods.

2.1. Non-impersonation-aware approaches

Liu et al. (2020) investigated particular vulnerabilities in the NSL-KDD dataset that potentially affect sensor nodes in IoT networks. This work used bagging and boosting algorithms to identify malicious sensor nodes in the NSL-KDD datasets. Eleven machine learning methods were applied, and the performance of their anomaly behavior detection was compared. According to this work, the ensemble and tree-based techniques were the most accurate. The XGBoost algorithm comes first, outperforming the other supervised algorithms tested. While this effort improves the accuracy of the IoT network, it neglects to account for client mobility and spoofing.

Malik et al. (2017) presented a method to countermeasure UDP flooding attacks in the Contiki operating system. Their idea makes use of an intrusion protection algorithm that is installed on IoT devices. This method employs D2D communication tightly coupled to services, monitoring and intercepting requests to mitigate intrusions. In this paper, the authors implement an ICMP rate limitation method on IoT devices, effectively reducing bandwidth usage on IoT networks. This approach reduces the victim's total transmission power by 55%; however, it does not account for mobile IoT devices and relies on spoofing detection approaches.

Reddy et al. (2021) published an experimental investigation report for novel intrusion detection that used different machine learning methods for anomaly detection. Then, using XGBoost, they devised a method for implementing ensemble machine learning. Compared to machine learning techniques, the results demonstrated that XGBoost is a promising solution for intrusion detection in categorizing attacks. Their method is a greedy algorithm-based split finding strategy that employs several machine learning methodologies to detect various anomaly behaviors. Still, as there is no centralized controller, the network remains vulnerable to new emerging attacks. While this research covers a broad spectrum of threats, it ignores IoT devices' mobility and spoofing attacks.

Sharma and Gupta (2021) developed a framework for detecting and mitigating DDoS flooding threats on smart city IoT networks. By utilizing SDN for feature extraction and security management, the proposed IoT-Fog framework intends to lower the latency of attack detection. It enables scalability by utilizing SDN-based IoT-Fog infrastructure for attack mitigation. The authors used packet-level features that effectively distinguish between fog layer resources and attack data. Moreover, the authors trained and statistically compared five cutting-edge supervised machine learning models for attack detection, obtaining an accuracy of 99.9% in attack detection without considering mobile clients. Besides, it relies on spoofing detection strategies to detect attackers with forged identities.

Sharma et al. (2021) developed an intrusion detection architecture for the IoT paradigm with various security concerns to detect DDoS attacks, where fraud detection occurs at the fog layer. Their research employs a single-variable statistical method known as CRPS. Because the applications in the IoT-Fog networks comprise wireless communication and big data management (Santos et al., 2021; Junior and Kamienski, 2021), the author proposed fog network performance improvement in a data resilience system. This paper covers many threats without considering the mobility of IoT devices. Moreover, it does not detect the attackers with falsified identities.

Bovenzi et al. (2020) suggested a new IDS with a hybrid two-stage methodology. They used a multimodal Deep Auto Encoder for the first stage and a soft output classifier for the second stage. They assessed their technique by utilizing the Bot-IoT dataset to demonstrate how their approach is acceptable for IoT design. The authors used a binary classification followed by a multiclass classification in their investigation. The usage of the Deep Auto Encoder reduced dimensionality, resulting in a lightweight method for IoT networks. Without taking into consideration mobile IoT devices or attackers with forged identities, this article covers a broad spectrum of assaults.

Javanmardi et al. (2021b) presented FUPE, which uses multi-objective optimization to protect IoT-Fog scheduling services from DDoS flooding attacks. It is made up of an IDS and a scheduler. FUPE first detects and eliminates malicious IoT devices, then uses a MOPSO technique to integrate security and efficiency into the application scheduling step. FUPE employs a fuzzy function that uses TRW-CB and RL techniques to differentiate between benign and malicious nodes. It then computes a final solution for application scheduling using MOPSO. FUPE can integrate efficiency and security goals. The problem addressed in this paper is critical to IoT-Fog networks. FUPE is the first to attempt to include DDoS defense mechanisms into RMS. This research ignores mobility, and the attack detection method lacks spoofing methods.

Javanmardi et al. (2023b) proposed an approach named S-FoS, an SDN-based security-aware workflow scheduler for IoT-Fog networks. S-FoS could defend scheduling services against UDP flooding and port scanning threats. S-FoS uses fuzzy-based anomaly detection algorithms to identify the source of attacks and block malicious requestors. To strike a balance between the load and delay, it uses an NSGA-III multi-objective scheduler optimization method. In addition, the authors also evaluate S-FoS with cutting-edge methods in IoT-based scenarios through extensive simulations. The results show that by altering the attack rates, the number of IoT devices, and the number of fog devices, S-FoS can make better results than NSGA-II and MOPSO algorithms. This study disregards mobility, and the assault detection system lacks spoofing techniques.

2.2. Impersonation-aware approaches

Another method for detecting hostile conduct is to use authentication protocols (Ghahramani and Javidan, 2021). Cryptanalysis methods (Ghahramani et al., 2023) and (Ghahramani, 2023) can be used to detect the weaknesses of these protocols before they are put into practice on the global mobility networks (Ghahramani et al., 2020a). Many of these flaws are buried in such analyses, and attackers can penetrate the system using software techniques to change their behavior. Adversaries are not only able to penetrate the target system, but they can also obtain confidential information of other devices that have communicated with this system (Ghahramani and Javidan, 2022). To deal with such issues, new solutions have been developed. One of these techniques is to use the strength of the received signals (Ghahramani et al., 2020b). This approach can detect harmful activities even if there is no previous information about the packet and the content is randomly produced or fabricated. The distance of the sender node is estimated using the intensity of the received signal, regardless of the content of the packets, and poisoned data refers to packets delivered from the exact coordinates. Unfortunately, this strategy is ineffective against hardware fraud, significantly when the signal strength can be modified or when the nodes move. While this approach detects attackers with spoofed identities, it fails in the presence of malicious mobile nodes.

For DDoS attack detection and mitigation, Mao et al. (2018) used various packet header features and employed a joint-entropy technique. This work utilized information theory to improve scalability, detection accuracy, and simplicity. Furthermore, the combined entropy approach detects DDoS attacks by taking into account flow time, source IP address, packet length, and destination port. The authors conducted experiments using packet length and source IP to compare the combined entropy approach to a single entropy method. The combined entropy method outperforms the single entropy method in terms of detection accuracy and false-positive rate. The disadvantage of this technique is that it cannot identify an anomaly early because it takes extended to detect an attack. On the other hand, it mitigates DDoS abnormalities that use both spoofed and non-spoofed IP addresses. This Joint-Entropy-based technique for detecting DDoS attacks considers spoofing attacks while it does not consider mobile IoT devices.

2.3. Positioning of the proposed approach

M-RL is an IDS that protects Edge resources by constantly monitoring the IoT-Fog network for abnormal behavior and hazardous network traffic and implementing UDP flooding and spoofing attack countermeasures. Unlike the previous solutions in this category, M-RL detects and mitigates UDP flood attacks by considering both mobile IoT devices and IoT devices with falsified identities in this study. We employed Rate Limiting (Birkinshaw et al., 2019), a connection-based algorithm, and an RSS detection technique (Ghahramani et al., 2020b) to protect against UDP flooding attacks that leverage forged IP addresses. Our suggested IDS is a hybrid technique that leverages both Rate and RSS simultaneously to combat hostile mobile IoT devices that perform UDP flooding assaults using forged source IP addresses. RSS is used to determine distance and aid mobility, whereas Rate is used to detect IP forgery. M-RL uses RSS to provide a density parameter that, when multiplied by the Rate at which RSS forging and other vulnerabilities are identified, overcomes the limitations of the threshold technique. M-RL detects suspicious behavior and notifies the fog gateway's resource management system, removing the rogue IoT device from the network. In the next section, we describe how to use T_r and combine RL and RSS features for proposing a new equation (Equation (13)) to detect the attacker's mobility and malicious RSS modifications.

3. IDS approaches

In this Section we review the theoretical background and reference architecture to present M-RL, then we examine the problem statement, and discuss RSS, RL, and their disadvantages, finally, we present in detail M-RL, the proposed mobility-aware IDS.

3.1. Reference architecture

The reference architecture, which connects the IoT devices (user devices) to the IoT-Fog resources, is described in this section. We use an IoT-Fog architecture based on the most typical architecture with three layers, the Cloud layer, the Fog layer, and the IoT layer, as illustrated in Fig. 1 (Hu et al., 2017; Javanmardi et al., 2023a). The core networks deliver network services to users and are placed between the cloud and fog layers. The cloud data center (Shojafar et al., 2015) is located at the upper core level, far from the IoT devices. In IoT-Fog networks, the D2D (Bello and Zeadally, 2014), and broker approaches (Javanmardi et al., 2021a,b) are the two most frequent ways to implement three-layer architecture. In the first, IoT devices link directly to fog devices, whereas in the second, IoT devices connect to a node called a fog gateway, with the broker acting as an interface between them. A fog gateway is a type of fog server with advanced computing capabilities. In this research paper, we use the broker approach. The fog gateways act like brokers and collect the relevant data received by IoT devices (e.g., sensors).

3.2. Problem statement

Assume an IoT device requests a fog gateway. For real-world applications, their request may be Voice over IP (VoIP), online games, or media streaming. An attacker who wishes to flood the resources at the fog layer with excessive network traffic may send UDP packets with a faked IP source address. The goal of this research article is to develop an approach for preventing the transmission of bogus data to IoT-Fog resources. M-RL mitigates UDP flooding attacks by using both spoofed and non-spoofed IP addresses while considering the mobility of the IoT device.

3.3. Rate limiting (RL) method

RL approach assumes that an IoT device does not send a high number of UDP packets in a short period, whereas an attacker IoT device does. This technique identifies UDP flooding behavior in threshold-based approaches when the rate of UDP packets surpasses a predetermined threshold value.

Suppose the sending rate of the j-th attack and the i-th node are M_{r_j} and B_{r_i}, respectively. In this case, if M_{r_j} and B_{r_i} are isolated bounded, the threshold T_r can be adjusted so that the accuracy is 100%. This result can be mathematically represented as Equation (1).

$$\begin{aligned}
&\exists\, \alpha_1 < \alpha_2 < \alpha_3 < \alpha_4 \quad s.t.: \\
&\forall\, i : \alpha_1 \le B_{r_i} \le \alpha_2 \\
&\forall\, j : \alpha_3 \le M_{r_j} \le \alpha_4 \\
&\alpha_2 + 1 \le T_r \le \alpha_3 \Longrightarrow Accuracy = 100\%
\end{aligned} \tag{1}$$

Now the issue arises: *why do we need a new method when we already have one that is 100% accurate?* Unfortunately, the prior technique is vulnerable to malicious operations, and the accuracy of this method will suffer if an adversary fakes the source addresses.

3.4. Received signal strength (RSS) method

As previously stated, adversaries can diminish the accuracy of the preceding procedure by faking source addresses and terminating unidentified attacks. When received, packets in wireless media are sent by a wave that has a specific strength. The distance to the transmitter can be calculated using the received signal strength (RSS), and the distance can be used to detect and validate the source addresses. Similarly to the transmission rate, if we choose a given distance as the attack threshold, the adversary can travel a bit further away from it and launch its attack. A fuzzy method could be utilized to solve this problem. For example, the work (Janarthanan et al., 2020) detects assaults using fuzzy inputs, and after computing the RSS, fuzzy roles are

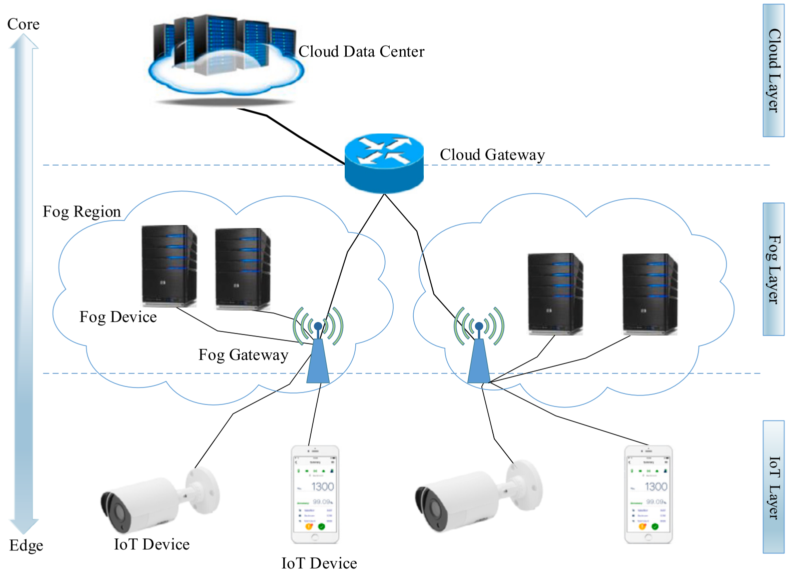

Fig. 1. M-RL architecture.

established based on the distance between the receiver and the sender. We shall cover two issues with RSS-based techniques further down.

3.5. *RSS in reality*

This section finds the location of the target node that sent a signal to the reference node at a distance of d_0. According to Jin et al. (2015), if there are n nodes in the network such that the distance between the k-th node and the target node is equal to d_k, then the power difference of the received and transmitted signal is as Equation (2).

$$P_0 - P_k = 10 \times \epsilon \times \log\left(\frac{d_k}{d_0}\right) + v_k \tag{2}$$

In addition to the distance, this equation also depends on two parameters, shadowing effect v_k and path loss exponent ϵ, which change for different propagation environments. Therefore, the distance to the target node satisfies Equation (3).

$$d_k = d_0 \times 10^{\left(\frac{P_0 - P_k - v_k}{10 \times \epsilon}\right)} \tag{3}$$

After calculating the distance from the target node, the location of the target node can be obtained using Equation (4).

$$\hat{X} = \begin{bmatrix} x \\ y \end{bmatrix} = \left(A^T A\right)^{-1} A^T B. \tag{4}$$

In the last equation, matrices A and B are defined as Equation (5), where k-th node is located at (x_k, y_k) and $0 \le k \le n-1$.

$$\begin{cases} A_{k,1} = -2 \times \left(x_n - x_k\right), A_{k,2} = -2 \times \left(y_n - y_k\right) \\ B_{k,1} = (x_k^2 + y_k^2 + d_n^2) - (x_n^2 + y_n^2 + d_k^2) \end{cases} \tag{5}$$

3.6. *Simulating RSS*

Equation (3) showed the relationship between distance and RSS in practice. Unfortunately, this relationship may not be established in all situations (Pagano et al., 2015). For example, the relationship in Tmote Sky nodes of the Cooja simulator is linear as shown in Equation (6), while Equation (3) shows a non-linear form (Tmote sky datasheet).

$$d_k \approx 1.177 - 0.588 \times (12 + RSS) \tag{6}$$

Additionally, $A^T A$ may not be invertible if the actual instruments cannot calculate the received signal strength with 100% accuracy. In such a case, calculating the precise location of the nodes is challenging, and Equation (4) has no solution. RSS is typically represented by a negative integer, which produces collisions at different targets, implying that the signal strength received from two transmitters in different locations may be the same. As a result, there is an *error range* in real implementations. When two benign nodes deliver packets inside an *error range*, they are misidentified as attackers. According to reference (Ghahramani et al., 2020b) the *error range* can be represented as a ring. The difference between this ring's external and internal radius depends on various factors, including weather and hardware. Still, in simulators such as Cooja, it is roughly 60 cm. For $n \ge 3$ receivers, the target location (x'_i, y'_i) maximizes Equation (7), where $[d^j_{min}, d^j_{max}]$ represent the error range of the j-th receiver (Ghahramani et al., 2020b). Equation (8) also defines the function H.

$$\sum_{j=1}^{n} H\left((x_j - x'_i)^2 + (y_j - y'_i)^2 - \left(d^j_{min}\right)^2\right) + \sum_{j=1}^{n} H\left(\left(d^j_{max}\right)^2 - (x_j - x'_i)^2 - (y_j - y'_i)^2\right) \tag{7}$$

$$H(\lambda) = \begin{cases} 1 \text{ if } \lambda \ge 0 \\ 0 \text{ if } \lambda < 0 \end{cases} \tag{8}$$

The scenario becomes more complicated when only one receiver is present, and utilizing RSS, the exact amount of movement cannot be computed, albeit a range can be supplied. Unfortunately, RSS is not immune to hostile activity. RSS-based results will be unreliable if the transmitter does not adhere to conventional protocols and broadcasts packets while moving or continually changing its strength. Fig. 2 depicts a summary of these issues. The recommended remedy will address the issues.

3.7. *Proposed M-RL approach*

The suggested method comprises three factors to identify adversarial behavior and solve past problems:

1. Rate limiting
2. Movement
3. Impersonation prediction

We use the first parameter to prevent malicious behaviors and specify a sending rate less than T_r. The second is used to cover the moving nodes. Assume a random node at position (x_i, y_i) with address β delivers a packet to the receiver, and the signal strength received from this

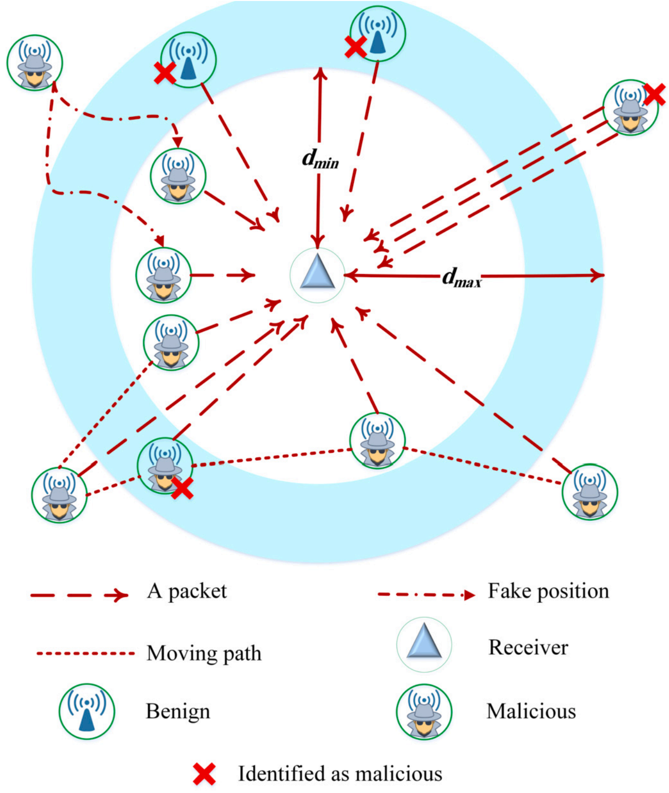

Fig. 2. Error range and disadvantages of RSS.

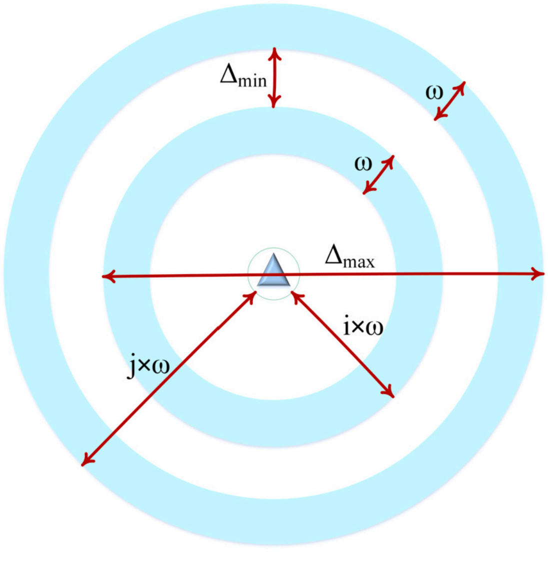

Fig. 3. Movement parameters from i-th to j-th error range.

point at time t_i is equal to RSS_{β,t_i}. Equation (9) can be used to calculate the movement if there is a function f such that $(x'_i, y'_i) = f(RSS_{\beta,t_i})$ estimates the location of the node. Equation (7) plays the role of f. Similarly, Equation (6) can be used if only one receiver is available.

$$\sqrt{\left(x'_{i+1} - x'_i\right)^2 + \left(y'_{i+1} - y'_i\right)^2} \tag{9}$$

Assume that the maximum allowable speed is v_{max}. However, Equation (10) shows the maximum permitted movement Δ for each node.

$$\Delta = \left(t_{i+1} - t_i\right) \times v_{max} \tag{10}$$

Assume the error range's width is ω, and the sender is in the ird error range at time t_i. When the transmitter is in the jth error range at time t_{i+1}, the lowest and maximum movement are as stated in Equation (11), with details in Fig. 3.

$$\Delta_{min} = (j-1-i) \times \omega, \Delta_{max} = (j+i) \times \omega \tag{11}$$

The final security parameter is essential to protect against RSS forgery. Assume an attacker disregards common IoT standards and sends packets of varying strengths. In this situation, the receiver can count the number of packets received from the i-th error range. Consider physical devices to be a circle with a radius of r. Given that the size of the i-th error range is as stated in Equation (12), only δ physical devices, as defined in Equation (13), can exist. The parameter δ can be used to detect RSS hardware forgery. This parameter does not allow the adversary to choose any desired power in the hardware change of the signal. For example, if we consider the range covered by wireless sensors as 120 meters, there are $\frac{120}{\omega} = \frac{120}{0.588} = 205$ error ranges in this area. Equation (13) shows that the capacity of the i-th error range is equal to δ. Therefore, using Equation (6), it can be concluded that the adversary has to send signals in which $\frac{120-1.177}{-0.588} - 12 \leq RSS \leq -11$. In other words, the calculated error range should be less than 205; Otherwise, the attack is detected. On the other hand, if more than 205 hardware falsifications occur, more than one signal is detected in at least one of the error ranges, according to the pigeonhole principle. The worst case happens when δ forgery occurs in every error range (the maximum capacity is used). Therefore, if $(\frac{120}{r})^2$ hardware forgeries occur, the attack will be detected with probability 100%. Although this probability depends on r, in networks such as smart transport systems where physical devices are cars with $r = 1$, an adversary cannot overwhelm the network because sending more than 120^2 adversarial packets will be detectable. Even if the devices are very small, for example, $r = 0.01$, the attack can be prevented by checking the continuous growth of the RSS distribution before the adversary uses 1200^2 spoofs.

$$\pi \times \left((i \times \omega)^2 - ((i-1) \times \omega)^2\right) = (2i-1) \times \pi \times \omega^2 \tag{12}$$

$$\delta = \frac{(2i-1) \times \pi \times \omega^2}{\pi \times r^2} = (2i-1) \times \left(\frac{\omega}{r}\right)^2 \tag{13}$$

The steps of the proposed approach, which employs these security factors, are described in Algorithm 1. It demonstrates how to identify hostile data using security parameters.

The threshold T_r, a width of the error range ω, the maximum speed allowed for moving nodes v_{max}, and the radius r of the IoT devices are all provided as default parameters in line 1. The frequency distribution of RSS in available packages is calculated in lines 2 to 5, and the details are kept in the RSSD matrix. Because RSS is negative integers less than -11, they must be added by 10 to be correctly mapped to RSSD matrix members. Following this, the security parameters mentioned in the previous part must be calculated, which is done in lines 6 to 21.

The sending rate of each node with address β is determined on line 9. The origin i and destination j of the migrating nodes are estimated on lines 11 and 12. The 15th line provides the maximum amount of movement through Δ_{max}. The RSS density of each packet is determined at line 16 using RSSD. Finally, security parameters Δ and δ are defined in line 17 to detect hostile packets.

3.8. Complexity

Calculating the complexity of the proposed algorithm is not a difficult task. This algorithm uses the RSSD matrix with sizes n-10. Suppose the number of IP addresses is equal to k. As a result, the space complexity is as Equation (14), where $m = \max\{k, n-10\}$.

$$O(m) \tag{14}$$

Similarly, the time complexity of this algorithm can be calculated. Except for lines 3, 6 and 10, the complexity of all expressions is in $O(1)$.

Algorithm 1 Adversarial packet detection.

```
1: Set: $T_r = 20000$, $\omega = 0.588m$, $v_{max} = 25m/s$, and $r = 0.05m$.
   Data set RSS density computation phase:
2: Create 1-by-$(n-10)$ zero matrix RSSD, where $n$ is the number of available RSS's.
3: for $x = 1$ to $n - 10$ do
4:     $RSSD[x] \longleftarrow$ The number of packets with RSS equal to $-(x+10)$.
5: end for
6: for each packet $p$ do
7:     $\beta \longleftarrow$ IP address of $p$.
8:     $RSS_{\beta,t_i} \longleftarrow$ Received signal strength from $\beta$ at time $t_i$.
   Rate limiting computation phase:
9:     $RL \longleftarrow$ The number of packets with address $\beta$.
   Distance computation phase:
10:    Find the next packet from $\beta$ at time $t_{i+1}$ with $RSS_{\beta,t_{i+1}}$.
11:    $i \longleftarrow \left\lceil \frac{1.177-\omega\times(12+RSS_{\beta,t_i})}{\omega} \right\rceil$
12:    $j \longleftarrow \left\lceil \frac{1.177-\omega\times(12+RSS_{\beta,t_{i+1}})}{\omega} \right\rceil$
13:    The node with address $\beta$ moved between $\Delta_{min}$ and $\Delta_{max}$, where:
14:    $\Delta_{min} = |j - i - 1| \times \omega, \Delta_{max} = (j + i) \times \omega$.
15:    Set $\Delta_{max}$ as a worst case for the movement of $\beta$.
   RSS spoofing prediction phase:
16:    Set RSS density of $p$ to $RSSD[-(RSS_{\beta,t_i} + 10)]$.
   Verification phase:
17:    Set $\Delta = (t_{i+1} - t_i) \times v_{max}$, and $\delta = (2i - 1) \times \left(\frac{\omega}{r}\right)^2$.
18:    if $RL > T_r$, $\Delta_{max} > \Delta$, or $RL \times (\text{RSS density}) > \delta$ then
19:        The packet is adversarial.
20:    end if
21: end for
```

The first and second **for** loops are repeated $n-10$ and k times, respectively. In the 10th line, to search for the next position of moving nodes in the worst case, k searches should be performed. As a result, the time complexity of this algorithm is equal to $O(n-10+k^2)$. This complexity can be summarized as Equation (15), where $m = \max\{k, n-10\}$.

$$O(m^2) \tag{15}$$

Note that this algorithm can be implemented to reduce its time complexity to $O(m)$. To this end, *hashing techniques* can be used. Suppose there is a hash function h such that it maps IP addresses to an integer smaller than k. The information for each package is kept in certain positions of the array in this case; thus, there is no need to search in the 10th line.

4. Performance evaluations

In this section, we give numerous scenarios for evaluating the performance of Rate Limiting, RSS, and the proposed approach M-RL.

4.1. Simulation setup

For evaluation, we use the DDoS UDP flood Dataset (CIC-DDoS2019). The client that initiates UDP floods in this dataset has attack rates of 24165 packets/second. We used this dataset and fed our detection algorithms the number of UDP packets sent by each client. To make this dataset suitable for evaluation, we employed SMOTE data augmentation to develop new data for malicious IoT devices because our goal needed to improve the number of malicious clients. We classified 30% of IoT devices as benign requests. Accordingly, we utilize 385 benign IoT devices and 165 IoT devices that initiate UDP flooding attacks. Because this dataset lacks RSS quantitative values, we analyzed our suggested technique by installing these 550 nodes in various locations and using the transmission rates as a new dataset.

Our study utilized real-world datasets within a custom Java simulation environment to evaluate the proposed M-RL method. It's essential to clarify that our focus was leveraging real-world data rather than simulating all IoT-Fog features. To this end, we incorporated values from real datasets into our simulation to ensure a representative evaluation. Moreover, the establishment of the topology and the duration for which packets were transmitted were inherently tied to the characteristics of the real dataset. Accordingly, our simulation environment inherits the network topology and packet transmission patterns captured in the original data.

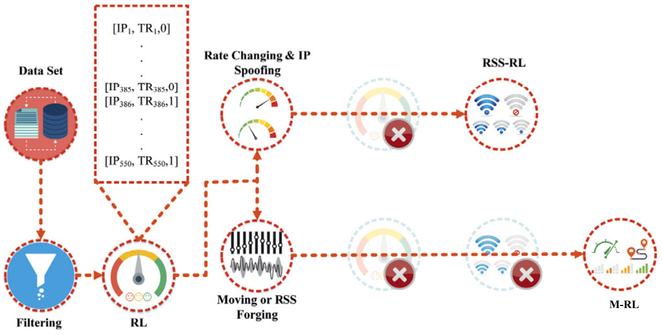
Data Set
[IP$_1$, TR$_1$,0]
[IP$_{385}$, TR$_{385}$,0]
[IP$_{386}$, TR$_{386}$,1]
[IP$_{550}$, TR$_{550}$,1]
Rate Changing & IP Spoofing
RSS-RL
Filtering
RL
Moving or RSS Forging
M-RL

Fig. 4. Simulation Process. (For interpretation of the colors in the figure(s), the reader is referred to the web version of this article.)

Equation (23) is used to calculate the RSS value of benign nodes, whereas random values are provided for attackers to assist RSS forging. Calculating the packet reception time and storing two rates and RSS parameters in the database is sufficient to implement Algorithm 1 and compare it to the other methods described in the following sections. In addition, we propose several scenarios to illustrate the weaknesses and strengths of common RSS and rate-based methods. The results show that our proposed method is able to identify scenarios that can bypass the previous methods. This process is summarized in Fig. 4. The picture starts from the red circle, indicating capturing data from the dataset. As there is no completely ready suitable dataset, the second circle (blue) indicates filtering the dataset to test different approaches. RSS-RL can detect rate changing and IP spoofing, while M-RL can detect them as well as moving or RSS forging.

4.2. Movement simulation

To simulate the movement, each node is initially placed at a random position (x_0, y_0) and sends a packet to the receiver. During movement, the position of the nodes changes, and another packet will be sent from the new position. Special patterns can be used to update the position of the nodes. For example, in vehicular networks that movement is on a straight horizontal road, Equation (16) can be used to update x_{i+1}. Similarly, on vertical movement y_{i+1} is updated, where $r_i \in [-1, 1]$ is a random number and Δ is maximum allowed movement.

$$\begin{cases} x_{i+1} = x_i + r_i \times \Delta, & y_{i+1} = y_i \\ x_{i+1} = x_i, & y_{i+1} = y_i + r_i \times \Delta \end{cases} \tag{16}$$

In random mode, the next position of the moving node should be in a circle with a radius of Δ. As a result, the random position of the moving node is updated as Equation (17). Fig. 5 depicts these strategies.

$$\begin{cases} x_{i+1} = x_i + r_i \times \Delta \\ y_{i+1} = y_i + r'_i \times \sqrt{\Delta^2 - \left(x_{i+1} - x_i\right)^2} \end{cases} \tag{17}$$

4.3. Simulation metrics

In this study report, we evaluate performance using the metrics listed below.

$$TPR = (TP/ActualPositive) = TP/(TP + FN) \tag{18}$$

$$FNR = (FN/ActualPositive) = FN/(TP + FN) \tag{19}$$

$$TNR = (TN/ActualNegative) = TN/(TN + FP) \tag{20}$$

$$FPR = (FP/ActualNegative) = FP/(TN + FP) \tag{21}$$

$$Accuracy = (TP + TN)/(TP + TN + FP + FN) \tag{22}$$

Table 1
RL accuracy evaluation.

Threshold	TN	FN	TP	FP	TNR	FNR	TPR	FPR	Accuracy
20000	385	0	165	0	1.0	0.0	1.0	0.0	1.0
21000	385	16	149	0	1.0	0.09	0.90	0.0	0.97
22000	385	82	83	0	1.0	0.49	0.50	0.0	0.85
23000	385	121	44	0	1.0	0.73	0.26	0.0	0.78
24000	385	150	15	0	1.0	0.90	0.090	0.0	0.72
25000	385	157	8	0	1.0	0.95	0.048	0.0	0.71
26000	385	165	0	0	1.0	1.0	0.0	0.0	0.70

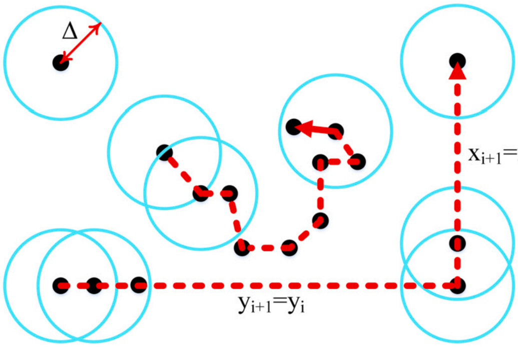

Fig. 5. Moving strategies.

Where TP stands for true positive and FN for false negative, while TN and FP stand for true negatives and false positives, respectively.

4.4. *Implementation scenarios and experimental results*

The following four scenarios are discussed in this section:

1. A scenario in which the attacker is stationary and delivers over 20,000 packets per second (PPS).
2. A scenario in which the attacker is stationary and forges the sender's IP address, sending fewer than 20,000 packets to each of the forged IP addresses but sending more than 20,000 PPS overall.
3. In A scenario in which the attacker is stationary, the enemy forges the sender's IP address and RSS and transmits fewer than 20,000 packets to each of the forged addresses but more than 20,000 PPS overall.
4. A scenario in which the attacker is on the move and forges the sender's address and RSS, sending less than 20,000 packets to each of the faked addresses but more than 20,000 PPS overall.

4.4.1. *First scenario*

To begin this part, we obtained the accuracy of the Rate Limiting algorithm that uses a threshold technique. We presume that the attackers do not use IP spoofing in this scenario. We want to indicate the drawback of utilizing a threshold-based Rate Limitation strategy in this experiment. Commercial firewalls nowadays have a default threshold for dealing with UDP flooding attacks. Even though the administrators can set a sensitivity level, the threshold is the cornerstone of the detection. For example, the default threshold in some firewalls is 500 PPS. As a result, a client sending 499 PPS is identified as a benign node, whereas a client sending 500 PPS is recognized as an attacker. In the first experiment, the attackers send packets between 20516 and 25882 per second. We want to demonstrate the accuracy of the various thresholds in the threshold-based RL strategy. Table 1 summarizes the accuracy evaluation for the threshold based RL approach.

According to Equation (1), in the analysed dataset, $\alpha_1 = 0.000892$, $\alpha_2 = 2.30775$, $\alpha_3 = 20516$, and $\alpha_4 = 25882$. As seen in Table 1, the accuracy for $T_r = 20000 < \alpha_3$ is 100%. The higher the T_r, the lesser the accuracy, until it reaches 70% at $T_r = 26000$.

Table 2
RSS accuracy evaluation: TN = 20,FN = 0 always.

Spoofed Ips	TP	FP	TNR	FNR	TPR	FPR	Accuracy
2	330	365	0.051	0.0	1.0	0.948	0.489
3	495	365	0.051	0.0	1.0	0.948	0.585
4	660	365	0.051	0.0	1.0	0.948	0.650
5	825	365	0.051	0.0	1.0	0.948	0.698
6	990	365	0.051	0.0	1.0	0.948	0.734
7	1155	365	0.051	0.0	1.0	0.948	0.762
8	1320	365	0.051	0.0	1.0	0.948	0.785
9	1485	365	0.051	0.0	1.0	0.948	0.804
10	1650	365	0.051	0.0	1.0	0.948	0.820

4.4.2. *Second scenario*

To get around the threshold-based detection mechanism, an attacker might spoof the sender's IP addresses and send malicious packets on their behalf without affecting the sender's sending rate. The threshold-based technique in this scenario classifies all incoming packets as innocuous. In this adversarial scenario, the accuracy of the prior method is $385/(385 + 165 \times n)$, where n is the number of faked IPs for each adversary. In this section, we'll put this scenario into action and discuss how to counter it The RSS accuracy is presented in the first section of this scenario. In this scenario, the nodes are in the space between *(-75, 75)*. Moreover, we calculate the RSS using Equation (23).

$$RSS_{\beta,t_i} = \frac{\sqrt{x^2_{\beta,t_i} + y^2_{\beta,t_i}} - 1.177}{-\omega} - 12 \tag{23}$$

Table 2 summarizes the accuracy evaluation for the RSS approach. The column *Spoofed IPs* in the table indicates the number of spoofed IPs used by malicious IoT devices. For example, *Spoofed IPs 10* means each of the attackers uses *ten* spoofed IP addresses.

Assume that the transmitting rate of the false addresses is $1/n$ that of the attacker in this situation. In our sample, there are 165 attacker nodes and 385 benign nodes. In this situation, the number of malicious packets is increased to $165 \times n$, but the number of safe packets remains unchanged. Only packages with distinct RSS are regarded benign in RSS technique (Ghahramani et al., 2020b), but installing nodes in random locations may result in the same RSS, and regular packets may be considered poisoned. Only 20 of our 385 benign nodes have distinct RSS, as seen in Table 1. As a result, $TN = 20$, $FP = 365$ and $TP = 165 \times n$ in this circumstance. As previously stated, the threshold method's minimal accuracy is $385/(385 + 165 \times n)$. In this situation, the number of falsified addresses must satisfy Equation (24) to enter the system.

$$\frac{\alpha_4}{n} < \alpha_2 \Longrightarrow n > \frac{\alpha_4}{\alpha_2} = \frac{25882}{2.30775} = 11215.25 \tag{24}$$

If $n = 11216$, the RSS method's accuracy will be as shown in Equation (25), which is perfect accuracy.

$$\frac{165 \times n + 20}{165 \times n + 385} = \frac{1850660}{1851025} = 99.98\% \tag{25}$$

This scenario implies that RSS vulnerability is caused by resistance to the threshold approach, and vice versa. The RSS approach can be improved by combining it with the threshold method. Instead of recognizing regular packages with unique RSS, packets with RSS distributions smaller than

Table 3
RSS-RL accuracy evaluation.

Spoofed Ips	TN	FN	TP	FP	TNR	FNR	TPR	FPR	Accuracy
2	130	0	330	255	0.337	0.0	1.0	0.662	0.643
3	130	0	495	255	0.337	0.0	1.0	0.662	0.710
4	130	0	660	255	0.337	0.0	1.0	0.662	0.755
5	130	0	825	255	0.337	0.0	1.0	0.662	0.789
6	130	0	990	255	0.337	0.0	1.0	0.662	0.814
7	130	0	1155	255	0.337	0.0	1.0	0.662	0.834
8	130	0	1320	255	0.337	0.0	1.0	0.662	0.850
9	130	0	1485	255	0.337	0.0	1.0	0.662	0.863
10	130	0	1650	255	0.337	0.0	1.0	0.662	0.874

Table 4
RSS-RL accuracy evaluation for RSS forgery scenario.

Spoofed Ips	TN	FN	TP	FP	TNR	FNR	TPR	FPR	Accuracy
2	383	165	165	2	0.99	0.5	0.5	0.01	0.77
3	384	221	274	1	1	0.45	0.55	0	0.75
4	385	261	399	0	1	0.4	0.6	0	0.75
5	384	301	532	1	1	0.36	0.64	0	0.75
6	385	396	609	0	1	0.39	0.61	0	0.72
7	384	444	740	1	1	0.38	0.63	0	0.72
8	384	432	939	1	1	0.32	0.68	0	0.75
9	385	585	968	0	1	0.38	0.62	0	0.70
10	384	576	1158	1	1	0.33	0.67	0	0.73

the threshold are considered innocuous. This method is known as RSS-RL.

4.4.3. *Third scenario*

In this scenario, we show a hybrid approach accuracy based on RL and RSS by setting the RL threshold to 20000. Table 3 summarizes the accuracy evaluation for the RSS-RL approach.

RSS and RSS-RL simulation results in adversarial circumstances are highly similar. Increasing n increases TP to $165 \times n$ in both approaches, while the remaining three parameters remain constant. The RSS-RL method raises the RSS method's TN value from 20 to 130 while lowering the FP number from 365 to 255. The RSS-RL accuracy for $n = 11216$ is shown in Equation (26), which is a great value.

$$\frac{165 \times n + 130}{165 \times n + 385} = \frac{1850770}{1851025} = 99.99\% \tag{26}$$

4.4.4. *Fourth scenario*

In the situation above, it was demonstrated that RSS-RL could accurately detect software forgery of IP addresses. We show that RSS-RL is not resistant to hardware forgery and that if adversaries send packets with forged addresses of varying powers, RSS-RL's accuracy will be considerably diminished, and the approach will lose its effectiveness.

Table 4 shows the findings of this experiment. With this behavior, the adversary can degrade the accuracy of the RSS-RL approach, as seen in the table. Although this behavior is a flaw in the approach, it benefits benign nodes because it raises TN. In the prior instance, FP increased; however, aggressive behavior increases FN in this one. As a result, IP forgery causes benign nodes' behavior to resemble that of attackers, whereas RSS forgery causes attacker nodes' behavior to resemble that of benign. The change of RSS for a fixed address is the cause of this drop in accuracy. The same behavior happens when the benign nodes move and send packets from different distances. As a result, in the final scenario, we apply IP spoofing, RSS forging, and mobile nodes to the processed dataset and evaluate the suggested method's correctness. To implement this scenario, the packet address β, its reception time t_i, and the strength of the received signal RSS_{β,t_i} at time t_i are used in Algorithm 1. In the processed dataset, $\alpha_1 = 0.000892$ means that for the results to be fair, we must allow the moving nodes to send packets within $1/\alpha_1 = 11212$ seconds, depending on their sending rate. Assume that the rate of the ist attacker node is $Tr^A_{\beta_i}$, and that the rate of the ird benign node is $Tr^B_{\beta_i}$. In this situation, Equation (27) shows the number of received packets in the processed dataset.

$$\frac{\sum_{i=1}^{165} Tr^A_{\beta_i} + \sum_{i=1}^{385} Tr^B_{\beta_i}}{\alpha_1} = \frac{3676626}{0.000892} = 4121778027 \tag{27}$$

Given the time commitment of analyzing such a large number of packages, the performance of the suggested solution against the adversarial behavior of the previous scenario is described in this part, and Table 5 indicates the accuracy of our proposed method for the RSS forging case.

Table 6 compares the analyzed methods. In this table, S_1 to S_4 represent scenarios 1 to 4, and "×" means that the analyzed method is vulnerable to the proposed scenario.

5. Discussion

5.1. *M-RL implementation feasibility considerations*

Different adversarial scenarios were simulated on many detection methods in the previous section, and the benefits and drawbacks of each were analyzed. We also demonstrated that our suggested solution inherits the benefits of earlier methods while eliminating their drawbacks by achieving greater than 99% accuracy. Table 7 summarizes the effectiveness of different strategies.

When using the RL approach, it was discovered that if the adversaries' transmission rate is high, increasing the threshold increases FN and decreases TP, as demonstrated by "↑" and "↓", respectively. Furthermore, at their best, FP and TN are nearly constant. FP is almost low in this strategy, indicating that benign nodes are never identified as attackers, while the greatest TN shows that all benign nodes are correctly identified. Unfortunately, by faking IP addresses, adversaries can lower the accuracy of this strategy. The more forgery, the larger FN and the lower TP, which is a dangerous weakness. This behavior can be detected using RSS-based approaches, and as the TP is increased, the accuracy against this adversarial behavior improves. These solutions solve the previous issue while taking TN and FP out of the ideal condition. Unfortunately, these systems are susceptible to RSS impersonation, which results in a rise in FN. Fortunately, our proposed solution overcomes all of these issues and is extremely near to being 100% accurate. Our technique identifies packages containing at least one of the following requirements as poisoned, proving this a straightforward effort.

Table 5
Proposed method evaluation for RSS forgery scenario.

Spoofed Ips	TN	FN	TP	FP	TNR	FNR	TPR	FPR	Accuracy
2	385	0	330	0	1	0	1	0	1
3	385	0	495	0	1	0	1	0	1
4	384	0	660	1	1	0	1	0	0.9990
5	385	2	831	0	1	0	1	0	0.9984
6	385	0	1005	0	1	0	1	0	1
7	385	5	1179	0	1	0	1	0	0.9968
8	385	4	1367	0	1	0	1	0	0.9977
9	385	5	1548	0	1	0	1	0	0.9974
10	385	0	1734	0	1	0	1	0	1

Table 6
Comparison of related works.

Method	S_1	S_2	S_3	S_4	TNR	FNR	TPR	FPR	Accuracy
RL	✓	×	×	×	1.0	0.0	1.0	0.0	1.0
RSS	✓	✓	×	×	0.05	0.0	1.0	0.95	0.82
RSS-RL	✓	✓	×	×	0.34	0.0	1.0	0.66	0.87
This paper	✓	✓	✓	✓	1.0	0.0	1.0	0.0	1.0

Table 7
Evaluation of different techniques.

Behavior	Detection method	TN	FN	TP	FP	Vulnerability
Constant rate	RL	*max*	↑	↓	*min*	IP spoofing
Impersonate IP	RSS/RSS-RL	·	*min*	↑	·	RSS forging
Fake RSS	RSS/RSS-RL	≈ *max*	↑	↑	≈ *min*	
Fake IP/RSS	Proposed Method	≈ *max*	≈ *min*	↑	≈ *min*	

- $RL > T_r$
- $\Delta_{max} > \Delta$
- $RL \times RSSD[-(RSS_{\beta,t_i} + 10)] > \delta$

The *two* last terms are used to advocate RSS forgery. The first condition is an RL approach for identifying adversaries who do not alter settings. The second condition is utilized when the RSS changes, such as when it is moving. It is a regular occurrence for legal migrating nodes that should not be mistaken forgeries. The likelihood of achieving this requirement improves if the opponents imitate the RSS. The last condition also resolves the problems that plagued the prior methods. Physically, at most δ, nodes can have the same RSS. To hide from our approach, adversarial behavior must meet none of these three characteristics, which is a challenging task. The first criterion is satisfied by the high transmission rate, and the second condition is met by random RSS generation to imitate permissible moving nodes. Even if the adversary avoids the second condition and generates the RSS in a way that is unrelated to the condition, the latter condition can still be used to identify it because IP forging and lowering the transmission rate for each of the forged addresses reduces RL while increasing the number of RSS's, which are discrete values. As a result, in the worst situation, if the opponent employs various forging techniques, the maximum number of sent packets required to identify the adversary is as Equation (28), where n denotes the number of available RSS's.

$$\left(\frac{\omega}{r}\right)^2 \times \sum_{i=1}^{n}(2i-1) = \left(\frac{\omega \times n}{r}\right)^2 \tag{28}$$

If we set $n = 75/\omega, r = 0.05, \omega = 0.588$, then any of 2250000 packets received on the network, regardless of whether they are adversarial or not, are considered attacks. In other words, the suggested system's maximum throughput is 2.25 million IoT devices. All of the theoretical analyses in this section are based on the Tables 1 to 7 results; however, different results may be achieved for various datasets or circumstances. In our dataset, there were 165 attackers, each with a maximum of 10 address RSS forgers. As a result, the suggested method's high accuracy is assured in a condition with a maximum of 1650 attacks, but ensuring accuracy in more complex situations necessitates more investigation. Our simulation reveals that if a maximum of 9,000 attacks are made according to the observed dataset's behaviors, the suggested method's accuracy will still be over 99 percent. However, any number greater than this will severely diminish the method's accuracy. However, this causes a significant drop in the accuracy of others. Statistical and mathematical methods can be used to overcome this problem, ensuring that the outcomes are independent of the dataset. For example, the similarity of parameters that are prone to fraud can be employed. This concept has recently been utilized to accurately identify Android malware (Taheri et al., 2020).

Combining our proposed solution with the studies of Zhang et al. (2017) and Zhou et al. (2017) has the potential to produce outstanding outcomes. Hardware fraud can be identified by examining the inaccuracy in the propagated signals, and packet receipt time analysis leads to the identification of software forgeries and support for node mobility. Another option is to employ secret sharing techniques, such as those described in Ayat and Ghahramani (2019). Fake parameters might be thought of as a secret that the opponent knows how to manufacture to match this strategy. These parameters are created by a random generator on the adversary side, whereas the parameters in secure packets are independent. We discovered malicious traffic outnumbered regular traffic when we examined the real-world UDP flooding statistics. For example, the UDP flood in the BOUN dataset (Erhan and Anarım, 2020) includes attack rates of 1000, 1500, 2000, and 2500 PPS. Furthermore, GitHub was the target of a DDoS attack in February 2018, during which the perpetrators sent 126.9 million PPS.

Rate limiting and RSS methods can be used separately to countermeasure UDP flooding and spoofing attacks. A popular strategy is to detect anomalies using a threshold based on the output of the detection algorithms. The primary disadvantage of threshold-based efforts is that they do not give the IDS sufficient sensitivity and specificity for accurate categorization. For instance, if the threshold number is 500, the IDS recognizes the node as a common node even though 499 is quite close to the threshold. In this situation, the attacker can initiate an attack if they know the threshold. Using a fuzzy function (Makkar et al., 2021) is an alternative solution to countermeasure the attacks simultaneously, overcoming the disadvantages of the threshold technique. Furthermore, fuzzy logic allows us to make the IDS mobility aware using the third parameter, distance.

5.2. RSS implementation feasibility considerations

Although RSS provides valuable information about the level of network activity and potential attacks, the problem with RSS is that it needs to interpret with the same accuracy across different types of Link layer technologies, e.g., 5G vs. 802.11. In other words, devices do not use/report the same granularity; generally, the number gets tweaked based on a formula. One way to overcome the accuracy problem with RSS is to use a standardized unit of measurement. For example, the IEEE 802.11 standard defines the unit of measure for RSS as the dBm (decibel-milliwatt). It allows for more precise and consistent measurement across different types of link layer technologies. Additionally, using multiple metrics to assess the quality of the link (e.g., signal-to-noise ratio, bit error rate, latency) can provide a complete picture of the link's performance and help compensate for inaccuracies in RSS measurements. Finally, calibration of the measurement equipment and consistent measurement techniques can also help improve RSS measurements' accuracy (Hoang et al., 2019).

The accuracy of Received Signal Strength (RSS) to determine where attackers are starting from is about 99%, which makes it hard for attackers to simply modulate the strength of the signal to bypass it. For instance, in our former work (Ghahramani et al., 2020b), we indicated that the placement of the receivers would significantly affect the results, and internal inaccuracy of the receivers is not the only issue affecting estimation accuracy. We demonstrated that the probability of a false alarm in the case study is less than 1% by providing an explicit calculation for it. Moreover, we illustrated localization in theory and practice. 99% accuracy is theoretically valid, but how do the receivers inside the fog gateways calculate the distance in practice? We explained thoroughly that it depends on the receiver type due to the different errors that affect the sender's location estimation. We refer the enthusiastic readers to the former work (Ghahramani et al., 2020b) in which we comprehensively analyzed RSS's theory and practice aspects for location detection accuracy.

In the real world, RSS is significantly impacted by noise or environmental phenomena, e.g., someone walking in front of the receiver. We can use several techniques to overcome the sensitivity of the RSS to environmental phenomena, such as someone walking in front of the receiver: *Antenna Diversity* (Boussad et al., 2021): One approach is to use multiple antennas in different locations so that the signal can be received from various paths, reducing the impact of obstructions. *Signal Processing* (Zhu et al., 2018): Another technique is to use signal processing algorithms such as equalization, channel estimation, and beamforming to improve the quality of the received signal and minimize the effects of obstructions. *Location Awareness* (Wu et al., 2019): In some cases, it may be possible to estimate the location of the obstructions and adjust the receiver accordingly to minimize the impact on the RSS. *Power Level Control* (Geok et al., 2022): Another technique is to adjust the power level of the transmitter so that it is not too high or too low. It can reduce interference from other sources and improve the reliability of the RSS. As a result, we should use a combination of these techniques to overcome the RSS's sensitivity to environmental phenomena and make RSS proper in real-world applications.

6. Conclusions and future work

DDoS UDP flooding attacks differ from other IoT-Fog network attacks in that they frequently do not display any first indicators of failure on the targeted edge resource. Instead, they gradually deplete all available resources and consume all network bandwidth, resulting in an edge resource shutdown. This research paper proposed M-RL, a combined hybrid IDS that combines the RL and RSS approaches while taking UDP flooding attacks into account in IoT-Fog networks. M-RL overcomes the disadvantages of the above-described techniques. The RL technique addresses the threshold problem, and the RSS approach solves the problem of mobile IoT devices. We investigate the adversarial behaviors that lead to anonymity when using RL and RSS-based approaches, combine their benefits, and address their flaws to propose an IDS that detects UDP flooding attacks. We detailed how to alter the RL method's threshold to obtain 100 percent accuracy, and we demonstrated that increasing the threshold results in a 30% loss in accuracy. Implementation of the RSS approach revealed that if the source addresses are forged, this method can enhance the accuracy of the prior method by 30 to 63 percent. Although the RSS-RL approach can boost the accuracy of the RSS-based method from 5.4 to 15.4 percent, the vulnerability of these methods to RSS forging makes it challenging to attain more than 77 percent accuracy in the event of this harmful behavior. The findings of this research show that the suggested method is immune to software forgery of source addresses, as well as impersonation and alteration of sent signals. It not only allows for node mobility but also provides over 99% accuracy. We compared the suggested method against RL, RSS, and RL-RSS and found that M-RL delivers more than 99% accuracy, while the other approaches' most incredible potential accuracy was 77%.

We will employ different anomaly detection techniques for the feature work and apply fuzzy logic to create a balance between their output to countermeasure attacks in IoT-Fog architecture because the given approach is versatile and lightweight. Another interesting area of research is to properly protect fog nodes powered by energy harvesting devices (Kuzman et al., 2019; Caruso et al., 2019), when too many requests are received and the energy of the system is limited.

CRediT authorship contribution statement

Saeed Javanmardi: Conceptualization, Formal analysis, Methodology, Writing – original draft. **Meysam Ghahramani:** Conceptualization, Writing – original draft, Writing – review & editing. **Mohammad Shojafar:** Writing – original draft, Writing – review & editing. **Mamoun Alazab:** Writing – original draft, Writing – review & editing. **Antonio M. Caruso:** Conceptualization, Funding acquisition, Writing – original draft, Writing – review & editing.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

No data was used for the research described in the article.

Acknowledgements

This work is partially funded by the Puglia Region in Italy, with the grant RIPARTI n. 11070ad0. It finances research grants in collaboration with PMI, for researchers and their inclusion in the regional production system.

References

Aldabbas, H., Amin, R., 2021. A novel mechanism to handle address spoofing attacks in sdn based iot. Clust. Comput. 24 (4), 3011–3026.

Ayat, S.M., Ghahramani, M., 2019. A recursive algorithm for solving "a secret sharing" problem. Cryptologia 43 (6), 497–503.

Bello, O., Zeadally, S., 2014. Intelligent device-to-device communication in the Internet of things. IEEE Syst. J. 10 (3), 1172–1182.

Birkinshaw, C., Rouka, E., Vassilakis, V.G., 2019. Implementing an intrusion detection and prevention system using software-defined networking: defending against port-scanning and denial-of-service attacks. J. Netw. Comput. Appl. 136, 71–85.

Boussad, Y., Mahfoudi, M.N., Legout, A., Lizzi, L., Ferrero, F., Dabbous, W., 2021. Evaluating smartphone accuracy for rssi measurements. IEEE Trans. Instrum. Meas. 70, 1–12.

Bovenzi, G., Aceto, G., Ciuonzo, D., Persico, V., Pescapé, A., 2020. A hierarchical hybrid intrusion detection approach in iot scenarios. In: GLOBECOM 2020-2020 IEEE Global Communications Conference. IEEE, pp. 1–7.

Conti, M., Lal, C., Mohammadi, R., Rawat, U., 2019. Lightweight solutions to counter ddos attacks in software defined networking. Wirel. Netw. 25 (5), 2751–2768.

Erhan, D., Anarım, E., 2020. Boğaziçi university distributed denial of service dataset. Data Brief 32, 106187.

Fichera, S., Galluccio, L., Grancagnolo, S.C., Morabito, G., Palazzo, S., 2015. Operetta: an openflow-based remedy to mitigate tcp synflood attacks against web servers. Comput. Netw. 92, 89–100.

Geok, T.K., Hossain, F., Rahim, S.K.A., Elijah, O., Eteng, A.A., Loh, C.T., Li, L.L., Tso, C.P., Abd Rahman, T., Hindia, M.N., 2022. 3d rt adaptive path sensing method: Rssi modelling validation at 4.5 ghz, 28 ghz, and 38 ghz. Alex. Eng. J. 61 (12), 11041–11061.

Ghahramani, M., 2023. Find it with a pencil: an efficient approach for vulnerability detection in authentication protocols. IEEE Trans. Inf. Forensics Secur. 18, 2005–2014.

Ghahramani, M., Javidan, R., 2021. A robust anonymous remote user authentication protocol for iot services. Wirel. Pers. Commun. 121 (3), 2347–2369.

Ghahramani, M., Javidan, R., 2022. Time dependency: an efficient biometric-based authentication for secure communication in wireless healthcare sensor networks. J. Comput. Virol. Hacking Tech. https://doi.org/10.1007/s11416-022-00448-9.

Ghahramani, M., Javidan, R., Shojafar, M., 2020a. A secure biometric-based authentication protocol for global mobility networks in smart cities. J. Supercomput. 76 (11), 8729–8755.

Ghahramani, M., Javidan, R., Shojafar, M., Taheri, R., Alazab, M., Tafazolli, R., 2020b. Rss: an energy-efficient approach for securing iot service protocols against the dos attack. IEEE Int. Things J. 8 (5), 3619–3635.

Ghahramani, M., HaddadPajouh, H., Javidan, R., Kumari, S., 2023. Vqr: vulnerability analysis in quadratic residues-based authentication protocols. J. Ambient Intell. Humaniz. Comput., 1–16.

Hoang, M.T., Yuen, B., Dong, X., Lu, T., Westendorp, R., Reddy, K., 2019. Recurrent neural networks for accurate rssi indoor localization. IEEE Int. Things J. 6 (6), 10639–10651.

Hu, P., Dhelim, S., Ning, H., Qiu, T., 2017. Survey on fog computing: architecture, key technologies, applications and open issues. J. Netw. Comput. Appl. 98, 27–42.

Janarthanan, A., Kumar, D., Antony, R.R., Parvathe, C., 2020. Iadf security: insider attack detection using fuzzy logic in wireless multimedia sensor networks. Soft Comput. 24 (18), 13893–13902.

Javanmardi, S., Shojafar, M., Persico, V., Pescapè, A., 2021a. Fpfts: a joint fuzzy particle swarm optimization mobility-aware approach to fog task scheduling algorithm for Internet of things devices. Softw. Pract. Exp. 51 (12), 2519–2539.

Javanmardi, S., Shojafar, M., Mohammadi, R., Nazari, A., Persico, V., Pescapè, A., 2021b. Fupe: a security driven task scheduling approach for sdn-based iot–fog networks. J. Inf. Secur. Appl. 60, 102853.

Javanmardi, S., Shojafar, M., Mohammadi, R., Alazab, M., Caruso, A.M., 2023a. An sdn perspective iot-fog security: a survey. Comput. Netw. 229, 109732.

Javanmardi, S., Shojafar, M., Mohammadi, R., Persico, V., Pescapè, A., 2023b. S-fos: a secure workflow scheduling approach for performance optimization in sdn-based iot-fog networks. J. Inf. Secur. Appl. 72, 103404.

Jin, R., Xu, H., Che, Z., He, Q., Wang, L., 2015. Experimental evaluation of reducing ranging-error based on receive signal strength indication in wireless sensor networks. IET Wirel. Sensor Syst. 5 (5), 228–234.

Junior, F.M.R., Kamienski, C.A., 2021. Data resilience system for fog computing. Comput. Netw. 195, 108218.

Khater, B.S., Abdul Wahab, A.W., Idris, M.Y.I., Hussain, M.A., Ibrahim, A.A., Amin, M.A., Shehadeh, H.A., 2021. Classifier performance evaluation for lightweight ids using fog computing in iot security. Electronics 10 (14), 1633.

Kumari, P., Jain, A.K., 2023. A comprehensive study of ddos attacks over iot network and their countermeasures. Comput. Secur., 103096.

Laroui, M., Nour, B., Moungla, H., Cherif, M.A., Afifi, H., Guizani, M., 2021. Edge and fog computing for iot: a survey on current research activities & future directions. Comput. Commun. 180, 210–231.

Lawal, M.A., Shaikh, R.A., Hassan, S.R., 2021. A ddos attack mitigation framework for iot networks using fog computing. Proc. Comput. Sci. 182, 13–20.

Liu, J., Kantarci, B., Adams, C., 2020. Machine learning-driven intrusion detection for contiki-ng-based iot networks exposed to nsl-kdd dataset. In: Proceedings of the 2nd ACM Workshop on Wireless Security and Machine Learning, pp. 25–30.

Makkar, A., Ghosh, U., Sharma, P.K., Javed, A., 2021. A fuzzy-based approach to enhance cyber defence security for next-generation iot. IEEE Int. Things J.

Malik, M., Dutta, M., et al., 2017. Contiki-based mitigation of udp flooding attacks in the Internet of things. In: 2017 International Conference on Computing, Communication and Automation (ICCCA). IEEE, pp. 1296–1300.

Mao, J., Deng, W., Shen, F., 2018. Ddos flooding attack detection based on joint-entropy with multiple traffic features. In: 2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE). IEEE, pp. 237–243.

Mehdi, S.A., Khalid, J., Khayam, S.A., 2011. Revisiting traffic anomaly detection using software defined networking. In: International Workshop on Recent Advances in Intrusion Detection. Springer, pp. 161–180.

Pagano, S., Peirani, S., Valle, M., 2015. Indoor ranging and localisation algorithm based on received signal strength indicator using statistic parameters for wireless sensor networks. IET Wirel. Sensor Syst. 5 (5), 243–249.

Reddy, D.K.K., Behera, H., Nayak, J., Naik, B., Ghosh, U., Sharma, P.K., 2021. Exact greedy algorithm based split finding approach for intrusion detection in fog-enabled iot environment. J. Inf. Secur. Appl. 60, 102866.

Santos, J., Wauters, T., Volckaert, B., De Turck, F., 2021. Towards end-to-end resource provisioning in fog computing over low power wide area networks. J. Netw. Comput. Appl. 175, 102915.

Sharma, H., Gupta, S., 2021. Leveraging machine learning and sdn-fog infrastructure to mitigate flood attacks. In: 2021 IEEE Globecom Workshops (GC Wkshps). IEEE, pp. 1–6.

Sharma, D.K., Dhankhar, T., Agrawal, G., Singh, S.K., Gupta, D., Nebhen, J., Razzak, I., 2021. Anomaly detection framework to prevent ddos attack in fog empowered iot networks. Ad Hoc Netw. 121, 102603.

Shojafar, M., Javanmardi, S., Abolfazli, S., Cordeschi, N., 2015. Fuge: a joint metaheuristic approach to cloud job scheduling algorithm using fuzzy theory and a genetic method. Clust. Comput. 18, 829–844.

Taheri, R., Ghahramani, M., Javidan, R., Shojafar, M., Pooranian, Z., Conti, M., 2020. Similarity-based android malware detection using hamming distance of static binary features. Future Gener. Comput. Syst. 105, 230–247.

Tmote sky datasheet. https://fccid.io/TOQTMOTESKY/User-Manual/Users-Manual-Revised-613136. (Accessed 5 September 2022).

Vishwakarma, R., Jain, A.K., 2020. A survey of ddos attacking techniques and defence mechanisms in the iot network. Telecommun. Syst. 73 (1), 3–25.

Wu, C., Wang, X., Chen, M., Kim, M.J., 2019. Differential received signal strength based rfid positioning for construction equipment tracking. Adv. Eng. Inform. 42, 100960.

Zhang, P., Nagarajan, S.G., Nevat, I., 2017. Secure location of things (slot): mitigating localization spoofing attacks in the Internet of things. IEEE Int. Things J. 4 (6), 2199–2206.

Zhou, B., Chen, Q., Xiao, P., 2017. The error propagation analysis of the received signal strength-based simultaneous localization and tracking in wireless sensor networks. IEEE Trans. Inf. Theory 63 (6), 3983–4007.

Zhu, H., Zhuo, Y., Liu, Q., Chang, S., 2018. π-splicer: perceiving accurate csi phases with commodity wifi devices. IEEE Trans. Mob. Comput. 17 (9), 2155–2165.

Kuzman, M., Toro Garcia, X., Escolar, S., Caruso, A., Chessa, S., Lopez, J., 2019. A testbed and an experimental public dataset for energy-harvested IoT solutions 2019-July, 869–876.

Caruso, A., Chessa, S., Escolar, S., Del Toro, X., Kuzman, M., Lopez, J., 2019. Experimenting Forecasting Models for Solar Energy Harvesting Devices for Large Smart Cities Deployments. In: IEEE Symposium on Computers and Communications (ISCC). Barcelona, Spain, pp. 1177–1182.

Saeed Javanmardi concluded his Postdoc program at Salento University in Lecce, Italy, under the supervision of Professor Antonio Caruso in January 2024. He also got his PhD from the Department of Electrical Engineering and Information Technologies (DIETI), the University of Napoli (Federico II), Napoli, Campania, Italy, in May 2022 under the supervision of full professor Antonio Pescape. He is a security-aware IoT-Fog application scheduling scientist and has contributed to IoD research projects for RIPARTI corporation. His current research interests include the following: Fuzzy theory, Multi-objective optimization, Security-aware application scheduling, Privacy, efficiency, and SDN-based IoT-fog networks. Moreover, he published several journal papers on his interests and is a reviewer of IEEE Transactions on Intelligent Transportation Systems Journal, IEEE Transactions on Dependable and Secure Computing journal, IEEE Systems Journal, IEEE Transactions on Network and Service Management journal, IEEE Consumer Electronics Magazine, IEEE Transactions on Circuits and Systems for Video Technology, MDPI Applied Science, MDPI Future Internet, MDPI Drones, MDPI Micromachines, MDPI Symmetry, Taylor & Francis Cybernetics and Systems Journal, and Springer Journal of Grid Computing.

Meysam Ghahramani received the B.Sc. degree (Hons.) in mathematics and its applications from Zabol University, Zabol, Iran, in 2014, and the Ph.D. degree in computer engineering from the Shiraz University of Technology, in 2021. His research interests include post-quantum cryptography, cryptographic protocol analysis, applied mathematics, and information security. He won the first rank at the ACM programming competitions of the university, in 2013. He was admitted to the postgraduate in the field of cryptography, graduated with the first rank, and received the Award of a Distinguished University Student from Malek Ashtar University of Technology, Iran, in 2016.

Mohammad Shojafar (M'17-SM'19) is a Senior Lecturer (Associate Professor) in Network Security, an Intel Innovator, a Senior IEEE member, an ACM distinguished speaker, and a Fellow of the Higher Education Academy, working in the 5G & 6G Innovation Centre (5GIC & 6GIC) at the University of Surrey, UK. Before joining 5GIC & 6GIC, he was a Senior Researcher and a Marie Curie Fellow in the SPRITZ Security and Privacy Research group at the University of Padua, Italy. He was a Senior Researcher working on a network security project (~11 months) jointly with Ryerson University and Telus Communications Inc

(TELUS) in Toronto, Canada, in 2019. Also, he was a CNIT Senior Researcher at the University of Rome Tor Vergata and contributed to the 3GPPP European H2020 "SUPERFLUIDITY" project.

Dr Mohammad secured around £1.2M as PI in various EU/UK projects, including 5G Mode (funded by DSIT/UK;2023), TRACE-V2X (funded by EU/MSCA-SE;2023), AUTOTRUST (funded by ESA/EU;2021), PRISENODE (funded by EU/MSCA-IF:2019), and SDN-Sec (funded by Italian Government:2018). He was also COI of various UK/EU projects like HiPER-RAN (funded by DSIT/UK;2023), APTd5G (funded by EPSRC/UKI-FNI:2022), ESKMARALD (funded by UK/NCSC;2022), GAUChO, S2C and SAMMClouds (funded by Italian Government;2016-2018). He received a Ph.D. from the Sapienza University of Rome, Rome, Italy, in 2016 with an "Excellent" degree. He received the honored BSc in CS at Iran University of Science and Technology, Tehran, Iran, in 2006. He was a programmer/software analyzer at the National Iranian Oil Company (NIOC) and Tidewater ltd in Iran from 2008 to 2013. He published over 200 refereed top-tier articles in prestigious venues such as IEEE TII, IEEE TCC, IEEE TNSM, IEEE T-ITS, IEEE Network, Computer Networks, and FGCS. He is an Associate Editor in IEEE Transactions on Network and Service Management, IEEE Transactions on Intelligent Transportation Systems, IEEE Consumer Electronics Magazine, and Computer Networks Journals. He published three books on Cybersecurity Applications and Network Security, which appeared in Springer recently.

Mamoun Alazab is a full Professor at the Faculty of Science and Technology and the Inaugural Director of the NT Academic Centre for Cyber Security and Innovation (ACCI) at Charles Darwin University, Australia. He is a cyber security researcher and practitioner with industry and academic experience. His research is multidisciplinary and focuses on cyber security, data analytics, and digital forensics, focusing on cybercrime detection and prevention. He looks into the intersection use of AI as an essential tool for security and privacy, for example, authorship attribution, access control systems, detecting attacks, crime investigation, analyzing malicious code, or uncovering vulnerabilities in software.

Antonio Caruso received the M.S. degree (cum laude) and Ph.D. degree from the University of Pisa, Pisa, Italy, both in computer science. In 2005, he joined the Mathematical and Physics Department, University of Salento, Lecce, Italy, as an Assistant Professor. Prof. Caruso was a recipient of the Innovation Award from Italian–Canada in 2017. He has been a member of several Program Committees of conferences and workshops and his research has been published in international journals and conference proceedings mainly in the area of mobile distributed systems, Security, Internet of Things, Smart Environment, Wireless Sensor Networks. He is currently the site leader for the University of Lecce of the TEBAKA project (PON-MISE) an AgriTech project that use AI/ML and remote sensing (UAV and Satellite Images) for improving quality and productivity of crops.