Survey on Jamming Wireless Networks: Attacks and Prevention Strategies

S. Raja Ratna, R. Ravi

Abstract—Wireless networks are built upon the open shared medium which makes easy for attackers to conduct malicious activities. Jamming is one of the most serious security threats to information economy and it must be dealt efficiently. Jammer prevents legitimate data to reach the receiver side and also it seriously degrades the network performance. The objective of this paper is to provide a general overview of jamming in wireless network. It covers relevant works, different jamming techniques, various types of jammers and typical prevention techniques. Challenges associated with comparing several anti-jamming techniques are also highlighted.

Keywords—Channel, Cryptography, Frequency, Jamming, Legitimate, Security, Wavelength.

I. INTRODUCTION

SYSTEM issues and attack management have become prime importance for communication in wireless networks. Due to the broadcast nature of the wireless medium, wireless networks are highly vulnerable to attacks. There are many different attack strategies an adversary can use to disturb wireless communications. One of the most effective attacks on wireless networks is Denial-of-Service (DOS) attack. Jamming attack is a sub class of DOS attack [3], [6], [7], [9], [28], [36], [53]. DOS intensely attempt to prevent legitimate users from reaching a specific network resource. This paper focuses on jamming attack. Jamming attack intentionally disrupts the network service.

Jammer [3], [4] is an entity who is purposefully trying to interfere with the physical transmission and reception of wireless communications. The objective of jamming attack [16] is to prevent a legitimate sender or receiver from transmitting or receiving packets. A jammer may either corrupt control packets or reserve the channel for the maximum allowable number of slots, so that other nodes experience low throughput by not being able to access the channel [13], [54]. Jammer either continuously emits signal on the channel so that the sender will always sense the channel as busy or sends regular data packets and forces the receiver to receive junk packets all the time. In the latter case, the sender successfully sends the packets to the receiver, but the jammer

blast a radio transmission to corrupt the message that the receiver receives.

Jamming disrupt wireless transmission unintentionally either in the form of interference, noise or collision at the receiver side [12]. It overpowers the transmitted signals by injecting high level of noise which lowers the signal-to-noise ratio, thereby reducing the probability of successful packet reception [23]. An ideal jamming attack [5] should have high energy efficient, reduced probability of detection, resistant to anti jamming techniques and also disrupts the communications to maximum possible extent.

The paper proceeds as follows. Section II describes attack analysis and different types of jammers. Section III explains the comparison of various anti jamming techniques. Finally, Section IV concludes the paper.

II. ATTACK ANALYSIS

Communication security is correlated to two features, system reliability and message secrecy. Transmission of secret message to a legitimate receiver under certain conditions is known as message secrecy. The enemy of message secrecy is eavesdropper [1], [2], [27], [78]. If a certain encoded message intended for a specific legitimate receiver is reliably received by that receiver, it is known as system reliability. The enemy of system reliability is jammer [16], [65].

A. Active and Passive Attacks

Attacks can be categorized as active or passive. Passive attackers does not send any message, but just listens to the channel and also steal the packets containing IP addresses, location of nodes, etc. They do not disrupt communication or cause any direct damage to the network, but seek information and violates the network confidentiality. An example is eavesdropping. The sole purpose of an eavesdropper is to listen to the transmission and to obtain some confidential information that should be kept secret during communication. The confidential information includes the location, public key, private key, or even passwords of the nodes [25].

Active attackers disrupt the normal operation of a specific node or target the operation of the whole network. Active attacker performs injecting of packets to wrong destinations, dropping of packets, deleting packets and modifying the contents of packets which violate availability, integrity, authentication, and non-repudiation paradigm. An example is jamming attack. Active attackers like eavesdroppers can be prevented using cryptographic measures whereas passive attackers like jammers are hard to detect and prevent [24].
B. Internal and External Attacks

Jamming attack in wireless network falls under the following two categories [26], external attack [10], [28], [69] and internal attack [8], [43], [49], [61], [73], [77], [79]. In external attack, the jammer lies outside the network and is not a part of the network. It may either cause congestion or propagate fake routing information or disturb the nodes from providing services. In internal attack, the jammer becomes a part of the network knowing all network secrets and participates in various malicious activities.

C. Classification of Jamming Attack

There are two classifications of jamming attack, PHY jamming/RF jamming and MAC layer/Virtual jamming. Jamming is usually aimed at the physical layer, but they may also be occurred at the MAC layer [10]-[14], [22], [54].

Jamming at the physical layer is PHY jamming [15]. In PHY jamming [74], the jammer sends high power signal to cause extremely low SNR ratio at legitimate receiver, thereby corrupting the communication link. It is launched by continuous transmissions or by causing packet collisions at the receiver side. The goal of this jamming is to distort the legitimate signal by sending unwanted signals or noise on the same radio channel, thereby preventing proper reception of the signal at the receiver [45].

Jamming at the medium access control layer is MAC jamming. MAC jamming attacks either the control frames or data frames. The jammer [12], [13], [20] disrupts the legitimate user’s packet transmission by sending jamming packets on the RTS/CTS frames or DATA frames [17], [18]. A significant advantage of MAC jamming is that the attacker node consumes less power in targeting these attacks when compared to PHY jamming.

D. Jamming Methods

Generally one of the following four jammers is used for jamming. The jamming models [3], [19], [21] in PHY jamming are constant, deceptive, random, and reactive.

1. Constant Jammer

Constant jammer constantly emits random meaningless noise signals on the wireless medium and it will not wait for the channel to be idle before transmitting.

2. Deceptive Jammer

Deceptive jammer constantly injects regular packets of noise signal with no gap between them. Deceptive jammer is similar to constant jammer [3]; the similarity between the two is that both continually emit noise signals. The main difference is that constant jammer continuously emits random noise signal, whereas the deceptive jammer continually emits noise signal on the channel without any gaps between the transmissions. Therefore, the user believes that some legitimate transmission is going on. Deceptive jamming is harder to detect than constant jammer. Both constant and deceptive jamming hinders the transmission and target transmission at the receiver side. One disadvantage of both the jammers is their power efficiency, because the signal is emitted continuously on the channel, their power efficiency is poor.

3. Random Jammer

A random jammer randomly emits noise signal on the wireless medium and considers energy conservation. For a random period of time the jammer behaves like constant jammer or deceptive jammer and then remains ideal for another random period of time. Main advantage of this jammer is that it saves energy which is very important.

4. Reactive Jammer

Of the four jammers, the smarter and most power efficient one is the reactive jammer which targets the reception of a packet and deterministically jams only when the communication medium is busy [30]-[35]. This jammer remains quiet until there is activity on the channel, it constantly senses the channel and when it finds packet transmission it immediately transmits radio signal and causes collision at the receiver side. Reactive jammer spent more energy for sensing the channel and spends little energy to interrupt the packet. It takes smarter jamming decision. Detection of this jamming is very challenging because it minimizes the risk of exposure. Its network performance does not degrade heavily; the overall throughput under reactive jammer is higher than the throughput obtained against other jammers.

III. COMPARISON OF ANTI JAMMING TECHNIQUES

Recovery from jamming attack requires an efficient prevention mechanism. In wireless network, prevention approaches are more important because an efficient approach can increase the network performance. Existing jamming prevention techniques are wavelength assignment [37], [38], [62], Channel surfing [39], [40], [52], [63], [70], Game theory approach [41], [44], [46], [51], [71], Zonalization [42], Trigger identification [33], Frequency hopping [23], [29], [47], [50], [60], [64], [68], [73], [75], Threshold based technique [31], [48], Cryptographic key distribution [56], [66], Detection based prevention [58], [67], Multi path routing [55], [57], [59], Packet hiding [27], [72], [76].

A. Channel Surfing

Channel surfing is an effective method to prevent jamming attack in wireless communications. Two parties have to negotiate beforehand, in order to agree on the channel switching sequence. Different channel surfing techniques are listed in Table I.

B. Wavelength Assignment

Deliberate high powered jamming attack seriously degrades the network performance and must be dealt efficiently. One of the most important challenges in preventing jamming attack is successfully solving using routing and wavelength assignment problem. Different wavelength assignment techniques are listed in Table II.
In frequency hopping techniques, a transmitter changes the frequency bands on which the signals are transmitted. The entire spectrum of the communication system is divided into a number of frequency bands and the time is divided into time slots. Each user is assigned a frequency-hopping pattern that is served as the spreading code. Frequency hopping techniques are very effective in coping with jamming attacks and different techniques are listed in Table IV.

**Table IV**

<table>
<thead>
<tr>
<th>Technique Description</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Each node has a designated control channels. They communicate with its neighbours on different channels and are dynamically coordinated between them. Wireless fading channel state is used as a random shared secret between legitimate parties to achieve channel agreement. Provides jamming-resistant communication.</td>
<td>Efficient as compared to other proactive schemes. No extra communication overhead. Strong security and robust. Achieve better robustness. Packet delivery ratio is better than channel surfing. Detects attackers efficiently. Increase packet delivery ratio. Increases network throughput.</td>
<td>Efficiency reduces if burst of packets are exchanged between pairs of nodes. Performance degrades when two parties use different transmission power. Works well only for infrastructure-based networks and not for ad hoc networks. Does not deal with multiple malicious nodes in collision. Could not overcome sophisticated smart jammers.</td>
</tr>
</tbody>
</table>

**Table II**

<table>
<thead>
<tr>
<th>Technique Description</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimizes the damage caused by jamming and achieves significant prevention measures without the need for specialized equipment. Prevention oriented method help attack localization and source identification in the network planning phase.</td>
<td>Improves network security and robustness. Minimizes in-band cross talk jamming and number of wavelengths used. Improve network security and robustness. Minimum extra cost.</td>
<td>Attacking probability varies with respect to the distance from attacking point. Jamming attack scenarios are not included in the network planning phase. Attack-aware wavelength assignment is not considered.</td>
</tr>
</tbody>
</table>

**Table III**

<table>
<thead>
<tr>
<th>Technique Description</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Achieve better performance than from myopic learning. Minimizes worst-case damage caused by attackers. Smart jammers are dealt. Achieve higher payoff than existing approaches. Lower jamming probability.</td>
<td>Does not work well for ad hoc networks. Learning process goes wrong if SU wrongly estimate the parameters. Does not deal with Nash equilibrium points. Signal to Noise ratio is reduced.</td>
<td></td>
</tr>
</tbody>
</table>
One solution is to randomly assign keys and then connect each other with some probability. Different cryptographic key distribution techniques are listed in Table VII.

### TABLE IV

<table>
<thead>
<tr>
<th>Technique</th>
<th>Description</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Code tree based system [23]</td>
<td>A protocol allows a broadcast communication system to dynamically change the spreading codes used by subsets of receivers. The receiver detects jamming by receiving a secondary message without a primary message.</td>
<td>It uses much shorter packets thereby reducing the packet error rate. Spreading codes are dynamically changed.</td>
<td>To mitigate jamming it relies only on keying and not on other physical characteristics.</td>
</tr>
<tr>
<td>Time-delayed broadcast [29]</td>
<td>This scheme is used for jamming-resistant broadcast communications in the presence of inside jammers. The broadcast is realized as a series of uni cast transmissions distributed in frequency and time.</td>
<td>Maintain broadcast communications even when multiple nodes are compromised. Network throughput is maximized.</td>
<td>It is designed only for temporarily restoring communications.</td>
</tr>
<tr>
<td>MAC-Uncoordinated Frequency Hopping [47]</td>
<td>This scheme uses Media Access Control strategies for collaborative UHF-based broadcast requiring no pre-shared secret keys. Its communication efficiency is improved through node cooperation.</td>
<td>Minimal broadcast delay and reduce the overall energy consumption without pre-shared keys.</td>
<td>Communication efficiency is a bottleneck for practical applications.</td>
</tr>
<tr>
<td>Randomized Distributed using frequency hopping [50]</td>
<td>Prevents control-channel jamming as well as identifies compromised nodes through their unique sequences and excludes them from the network.</td>
<td>Each node follows a unique hopping sequence. No extra overhead.</td>
<td>Not applicable for full-duplex communication. Used as a temporary solution for control channel re-establishment.</td>
</tr>
<tr>
<td>Anti-jamming Reinforcement ARES [60]</td>
<td>ARES is composed of a rate adaptation and power control modules. Rate adaptation decides between fixed or adaptive-rate assignment. Power control facilitates appropriate clear channel assessment threshold tuning.</td>
<td>Tunes the parameters of rate adaptation and power control. Improve throughput in the presence of jammers.</td>
<td>Utilizes functionalities that are currently unavailable in commercial NIC.</td>
</tr>
<tr>
<td>Frequency Hopping anti-jamming [64]</td>
<td>A game theoretic Framework is provided to capture the interactions between a link and a jammer employing FH</td>
<td>FH seems to be inadequate in coping with jamming attacks. Hybrid scheme by combining the three approaches is not considered.</td>
<td></td>
</tr>
<tr>
<td>Wormhole-Based Anti jamming [68]</td>
<td>Wormholes are used as a defense mechanism using wires, frequency hopping and uncoordinated channel hopping.</td>
<td>Nodes need not to be synchronized.</td>
<td></td>
</tr>
<tr>
<td>Uncoordinated Spread Spectrum [73]</td>
<td>Mathematical models are developed. Randomize the selection of the spreading key such that attackers cannot jam the communication.</td>
<td>Handle an unlimited amount of malicious receivers.</td>
<td></td>
</tr>
<tr>
<td>Optimal Uncoordinated Frequency Hopping [75]</td>
<td>The UHF-based anti-jamming communication is a non-stochastic multi-armed bandit problem. It introduced online optimization theory into the frequency hopping strategy design.</td>
<td>The time and space complexity are reduced.</td>
<td></td>
</tr>
</tbody>
</table>

### TABLE V

<table>
<thead>
<tr>
<th>Technique</th>
<th>Description</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jamming-aware source routing [57]</td>
<td>Traffic is allocated in multiple-path routing in the presence of jammers. Multiple paths are selected based on the knowledge of paths history. Jamming is addressed at the network level and end-to-end data delivery is restored through multipath routing by improving jamming resilience.</td>
<td>Achieves optimized throughput. Achieves smaller communication cost and effectively identifies multiple paths. Resistant to variety of jammers.</td>
<td>Effects are characterized statistically and not practically. Wrongly predicts future correlation if the previous path history is not updated correctly.</td>
</tr>
<tr>
<td>Availability History Vectors algorithm based on Multi path Routing [59]</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### TABLE VI

<table>
<thead>
<tr>
<th>Technique</th>
<th>Description</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multi-packet transmission (MPT) and Multi-packet reception (MPR) [48]</td>
<td>The effect of jamming signals mitigated based on the probability of success and throughput. Maximum throughput is obtained by the proper adjustment of the transmitting and receiving probability of each node.</td>
<td>Attains maximum throughput. If either MPT or MPR is used, throughput reduces.</td>
<td></td>
</tr>
<tr>
<td>ANTIJAM MAC protocol [31]</td>
<td>It is a simple, fair, and self-stabilizing distributed MAC protocol that is able to make efficient use of a shared communication medium. It mitigates internal and external threats.</td>
<td>Low convergence time and excellent fairness property. Achieves constant throughput at varying network size.</td>
<td>Jammers affecting few bits in a packet cannot be detected.</td>
</tr>
</tbody>
</table>

### TABLE VII

<table>
<thead>
<tr>
<th>Technique</th>
<th>Description</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hybrid key pre-distribution [56]</td>
<td>Supports local connectivity and evaluates spatial retreat strategies. Utilizes the properties of random key pre distribution schemes.</td>
<td>Robust key distribution and provides high key connectivity. Identifies compromised users without its prior knowledge.</td>
<td>Jammers location cause some un jammed nodes to be disconnected from the network. Control messages are not analyzed.</td>
</tr>
<tr>
<td>Greedy User IDENTification algorithm [66]</td>
<td>Mitigates jamming by identifying compromised users using random assignment of cryptographic keys to hide the location of control channels.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
TABLE VIII
HIDING SCHEME

<table>
<thead>
<tr>
<th>Technique</th>
<th>Description</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packet hiding schemes [27]</td>
<td>Three schemes are developed to combine cryptographic primitives with physical layer attributes, to hide the packets between physical and MAC layers.</td>
<td>Prevents real time packet classification.</td>
<td>Network performance degrades under non congestion when compared to under congestion.</td>
</tr>
<tr>
<td>Hiding traffic with camouflage [72]</td>
<td>Min-max approach analyzes the worst-case message delay under jamming. Minimizes delay by increasing redundant traffic into the network.</td>
<td>Decreases message invalidation probability and minimizes delay.</td>
<td>It doesn't improve the performance of nonreactive jamming.</td>
</tr>
<tr>
<td>Resource-efficient hiding [76]</td>
<td>Prevents the leakage of contextual information by involving in bogus traffic source selection phase and rate assignment phase.</td>
<td>Reduces communication overhead. Needs smaller number of fake sources.</td>
<td>Fake sources are static and not dynamic.</td>
</tr>
</tbody>
</table>

H. Hiding Scheme

Hiding schemes are used to hide contextual information's like traffic, data from attackers. It can be hidden using fake data source or between layers. Some hiding schemes are listed in Table VIII.

IV. CONCLUSION

The shared nature of wireless network enables the attacker to carry out attacks easily. This paper has surveyed the main aspects of security against jamming attacks, its vulnerabilities, classification of jamming attacks, jamming models and its effective countermeasures. Four different types of jammers involved in PHY jamming have also been discussed. Among the four, reactive jammer at physical layer is found to be the smarter and efficient one. Various jamming prevention techniques are surveyed and its methodology, advantages, and disadvantages are also compared.

ACKNOWLEDGEMENT

This work was supported in part by Anna University recognized research center lab at Francis Xavier Engineering College, Tirunelveli, India.

REFERENCES

null


S. Raja Ratna received her B.E degree in Electrical and Electronics Engineering from The Indian Engineering College, Tirunelveli in 2000, and the M. Tech degree in Computer and Information Technology from Manonmanium Sundaranar University, Tirunelveli in 2005. She is working towards Ph. D degree at the Information and Communication Engineering at Anna University, Chennai. Her research interests include denial-of-service attacks, jamming attacks, secure routing algorithm and security in networks.

Dr. R. Ravi is an Editor in International Journal of Security and its Applications (South Korea). He is presently working as a Professor & Head and Research Centre Head, Department of Computer Science and Engineering, Francis Xavier Engineering College, Tirunelveli. He completed his B.E in Computer Science and Engineering from Thiagarajar College of engineering, Madurai in the year 1994 and M.E in Computer Science and Engineering from Jadavpur Government research University, Kolkata. He has completed his Ph. D in Networks from Anna University Chennai. He has 19 years of experience in teaching as Professor and Head of department in various colleges. He published 25 International Journals. He is also a full time recognized guide for various Universities. Currently he is guiding 18 research scholars. His areas of interest are Virtual Private networks, Networks, Natural Language Processing and Cyber security.