

Resilient Secure Military IoT Mesh with Rogue Node and Jamming Awareness

Joga Jeevitha¹, Dr. S.Jhansi Rani²

¹ Computer Science and System Engineering, Andhra University, Vishakhapatnam, Andhra Pradesh, India

Abstract - In this study, a secure communication approach is developed for Military Internet of Things (IoT) networks to address challenges such as unauthorized node access and jamming attacks. To achieve this, an Elliptic Curve Cryptography (ECC)-based authentication mechanism is used to verify nodes and ensure that only legitimate devices participate in the network. When jamming occurs, a dynamic channel switching mechanism is applied to handle transmission disruptions under varying conditions. The proposed method is implemented using the ns-3 simulator and evaluated under different network scenarios. Performance is measured using metrics such as Packet Delivery Ratio (PDR), throughput, packet loss, and delay. The results show that the proposed approach maintains a Packet Delivery Ratio of approximately 93-98% and improves overall network performance during attack conditions. These findings indicate that the method can support reliable and secure communication in Military IoT environments.

Keywords: Military IoT, Secure Mesh Networks, Rogue Nodes, Jamming Awareness, Network Resilience.

1.INTRODUCTION

In recent years, the Internet of Things (IoT) has grown rapidly and is now being used in important areas such as military communication systems. Military IoT networks are made up of interconnected devices such as sensors and communication units, which continuously share information for tasks like surveillance, monitoring, and coordination. Since these networks are distributed and wireless in nature, they are highly vulnerable to security threats and operational disruptions. Among the various challenges, rogue node intrusion and jamming attacks are two major concerns. Rogue nodes are unauthorized devices that try to access the network and disrupt communication by injecting false data or interfering with legitimate transmissions. On the other hand, jamming attacks introduce interference into the communication channel, which leads to packet loss, increased delay, and degradation of overall network performance. In severe situations, such attacks can completely disrupt communication within the network.

To address these challenges, a secure and adaptive communication framework is needed. The proposed approach uses an authentication mechanism based on Elliptic Curve

Cryptography (ECC) to ensure that only legitimate nodes can participate in the network. This helps prevent unauthorized access and improves overall network security. In addition, a jamming mitigation strategy based on dynamic channel switching is used to maintain stable communication. The results show that, through this mechanism, the network adapts to interference by shifting communication to a less affected channel. The framework is implemented using the ns-3 network simulator along with the AODV routing protocol. Network performance is evaluated using key metrics such as Packet Delivery Ratio (PDR), throughput, packet loss, and end-to-end delay. Furthermore, Net Anim visualization is also used to analyse network behaviour under normal conditions, attack scenarios, and recovery phases. The simulation results demonstrate that the system maintains a high Packet Delivery Ratio of approximately 93–98%, along with improved throughput and reduced packet loss under adverse conditions.

Along with improving security and performance, the framework also focuses on adaptability in dynamic and hostile environments. Military IoT networks often operate under rapidly changing conditions, where factors like network topology, interference levels, and threat intensity can vary. By combining authentication with adaptive channel switching, the system is able to respond effectively to these changes, which helps reduce the chances of communication failure. This combined approach improves the overall reliability, stability, and efficiency of the network, making it suitable for real-time and mission-critical military applications.

2.RELATED WORK

The Internet of Things (IoT) has significantly transformed military communication systems, leading to the emergence of the Internet of Battlefield Things (IoBT). Ensuring secure and reliable communication in such environments has become a major focus of recent research, particularly in areas such as authentication, secure transmission, and attack detection.

end-to-end encrypted communication system for military IoT applications by integrating technologies such as ESP-NOW and LoRa to support both low-latency and long-range communication [1]. The system uses AES encryption and HMAC-based authentication to ensure data confidentiality and integrity. Although the approach improves communication reliability, it lacks mechanisms for intelligent threat detection. A digital signature-based authentication model was introduced by [2], to ensure data authenticity, integrity, and non-repudiation. While suitable for dynamic battlefield environments, the use of asymmetric cryptography

introduces computational overhead, making it less suitable for resource-constrained IoT devices. Kufakunesu et al. presented a comprehensive survey of IoBT systems, highlighting challenges such as interoperability, energy efficiency, network resilience, and security. However, the study identifies research gaps without proposing specific implementation strategies.

a machine learning-based authentication method that combines physical layer security with wireless fingerprinting for continuous node verification. This reduces dependence on computationally intensive cryptographic techniques, though performance may vary with environmental and channel conditions [3]. Similarly, explored a trust-based model using K-means clustering to detect malicious nodes such as black hole attackers, but it requires careful parameter tuning for optimal results [4].

A proposed framework integrating IoT devices, unmanned aerial vehicles (UAVs), and Mobile Edge Computing (MEC) to enhance communication efficiency [5]. The approach uses particle swarm optimization for cluster head selection, improving energy efficiency, reducing delay, and increasing packet delivery ratio, though it introduces additional system complexity. For jamming detection, Ashraf and Sagheer [6] proposed a cooperative method in which nodes monitor parameters such as packet forwarding ratio and received signal strength. This reduces detection delay and energy consumption but relies on effective node cooperation.

Paramesh and Zeng provided [7] a comprehensive survey of jamming attacks and countermeasures, including techniques such as frequency hopping and power control. While offering strong theoretical insights, it does not present practical solutions tailored to IoT constraints. Namvar [8,] proposed a game-theoretic approach for interference mitigation, where power allocation is dynamically adjusted across subcarriers; however, its centralized nature limits scalability in distributed networks.

In addition, various clustering and routing optimization techniques have been explored to improve network performance by enhancing throughput and ensuring reliable connectivity. However, many of these methods do not adequately address real-time security threats such as jamming and adversarial node behaviour. These limitations highlight the need for integrated solutions that combine authentication and adaptive mitigation mechanisms in Military IoT environments.

3.SYSTEM ARCHITECTURE

The system architecture is designed to provide secure and reliable communication in Military Internet of Things (IoT) networks. It includes multiple components that work together to handle data transmission, authentication, attack detection, and mitigation.

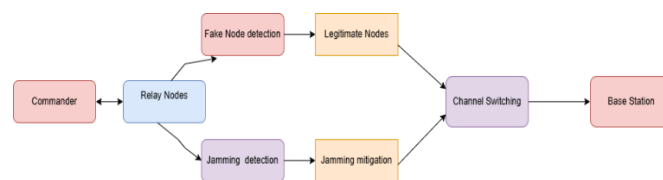


Fig 1: System Architecture

As shown in Figure 1, the communication process starts with a source node, which acts as a command or control unit responsible for initiating data transmission. The data is then forwarded through intermediate relay nodes that form an ad hoc network. These nodes use routing protocols to maintain connectivity and support efficient data delivery to the destination node.

To improve network security, a fake node detection mechanism based on Elliptic Curve Cryptography (ECC) authentication is incorporated. Each node is assigned a unique cryptographic identity, which is verified before it is allowed to participate in the network. Nodes that fail authentication are treated as malicious and are restricted from accessing the network, thereby improving overall trust and security.

In addition, a jamming detection module continuously monitors key performance parameters such as packet delivery and transmission success rate. A noticeable degradation in these metrics is considered an indication of possible interference or jamming activity. Once such interference is detected, a mitigation mechanism based on dynamic channel switching is activated. This allows the system to shift communication to a less congested channel, reducing the impact of interference and restoring normal data transmission.

Finally, the data reaches the destination node, which represents the receiving unit or base station. Successful delivery indicates that the system is able to handle both security threats and communication disruptions effectively.

4.METHODOLOGY

The methodology consists of several stages designed to provide secure and reliable communication in Military IoT networks. In the beginning, the network is created by configuring a set of nodes within the ns-3 simulation environment. Communication between nodes is enabled wirelessly, and the AODV routing protocol is used to manage dynamic routing. A mobility model is applied to define node positions, followed by the initiation of data transmission. To maintain security, an authentication mechanism based on Elliptic Curve Cryptography (ECC) is used. Each node is given a unique cryptographic identity, allowing only verified nodes to access the network. Any node that does not pass authentication is considered malicious and is removed from communication, which improves the overall integrity of the network.

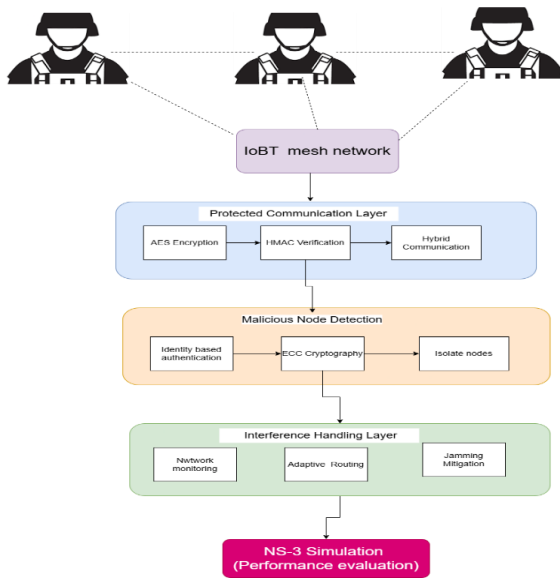


Fig 2: Methodology

Network behaviour is continuously observed to identify possible jamming attacks. Key performance parameters such as packet delivery and transmission success are analysed during this process. A noticeable drop in these metrics is treated as an indication of interference in the communication channel. Once such interference is detected, a mitigation mechanism based on dynamic channel switching is used.

The system then switches communication to an alternative channel with lower interference, which helps restore stable communication and reduce packet loss. Finally, system performance is evaluated using metrics like Packet Delivery Ratio (PDR), throughput, packet loss, and end-to-end delay. These metrics together provide a clear assessment of network performance under normal, attack, and mitigation conditions.

4.1. Network Initialization and Communication Setup

A wireless, infrastructure-less network is created using the ns-3 network simulator to represent a Military Internet of Things (IoT) environment.

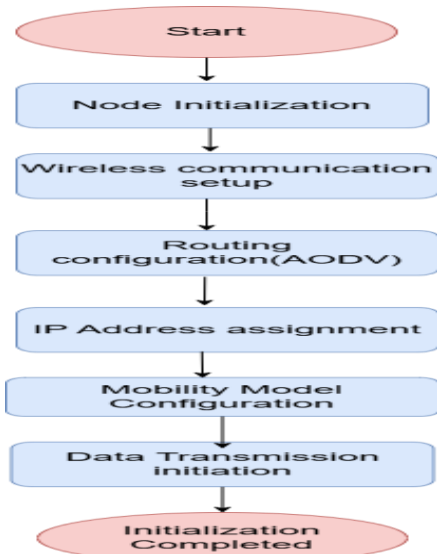


Fig 3: Network Initialization setup

Figure 3 shows the network initialization setup. The network is made up of multiple nodes, including sensors, communication units, and mobile devices, arranged in a defined topology to reflect realistic deployment conditions. The Ad hoc On-Demand Distance Vector (AODV) routing protocol is used to support efficient path discovery and communication between nodes. It also enables dynamic routing, allowing nodes to establish communication paths under mobility conditions. Each node is configured with suitable mobility and communication parameters to represent real-world battlefield scenarios. Continuous data transmission is maintained among nodes to evaluate network performance under normal operating conditions. This simulation setup provides a controlled environment for analysing network behaviour, identifying possible security threats, and evaluating the effectiveness of the protection and mitigation mechanisms.

4.2.ECC-Based Authentication for Secure Node Participation

To prevent unauthorized access, the system applies an authentication mechanism based on Elliptic Curve Cryptography (ECC). It is preferred due to its ability to offer strong security with low computational overhead, which makes it suitable for resource-constrained IoT devices.

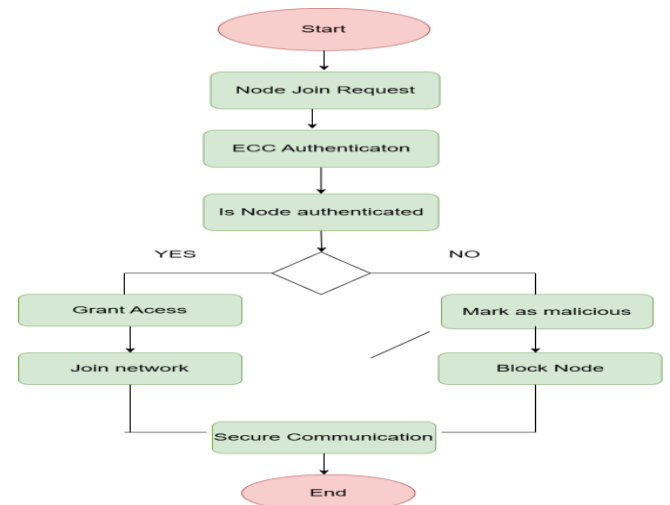


Fig 4: ECC Authentication

Figure 4 shows the ECC-based authentication process. Each node that attempts to join the network is assigned a unique cryptographic identity, which is verified during the authentication stage. Only nodes that successfully pass this verification are allowed to participate in network communication. Nodes that fail authentication or show abnormal behaviour are treated as rogue nodes and are denied access.

This mechanism ensures that only trusted devices can interact within the network, thereby improving overall security and preventing malicious activities. The use of ECC also supports efficient identity verification while maintaining low resource

consumption, making it suitable for Military IoT environments.

4.3. Jamming Attack Detection

During a jamming attack, normal communication is disrupted due to interference in the wireless medium, which significantly affects network performance. This interference introduces noise, resulting in increased packet loss and reduced communication efficiency.

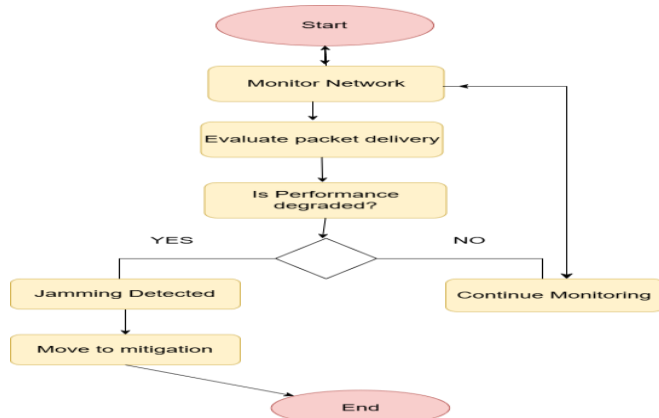


Fig 5: Jamming Attack detection

Figure 5 illustrates the jamming detection process. The system continuously monitors key performance parameters such as packet delivery ratio and transmission success rate. A decline in these metrics suggests the presence of jamming activity, as a noticeable degradation is considered an indication of interference within the network. This detection approach relies on performance analysis rather than direct identification of attack patterns, making it effective in dynamic environments. Once such conditions are detected, the system initiates appropriate mitigation mechanisms.

4.4. Jamming Mitigation using Dynamic Channel Switching

Due to interference in the communication channel, network performance is significantly degraded during jamming attacks. To address this issue, a mitigation mechanism based on dynamic channel switching is implemented.

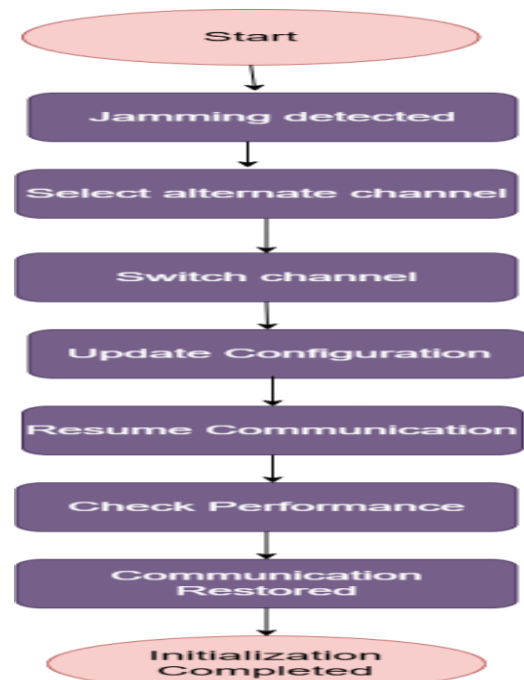


Fig 6: Jamming Mitigation

Figure 6 illustrates the jamming mitigation process. When interference is detected, the system selects an alternative communication channel with lower interference levels. The network configuration is then updated, and communication is shifted to the new channel. As a result, normal communication is gradually restored, and overall network performance is stabilized. This adaptive switching mechanism helps the network avoid congested or affected channels, thereby reducing packet loss and improving transmission reliability.

4.5. Performance Evaluation

Performance analysis of the proposed scheme is carried out by examining several performance factors using the Flow Monitor utility, which is part of the ns-3 simulation environment. The parameters considered for evaluation include Packet Delivery Ratio (PDR), throughput, packet loss, and end-to-end delay. These metrics provide a clear understanding of network performance under different scenarios.

After applying the mitigation method, the results indicate a noticeable improvement in overall network performance. In particular, the Packet Delivery Ratio increases significantly, reaching a range of about 93–98%.

5.Results and discussion

Simulation of this system was performed using the network simulator ns-3. This allows evaluating the ability of the system to detect the presence of malicious nodes and resist jamming attacks. Simulation is carried out for different scenarios, which include the behaviour of networks during

normal operation, during attack conditions, and during the application of mitigation methods.

Table 1: Comparison of different conditions

Parameter	Normal	Rogue Attack	Jamming	Mitigation
Packet Delivery Ratio	97–100%	87%	50–70%	93–98%
Throughput	223.98 Kbps	205.53 Kbps	80–120 Kbps	470.50 Kbps
End-to-End Delay	5.82 ms	9.81 ms	1000–1300 ms	30.95 ms

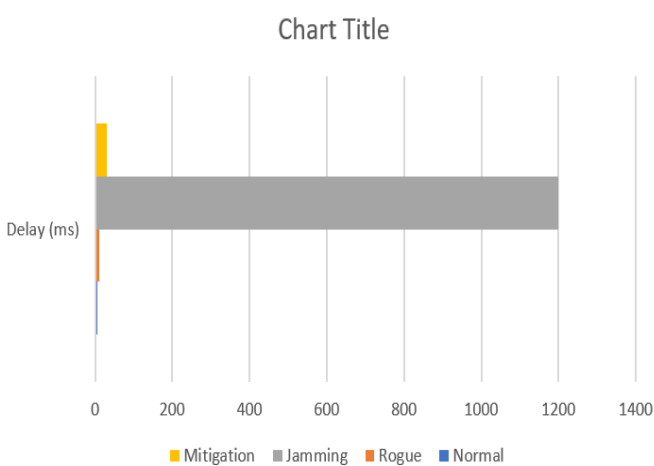


Fig 9: End-to-End delay variation under different network conditions.

The results summarized in Table 1 indicate that network performance is significantly affected by jamming attacks, as reflected in the reduction of packet delivery. To overcome this issue, an adaptive channel switching approach is applied, enabling a shift to a less congested communication channel and helping maintain stable data transmission. Performance evaluation is carried out using key metrics such as Packet Delivery Ratio (PDR), packet loss, throughput, and end-to-end delay. After applying mitigation techniques, clear improvements are observed. The Packet Delivery Ratio increases to approximately 93–98%, packet loss is reduced, throughput shows improvement, and delay remains within acceptable limits. The ECC-based authentication mechanism achieved a detection accuracy of 97.41%, ensuring effective identification of unauthorized nodes. Visualization using NetAnim illustrates network behaviour under different conditions. Initially, nodes operate normally, followed by noticeable degradation during the attack phase. After mitigation, recovery is observed, and stable communication is restored. These results indicate that the system is capable of effectively detecting malicious nodes and mitigating the impact of jamming attacks, thereby improving both network performance and communication reliability in Military IoT environments.

6.CONCLUSION

In this study, a secure and resilient communication framework is developed for Military Internet of Things (IoT) networks to handle challenges such as rogue node intrusion and jamming attacks. The system makes use of Elliptic Curve Cryptography (ECC)-based authentication to ensure that only legitimate nodes are allowed to participate, which improves overall security and trust. To deal with interference, a jamming detection and mitigation mechanism based on dynamic channel switching is applied, helping to maintain stable communication under different conditions. The system is tested using the ns-3 network simulator, and its performance is evaluated using metrics such as Packet Delivery Ratio (PDR), throughput, packet loss, and end-to-end delay.

Detection Accuracy of ECC-Based Authentication
ACCURACY (%)

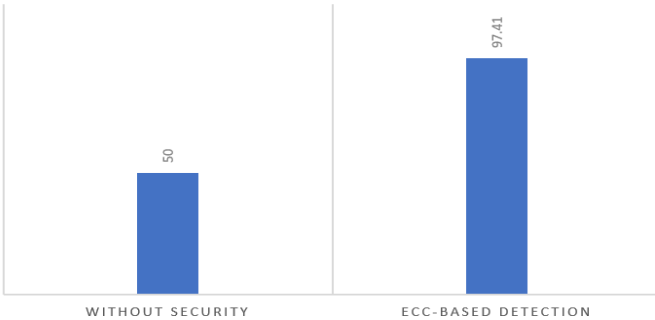


Fig 7: Detection accuracy of the ECC-based authentication mechanism

Packet Delivery Ratio under Different Network Conditions

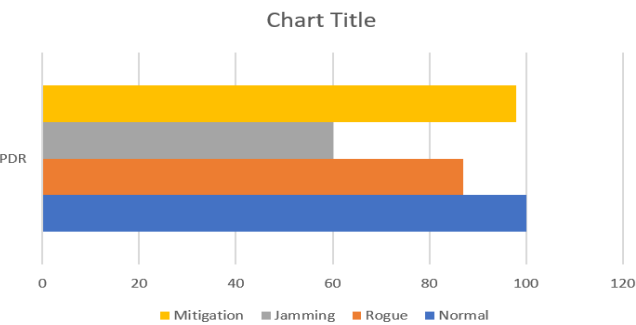


Fig 8: Packet Delivery Ratio under normal, attack, and mitigation conditions.

End-to-End Delay under Different Network Conditions

The results show that the approach maintains a high Packet Delivery Ratio of approximately 93–98%, along with improved throughput and reduced packet loss during attack scenarios. These observations suggest that the system is capable of maintaining reliable communication even under adverse conditions. Overall, the framework improves the security, stability, and efficiency of Military IoT networks, making it suitable for real-time and mission-critical applications. Compared to existing methods that focus only on authentication or jamming mitigation, this approach combines both mechanisms, leading to better overall network security and reliability.

7.FUTURE SCOPE

In future work, the system can be further improved by incorporating advanced techniques to enhance detection accuracy and adaptability. Machine learning algorithms may also be integrated to enable faster and more accurate identification of jamming attacks under dynamic conditions. In addition, adaptive frequency hopping techniques can be considered as an alternative to fixed channel switching, which can improve resilience against interference. Since the current work is based on simulation, future efforts may focus on real-time implementation using hardware-based IoT devices to validate practical feasibility. Further improvements can include adding security mechanisms to handle more complex threats such as denial-of-service attacks and coordinated multi-node attacks. Scalability can also be examined by evaluating system performance in larger and more dynamic network environments. These enhancements would help improve the robustness, efficiency, and applicability of the proposed framework in real-world Military IoT scenarios.

Statements and Declarations

Funding: The authors declare that no funds, grants, or other support were received during the preparation of this manuscript.

Competing Interests: The authors have no relevant financial or non-financial interests to disclose.

REFERENCES

- [1] M. M. U. Rahman et al., “End-to-End Encrypted IoT System for Military Communications,” 2025.
- [2] I. Vulić et al., “Model for Authenticating the Internet of Military Things and Internet of Battlefield,” 2020.
- [3] R. Kufakunesu et al., “The Internet of Battle Things: A Survey on Communication Challenges and Recent Solutions,” 2025.
- [4] D. Marabissi et al., “IoT Nodes Authentication and ID Spoofing Detection Based on Physical Layer Security and Machine Learning,” 2022.
- [5] P. Rutravigneshwaran et al., “Security Model to Mitigate Black Hole Attack Using Trust and K-Means Clustering,” 2023.
- [6] G. Ramkumar, “Innovative Models for Advanced Military IoT Communications using IO-CBCM,” 2025.
- [7] A. Ashraf and M. Sagheer, “Efficient Detection of Reactive Jamming Attacks in IoT Networks,” 2025.
- [8] H. Pirayesh and H. Zeng, “Jamming Attacks and Anti-Jamming Strategies in Wireless Networks: A Survey,” 2022.
- [9] N. Namvar et al., “Jamming in the Internet of Things: A Game-Theoretic Perspective,” 2016.
- [10] Additional clustering/optimization-based IoT communication study (from uploaded set).
- [11] Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of Things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys & Tutorials*, 17(4), 2347–2376.
- [12] Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks*, 76, 146–164.
- [13] Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed Internet of Things. *Computer Networks*, 57(10), 2266–2279.
- [14] Zhang, Y., Lee, W., & Huang, Y. (2003). Intrusion detection techniques for mobile wireless networks. *Wireless Networks*, 9(5), 545–556.
- [15] Karlof, C., & Wagner, D. (2003). Secure routing in wireless sensor networks: Attacks and countermeasures. *Ad Hoc Networks*, 1(2–3), 293–315.
- [16] Perrig, A., Szewczyk, R., Tygar, J. D., Wen, V., & Culler, D. E. (2002). SPINS: Security protocols for sensor networks. *Wireless Networks*, 8(5), 521–534.
- [17] Xu, W., Trappe, W., Zhang, Y., & Wood, T. (2005). The feasibility of launching and detecting jamming attacks in wireless networks. *Proceedings of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing*, 46–57.
- [18] Perkins, C. E., & Royer, E. M. (1999). Ad hoc on-demand distance vector routing. *Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications*, 90–100.