International Journal Of Latest Technology In Engineering & Management (IJLTEM)
Volume 8 - Issue 1 {Jan-Feb. 2023} {Page: 16-22}

A Review of Jamming Attacks in Wireless Systems

Sabbar Insaif Jasim[1], Oday Kamil Hamid[2], Nazar Jabbar Alhyani[3]
[1](*Department of Computer Techniques Engineering/ Dijlah university college, Iraq)*
[2](*Department of Computer Techniques Engineering/ Dijlah university college, Iraq)*
[3](*Department of Computer Techniques Engineering/ Dijlah university college, Iraq)*

ABSTRACT: *Jamming attacks in wireless systems involve the purpose of message of (RF) signals to disrupt or degrade the normal process of wireless communication systems. This can be accomplished using a jamming device, which transmits a strong RF signal at the same frequency as the targeted communication system, effectively overpowering and blocking the intended signals. The types of jamming attacks include directed jamming, spreading jamming, and Denial of Service (DoS) jamming. The consequences of jamming attacks can include disruption of critical communications, loss of revenue, and loss of personal privacy and security. To mitigate the effects of jamming attacks, various countermeasures are being developed such as frequency hopping, adaptive modulation, and error correction. However, it's important to note that new types of jamming attacks are likely to emerge as technology advances.*

Keywords: *Jamming Attack, Selective jamming, flooding, denial of service, cryptography and PCF*

Introduction

Jamming is a type of attack on wireless systems that involves transmitting disruptive radio frequency signals on the same frequency as legitimate communication, with the intent to block or disrupt it. The attacker's goal is to prevent communication between legitimate wireless devices or with a network. Various methods are used to carry out jamming, such as portable jammers, drones, and modified consumer devices. To defend against jamming, countermeasures include using spread-spectrum or frequency-hopping techniques to make it harder for the attacker to target a specific frequency, using directional antennas to concentrate the signal and reduce its vulnerability to interference, and implementing jamming detection and mitigation algorithms in wireless devices.

There are various jammer attack techniques [1], including:
1. Directed jamming: This type of attack involves targeting a specific communication link by transmitting a jamming signal directly at the receiver.
2. Flooding jamming: This type of attack involves transmitting a jamming signal on all available frequencies in a specific area in order to disrupt multiple communication links at once.
3. Selective jamming: This type of attack involves selectively jamming certain types of communication (such as voice or data) while allowing other types to pass through.
4. Denial of Service (DoS) jamming: This type of attack jams a wireless channel for an extended period of time to prevent legitimate users from connecting to the network. Jamming attacks can have serious consequences [2], such as:

- Disruption of critical communications, such as emergency services or military operations
- Loss of revenue for businesses that rely on wireless communications
- Loss of personal privacy and security
- Economic damage

Jamming attacks can be mitigated by using techniques such as frequency hopping, adaptive modulation, and error correction in wireless communication systems, see Fig.1. Additionally, using directional antennas and signal power control can also be effective in reducing the effects of jamming attacks. It's important to note that jamming attacks are a significant threat to wireless systems and various countermeasures are being developed to detect and prevent them. However, as technology evolves and new wireless technologies are introduced, new types of jamming attacks are likely to emerge.

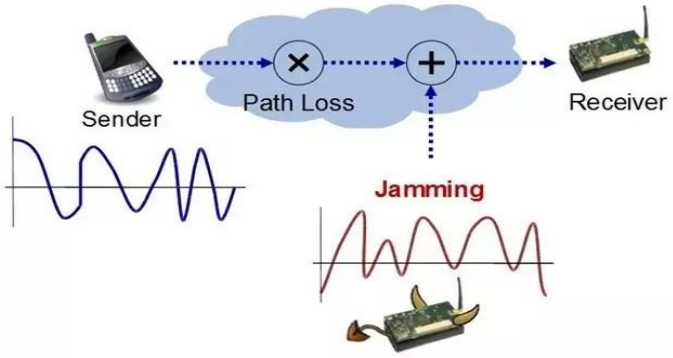

Fig. 1: Jamming attacks techniques

Jamming Attacks in Wireless Systems

Selective jamming attacks were examined in interior danger models, when the opponent knows about network keys and how a protocol is implemented. Bhoomi P. and Anand Ch. suggested solutions to prevent such attacks by using a variety of cryptographic primitives and physical layer attributes to protect real-time packet classification [3]. They explained the significance of particular jamming attacks by executing such attacks against the TCP protocol.

The issue of targeted jamming assaults in wireless networks can be solved. An interior enemy concept was taken into consideration by Vartika Gupta and M. Vinaya Babu[4], where the jammer is a component of the network as attacked and is thus aware of the cover page and network connections' secrets. A selective jammer can dramatically lower performance with relatively little effort, according to a study. They looked into the impact of targeted jamming assaults on route and TCP, two common network protocols. To avoid real-time package identification, systems integrate physical layer features with cryptographic techniques.

The concept of selective jamming in wireless networks was examined.by Parikh D. A , Dr Wandra K.H.[5] . A team of researchers has proposed a method to mitigate selective jamming attacks by using AODV and DSDV routing protocols. Researchers demonstrated how an enemy may boost the effect of his assault at a substantially lower energy cost by taking use of its understanding of how the protocol was implemented.

For rechargeable battery systems, package protection using encryption consumes energy. The demonstrated system enables energy savings and the beginning and termination of attacks by allowing for selective encryption. The number of encrypted packages can be adjusted in accordance with the existence of the attack, as demonstrated by T. K. P. Rajagopal and et, saving energy just when it is required. Because package transfer requires energy, the data stream should be adjusted to the controllability in real time [6]. The IDAS value is evaluated and generated in the system to locate the set of nodes that are engaging in harmful misconduct many others. Due to its ad-hoc nature, it faces multiple security risks. In the Physical Layer and MAC-Sub layer, jamming attacks are important [7].

A new technique that incorporates a recovery mechanism based on weighted backpressure into tree-based routing protocols to protect against jamming assaults in WSNs. The simulation findings provided by Amit Dvir and Levente ButtyanIn, show that the shortest path protocol enhances load, energy, and participation efficiency [8]. Additional study is suggested, including integrating it with RPL protocol, testing it on actual sensor nodes, and contrasting it with RPL global and local service.

A method for analyzing traffic using Received Signal Strength (RSS) to learn concerning jamming and spoofing assaults is proposed by K. Suganthi, K. Sahana, G. Santhiya, and S. Swathi. It serves as a baseline for comparing protection strategies and just needs a few pieces of information, like the timings of packets interception and the positions of jamming attempts and snoopers[9].

A method for spotting wireless network IP spoofing, a hard-to-forge physical characteristic shared by all wireless devices that are independent of cryptography. By spoofing the identification of a node, their method can both track the number of enemies and detect the existence of attacks.

A mitigating technique [10]was developed to extend the life of the WSN by taking into account the jammer's activity and then adopting contemporary paths. The model was developed by Peter S.u, Zeev .V. Zeev B. and Mati G. as an enhancement to the widely used LEACH electrical routing protocol. In simulations, they discovered that proposed protocol significantly extends the duration of the WSN while enhancing its resilience.
Wireless networks are susceptible to jamming assaults because of their open architecture, which makes them challenging to identify and categorize. These attacks can take place at many network layers and employ a range of strategies. One research examined different types of jamming techniques and the placement of jammers for effective jamming. Darko Pajkovski, Nikola Rendevski, Zoran Kotevski, and Tome Dimovski, have studied various jamming detection and localization mechanisms for detection and classification of jamming attacks [11]. Jammers can be classified as elementary or advanced based on their functionality, with both types further divided into sub-groups.

The open nature of wireless communications makes them susceptible to hacker assaults and intrusion efforts. The virtual jamming attack, which is simple to carry out and use little energy, is a significant threat. Newer and more potent identification methods are required to stop this threat. As a treatment, Network Intrusion Detection Systems (NIDSs) have been suggested. To combat practical jamming assaults on IEEE 802.11 networks, a group of scientists has presented a unique Hybrid-NIDS (H-NIDS) based on the Dempster-Shafer (DS), Model of Information [12]. The approach seeks to combine the benefits of an unusual case and handwriting NIDSs, and its effectiveness has been empirically assessed in a variety of circumstances in an IEEE 802.11 network.

R. Akila, T.J. Jeyaprapha, and Dr. G. Sumathi proposed RSA Technique as a method to provide authentication for data and control packets in wireless networks to prevent jamming attacks[13]. They use (Ad-hoc On-demand Distance Vector (AODV)) protocol for routing and OLSR routing protocol based on the identification of poor link stability to improve the route-finding method. They also use EDH as a cryptographic technique and compare the results of throughput, delay, and packet loss to find the best technique.

A selective jammer is considered a negative influence on performance with little effort, according to an evaluation of the effects of selective jamming attacks on network protocols like TCP and routing. Three strategies were created by Dr. Lalith Kumar Kaul, D. Srikanth, and A. Rakesh Reddy to avoid real-time packet categorization and change a selective jammer into an unexpected one, hence improving network performance [14]. Schemes devised to increase security and reduce computational and transmission overhead in wireless networks by fusing physical-layer characteristics with features cryptographic fundamentals including all-or-nothing operations, cryptographic puzzles, and commitment systems. To further safeguard packet delivery, a random key distribution is used.

Mahalakshmi, Shri Bharathi, and Shammi proposed a technique for sending messages in wireless networks even in the presence of an attacker, using wormholes to alert other nodes of the jammer's presence, and sending packets through the shortest path between sender and receiver, resulting in improved performance and reliability of wireless networks, particularly in emergency response operations and military and police networks [15]. In an interior scenario where the jammer is a component of the system and friendly with regardless of the protocol requirements and common network keys, it has been reported that the jammer can classify delivered packages in live time by interpreting the first few letters of a continuous communication, [16]. Nagaraju and UmaRani's examination of the consequences of selective jamming attacks on network protocols like TCP and routing [17]demonstrates how a certain jammer have a significant detrimental impact on performance with little effort. They developed three strategies to avoid real-time packet classification and transform a choosy jammer into an unexpected one by fusing physical-layer characteristics with cryptographic primitives such as commitment mechanisms, cryptographic conundrums, and all-or-nothing changes (AONTs). They next examined each scheme's security, computational expense, and communication overhead.

Dr. Tejinderpal Singh Brar suggested adopting an internal response model, for the jammer is reported of network secrets and protocol requirements, to prevent jamming assaults on wireless networks [18]. The solution involves using cryptographic primitives and physical-layer characteristics to stop real-time package category by the jammer. The effectiveness of the solution was tested and its security, computational, and communication overhead was analyzed. The solution concludes that intrusion detection and prevention systems are still necessary to ensure the security of a network.
Attacks on jamming have a significant impact on communication and autodiscovery, leading to errors in both. The RSSI localization technique is presented by Ahmed A. H., Tharek A. R., and Chee Y. L. in the existence of jamming assaults. The suggested approach, which uses multi-hop communication and different transmission channels and power levels, developed a reliable and precise localization method for wireless sensor systems[19]. They demonstrate that the highly accurate filtering strategy suggested dropped invalid received beacon packets brought on by capture and replay jamming assaults, which clearly minimizes localization error and improves the precision of sensor positioning applications.

From a game theoretical perspective, Moulay A. L., Majed H., Abdelillah K., and Abdelkrim H. presented a power control system based on anti-multi-jamming strategy to deal with numerous smart and common jammers[20]. The method offers analytic formulas for the stationary strategies and confirms the existence and originality of Nash and Stackelberg equilibrium. Additionally, it stated that the jammer with the best Jamming Efficiency Ratio plays the game actively, with the others acting as standby players. Accordingly, the game is limited from the transmitter's perspective to an anti-jamming contest against the jammer with the greatest JER, which is regarded as the only dangerous jammer for the transmitter.Here, we go through the idea of using cryptography-based methods to defend against targeted jamming assaults in wireless networks. This strategy is thought to be safer considering that it is built around the idea of using a fixed key to encrypt the transferred packets. By analyzing the initial several bits of a communication, the authors Rajesh K. Ch. and Sonam Ch. have shown that a jammer may analyze sent packages in real-time [21]. The effect of selective jamming on system performance has also been assessed, and four techniques have been designed to turn a selective jammer into an arbitrary one by prohibiting real-time packet identification. Their suggested approaches integrate physical layer properties with cryptographic techniques like commitment systems, cryptographic puzzles, and all-or-nothing transformations. They have also used six criteria that indicate the Successful Transmission Ratio to examine the security of their suggested schemes.
.It is important to talk about the security risks that Wireless Mesh Networks (WMNs) suffer from both internal and external attackers. However, insider threats are more difficult to thwart since the attacker is already familiar with the network secrets and protocols. It is noted that the majority of external attacks can be prevented with cryptographic techniques and robust communication strategies. In the article, the difficulties of jamming-resistant media transmission in the existence of internal jammers are expressly mentioned as a major obstacle. It was suggested by the author M. Sudhakar to stop using shared secrets to secure broadcast connections, although this compromises performance[22]. Regardless of the fact that there is a significant body of research addressing the issue of misconduct manifested as packet dropping, there are still many obstacles to overcome, including the creation of efficient measures that do not rely on constant overhearing and the efficient upkeep and dissemination of reputation metrics.

Many researchers' discussed the idea and experimental setup of jamming experiments in wireless sensor networks. The authors, Peter Langendoerfer, Steffen Ortmann, and Stephan Kornemann, propose an approach that reacts immediately to changes in the Received Signal Strength Indicator (RSSI) and eliminates the need for preconfigured values, which are difficult to obtain and use due to the impact on the channel depending on the position of the jammer [23]. The approach uses a variance-based estimate of RSSI measurements adapted to sensor needs, providing reliable jamming indication independently of the location of the jammer. The authors plan to further test the approach by implementing varying transmission power at the jammer to simulate different jamming intensities, and testing it on other channel characteristics.
Again many problems of anti-jamming in wireless networks still appear. The authors, Ankit Jain1, Mr. Kush, and Mr. Vijay Malviya, note that detecting jammers is a difficult task, especially for low-power networks[24]. They emphasize that numerous approaches, including intelligent machines, cognitive science, mobile agents, trans, territorial retreats, reliability testing, and spectrum or modulation scheme, have been attempted to address this problem. Nevertheless, precisely identifying jammers is only one aspect of the issue; energy efficiency is also crucial to take into account. Furthermore, it is challenging for a detection system to categorize the kind of detected jammer, and due to mobile nodes in IEEE 802.11n and mobile networks, anti-jamming is particularly challenging in these connections.

Ongoing investigation into the issue of targeted jamming assaults in wireless networks. The inner adversary model is taken into account by the authors O.S.C. Kesavulu and P. Harini, where the jammer is a component of the network that is being attacked and is informed of the purpose of the scheme and shared network secrets. They suggest two methods that turn a selected jammer into an arbitrary one by blocking real-time package identification: a secret method and a cryptography conundrum [25]. They point out that although All-Or-Nothing Transitions (AONT) involves a minimal transmission and processing overhead, it is not covered in the text. Packet headers is subjected to an openly known and fully invertible pre-processing step called AONT before being sent to a standard block encryption technique. The authors suggest methods that integrate the properties of the physical (PHY) layer with cryptographic primitives.

A packet hiding method is used to block selective jamming attacks. This method can quickly detect a jammer with minimal difficulty. The system presented in the article not only prevents real-time packet classification but also uses a Swarm intelligence algorithm to adapt to changes in network topology and traffic. This technique combines cryptographic primitives with physical layer characteristics, in order to counteract knowledge of the attackers and block real-time packet classification[26]. Underneath an interior danger paradigm, in which the attacker is a member of the system and is aware of network secret information and technical requirements, the issue of selectively jamming assaults in wireless networks needs to be considered. The authors G. Jayanthi, S. Babu, B Lakshmana, P Mohan, and B Sunil created three techniques to counteract these attacks by combining cryptographic techniques such the powerful hiding promise scheme, cryptographic

puzzle hiding system, and all or anything transformations[27]. They compare these systems' performances to examine the security of these systems using simulation, demonstrating that they can increase throughput.

The authors Shikha Jindal and Raman Maini compare two types of attacks, flooding and jamming, in wireless sensor networks. They explain the different types of flooding attacks and their effects on sensor networks and propose defense mechanisms to prevent them. They use two metrics, false positive ratio and false negative ratio, to evaluate the effectiveness of detection mechanisms for flooding attacks. They also explain different types of jamming attacks and detection mechanisms and use metrics to evaluate the effectiveness of these mechanisms. They then compare the two types of attacks and conclude that jamming attacks are harder to detect than flooding attacks [28].

For the goal of identifying and fighting off jamming assaults in wireless sensor networks, many defense measures were developed (WSNs). Basic tactics, like spectral efficiency, carrier sensing time, and PDR, are good at spotting jamming attacks but fall short when it comes to thwarting it. Modern techniques can locate the source of packet problems but cannot stop jamming. Spectrum hopping, locational getaways, and region-based signal to noise ratio are some techniques that Mehreen Shaikh, Abid, and H Syed employed to avoid jamming, however they have problems such asynchrony, delay, and complexity. Reactive jammers are not effectively blocked by these techniques. The researchers suggest a novel technique called the trigger identification method, which is mathematically predicted to be able to detect and protect versus reactive jammers with little communication overhead and temporal complication [29].

Wireless communications are particularly susceptible to malware activity since the common media is transmitted. Jamming in Wi-Fi communication is a challenge that Moulay A. L., Majed H., Abdelillah K., and Abdelkrim H. take on. They concentrate on a jammer that records the packet's regeneration efforts through to the point at when it is lost [30]. Thus according simulation implementation findings, the transmitter can increase its effectiveness by anticipating the jammer's response in accordance with its unique approach, ignoring the jammer's capacity to sense the active channel.

A proposed security mechanism is discussed by C. K. Marigowdaand et, to overcome common and critical attacks, such as denial of service (DoS), jamming, and replay attack in Wireless Sensor Networks (WSN). AES with OCB mode encryption algorithm is utilized to provide network layer security that offers both confidentiality and authenticity with low energy consumption. The proposed method is effective in providing security against these attacks without degrading network performance and increasing network lifetime[31].

A study looks into connection jamming techniques that require little to no previous information of the intended protocols. The suggested methods have been shown to be almost as efficient and energy-efficient as previous methods, which were based on detailed knowledge of MAC protocols. The encryption of data packets does not hinder the effectiveness of the least knowledge attacks. In order to increase security for wireless sensor networks against link-layer jamming, the authors Yee Wei Law, Lodewijk van Hoesel, Jeroen Doumen, Pieter Hartel, and Paul Havinga advice using encryption, spread spectrum hardware, and TDMA protocol. Future research should examine the qualities of MAC protocols that are resistant to connectivity jamming assaults [32].

A protection device was suggested by Dr. Syeda Gauhar Fatima to safeguard wireless networks from jamming assaults [33]. Five steps make up the method's shared key: traveling series generation, travelling process allocation, control channel capacity, affected node recognition, and hopping process updating. The network is capable of isolating malicious nodes and unusual receive data by enclosing any aberrant data packets in a secure coat and sending them to the target node with a spreading code.

The Intelligent Reflecting Surface (IRS) is a new technology in wireless communications that can enhance signal-to-noise ratio and spatial diversity of wireless channels. However, research by Paul Staat et al. has shown that the IRS can also be used to degrade available data rates in entire networks through an "Eavesdropping and Jamming attack" (ERA). Their study shows that the attack is effective with small IRS sizes and they demonstrate a practical ERA that can slow down a Wi-Fi network [34].

Shayma W. Nourildean, Sabbar Insaif Jasim, May T. Abdulhadi, Mustafa Musa Jaber investigated a jamming attack on a Mobile Ad Hoc Network (MANET) and how it affects network QoS parameters. The problem is solved by using the Point Coordination Function (PCF) mechanism in selected MANET nodes (guard nodes) to improve network performance. Results from simulations with different numbers of jammers and transmission power values show that PCF improves network throughput and reduces delay. The study concludes that PCF is a good solution for jamming attacks on ad hoc networks and can be applied in practice[35]

Conclusion

Jamming attacks in wireless systems have become a significant concern for the security and reliability of wireless networks. Research on jamming attacks has focused on various techniques to detect and prevent these attacks, including the use of spread-spectrum techniques, cooperative communication, and advanced encryption methods. Additionally, several countermeasures have been proposed to mitigate the effects of jamming attacks, such as using jamming-resistant protocols, and implementing anti-jamming algorithms in wireless devices. Overall, the research on jamming attacks in wireless systems has shown that these attacks can have a significant impact and more critical performance of wireless networks, that it is important to continue to develop new techniques to detect and stop these attacks to guarantee the safety of the security, stop these assaults.Reliability of wireless networks and further research is needed to understand how jamming attacks can be effectively mitigated in these high-consequence scenarios.

REFERENCES

[1] *E. Bout, V. Loscri, and A. Gallais, "Energy effective jamming attacker in wireless network," in Journée thématique du GT SSLR 2021 sur la sécurité des réseaux, 2021.*

[2] *H. Pirayesh and H. Zeng, "Jamming attacks and anti-jamming strategies in wireless networks: A comprehensive survey," IEEE Communications Surveys & Tutorials, 2022.*

[3] *B. Patel and A. Chauhan, "An Improved Packet Hiding Method for Preventing Selective Jamming Attacks in Wireless LAN."*

[4] *V. GUPTA and B. MVinaya, "Wireless Network Packet Classification Selective Jamming Attacks," 2014.*

[5] *D. Parikh and K. Wandra, "Performance Analysis of Routing Protocols for Preventing Selective Jamming Attacks in Wireless Network."*

[6] *T. Rajagopal, R. Balaji, K. Ravikumar, and N. Ranjith, "Securing the Wireless Network from Jamming Attacks Using Anonymity."*

[7] *T. Ramesh and S. Meenatchi, "A Survey on the Defense Mechanisms of Jamming Attacks in Wireless Networks," INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY, ISSN, pp. 2277-9655, 2013.*

[8] *A. Dvir and L. Buttyan, "Backpressure Approach for Bypassing Jamming Attacks in Wireless Sensor Networks," in Proceeding of the IEEE Conference on Computer Communications (INFOCOM), Poster Session, 2011.*

[9] *K. Suganthi, K. Sahana, G. Santhiya, and S. Swathi, "DETECTION OF SPOOFING AND JAMMING ATTACKS IN WIRELESS SMART GRID NETWORKS USING RSS ALGORITHM," 2018.*

[10] *P. Soreanu, Z. V. Volkovich, Z. Barzily, and M. Golani, "MITIGATING JAMMING ATTACKS IN WIRELESS SENSOR NETWORKS: AN ENERGY-EFFICIENT METHOD IN A MOBILE JAMMER ENVIRONMENT," International Journal of Pure and Applied Mathematics, vol. 56, no. 4, pp. 533-550, 2009.*

[11] *D. Pajkovski, N. Rendevski, Z. Kotevski, and T. Dimovski, "Classification of Jamming Attacks and Detection and Prevention Techniques in Local Wireless Networks," in Proceedings/8 th International conference on applied internet and information technologies, 2018, vol. 8, no. 1: "St Kliment Ohridski" University-Bitola, Faculty of Information and …, pp. 154-160.*

[12] *D. Santoro, G. Escudero-Andreu, K. G. Kyriakopoulos, F. J. Aparicio-Navarro, D. J. Parish, and M. Vadursi, "A hybrid intrusion detection system for virtual jamming attacks on wireless networks," Measurement, vol. 109, pp. 79-87, 2017.*

[13] *R. Akila, T. Jeyaprapha, and G. Sumathi, "Providing Authentication in Wireless Network to Prevent Jamming Attacks."*

[14] *L. K. Kaul, D. Srikanth, and A. R. Reddy, "Prevent Jamming Attacks in Wireless Networks by CPHS, SHCS and AONT Techniques."*

[15] *B. Mahalakshmi, S. S. Bharathi, and W. L. Shammi, "Maximizing the Performance and Reliability of Wireless Network by Preventing Jamming Attacks."*

[16] *J. M. McCune, E. Shi, A. Perrig, and M. K. Reiter, "Detection of denial-of-message attacks on sensor network broadcasts," in 2005 IEEE Symposium on Security and Privacy (S&P'05), 2005: IEEE, pp. 64-78.*

[17] *V. Nagaraju and N. UmaRani, "Preventing Jamming Attacks in Wireless Networks."*

[18] *T. S. Brar, "Study and Detection of Jamming attacks in Wireless Networks."*

[19] *A. A. Hussein, T. A. Rahman, and C. Y. Leow, "THROUGHPUT ENHANCEMENT OF WIRELESS SENSOR NETWORK LOCALIZATION ACCURACY AGAINST JAMMING ATTACKS," Journal of Theoretical and Applied Information Technology, vol. 78, no. 1, p. 53, 2015.*

[20] *M. A. Lmater, M. Haddad, A. Karouit, and A. Haqiq, "Several Jamming Attacks in Wireless Networks: A Game Theory Approach," International Journal of Advanced Computer Science and Applications, vol. 10, no. 2, 2019.*

[21] *R. K. Chakrawarti and S. Choubey, "Implementation of cryptography based methods to prevent selective jamming attacks for true communication in wireless network [EB/OL]," ed.*

[22] *M. Sudhakar, "A Study Of Wireless Mesh Networks Insider Attacks Of Selective Jamming Or Dropping," IOSR J. Electron. Commun. Eng, vol. 11, no. 2, pp. 60-66, 2016.*

[23] *P. Langendoerfer, S. Ortmann, and S. Kornemann, "Demonstrating self-contained on-node counter measures for various jamming attacks in wireless sensor networks," SIGMOBILE Mob. Comput. Commun. Rev, vol. 15, pp. 39-40, 2011.*

[24] *A. Jain, K. Bhushanwar, and V. Malviya, "A survey on jamming attacks and its types in wireless networks," International Journal of Technology Research and Management, vol. 4, pp. 1-8, 2017.*

[25] *O. Kesavulu and P. Harini, "Enhanced packet delivery techniques using crypto-logic riddle on jamming attacks for wireless communication medium," IJCSNS, vol. 14, no. 7, p. 65, 2014.*

[26] R. Naresh and K. P. Kumar, "Prevention of Selective Jamming Attacks Using Packet Hiding Methods in Wireless Networks," International Journal of Computer Science & Mobile Computing, vol. 3, pp. 25-28, 2014.

[27] G. J. Lakshmi, S. Babu, B. L. Rao, P. Mohan, and B. S. Kumar, "Jamming Attacks Prevention in Wireless Sensor Networks Using Secure Packet Hiding Method," International Journal of Advanced Research in Computer and Communication Engineering, vol. 2, no. 9, 2013.

[28] S. Jindal and R. Maini, "Comparative Analysis of Flooding and Jamming Attacks in Wireless Sensor Networks," International Journal of Engineering Research, vol. 3, no. 4, 2014.

[29] M. Shaikh and A. H. Syed, "A survey on jamming attacks, detection and defending strategies in wireless sensor networks," International Journal of Research in Engineering and Technology, vol. 3, no. 3, pp. 558-61, 2014.

[30] M. A. Lmater, M. Haddad, A. Karouit, and A. Haqiq, "Smart Jamming Attacks in Wireless Networks During a Transmission Cycle: Stackelberg Game with Hierarchical Learning Solution," International Journal of Advanced Computer Science and Applications, vol. 9, no. 4, 2018.

[31] C. Marigowda, J. Thriveni, S. Gowrishankar, and K. Venugopal, "An efficient secure algorithms to mitigate DoS, replay and jamming attacks in wireless sensor network," in Proceedings of the world congress on engineering and computer science, 2018, vol. 1.

[32] L. van Hoesel and J. D. P. H. P. Havinga, "Energy-efficient link-layer jamming attacks against wireless sensor network MAC protocols," Faculty of Electrical Engineering, Mathematics and Computer Science University of Twente, AE Enschede, Netherlands, 2005.

[33] S. G. Fatima, S. A. Sattar, and M. Sadiq, "Efficient Defense System for Jamming Attacks in Wireless Sensor Networks," Technology, vol. 9, no. 4, pp. 22-35, 2018.

[34] P. Staat, H. Elders-Boll, C. Zenger, and C. Paar, "Mirror Mirror on the Wall: Next-Generation Wireless Jamming Attacks Based on Software-Controlled Surfaces," arXiv preprint arXiv:2107.01709, 2021.

[35] S. Nourildean, S. Jasim, M. Abdulhadi, and M. Jaber, "Point coordination mechanism based mobile ad hoc network investigation against jammers," Eastern-European Journal of Enterprise Technologies, vol. 5, pp. 45-53, 10/27 2022, doi: 10.15587/1729-4061.2022.265779.