A Novel Defence Scheme for Jamming Attack Prevention in Computer Networks

Miss. Nikita S. Bahaley[1], Dr. V. M. Thakare[2], Dr. S. S. Sherekar[3]

Abstract- **The shared nature of wireless network makes easy for an adversary to launch various attacks in the network. A malicious node can continually transmit a radio signal in order to block any legitimate access to the medium and/or interfere with reception. This act is called jamming and the malicious nodes are referred to as jammers. Jamming techniques vary from simple ones to more sophisticated. Wireless networking plays an important role in civil as well as military applications. It is critical to ensure that the data going through network is visible or accessible only to legitimate users and not to the intruders. Jamming and eavesdropping are the two basic attacks at the physical layer. Physical layer characteristics have been considered as potential alternative to provide security services in wireless networks. There are various non-cryptographic ways available which can be used for security of the wireless network. This paper presents a novel approach for the better performance of the network.**

Index Terms— **Jamming attacks, Denial of service, wireless network, selective jamming.**

I. INTRODUCTION

In any communication system, security is an important issue. At the present time, with the advances in technology, wireless networks are becoming more affordable and easier to build. Many metropolitan areas deploy public WMANs for people to use freely. However, wireless networks are accompanied with an important security flaw; they are much easier to attack than any wired network. It makes it extremely easy for an adversary to launch an attack. The goal of traditional DoS attacks is to overflow user and kernel domain buffers. However, in wireless networks there are many occasions where the attack can be much easier for an adversary. Brute-force jamming techniques, which mainly exploit PHY and MAC layer vulnerabilities, can be detected easily. The ability to share secret information reliably in the presence of adversaries is extremely important. Adversaries may attempt to launch various attacks to gain unauthorized access to and modify the information, or even disrupt the information flows. Because of the broadcast nature of the wireless medium, communication can easily be eavesdropped or intercepted. The wireless devices can be compromised and modified to behave maliciously or selfishly. These vulnerabilities in wireless networks could undermine the authenticity, confidentiality, integrity, and availability if they are not carefully addressed.

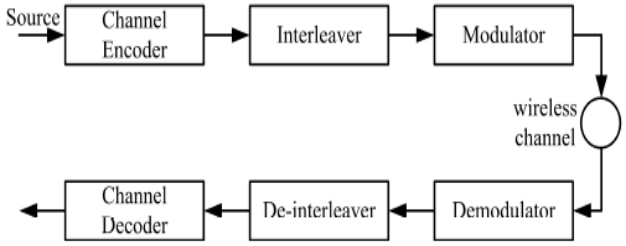

Fig 1: A generic communication system.

II. BACKGROUND

Brown proposed a system for jamming and sensing of encrypted wireless ad hoc networks. Pelechrinis proposed a system for detection selfish exploitation of carrier sensing in 802.11 networks. Aime proposed a wireless distributed intrusion detection system and a new attack model. Chatzigiannakis proposed data fission algorithms for network anomaly detection. The goal of traditional DoS attacks is to overflow user and kernel domain buffers [4]. However, in wireless networks there are many occasions where the attack can be much easier for adversary. Brute-force jamming techniques which mainly exploit PHY and MAC layer vulnerabilities can be detected easily. The basic jamming models that capture the strategy followed by the malicious attacker are: Constant jammer, Deceptive jammer, Random jammer and reactive jammer. Intelligent jamming models like layered model for jamming, intelligent jamming in IEEE 802.11 are also given. The various intrusion detection systems given by the methodology are PHY layer intrusion detection, detection of MAC layer DoS/ Misbehaviour. This methodology presents the detection as well as prevention techniques for the denial of service attacks in wireless networks [1].

Most commonly used security methods rely on cryptographic techniques employed at the upper layers of the wireless network. The existing physical layer security techniques can be classified in to five major categories as: theoretical secure capacity, and the power, code, channel and signal detection approaches. It was suggested that perfect secrecy is achievable using physical layer techniques subject to the condition that the channels are unknown to the unauthorized users or the channel of the unauthorized users is noisier than that of the authorized users. While the traditional encryption techniques rely heavily on the upper-layer operations. Most of the works focused on the study of secrecy capacity that is maximum rate achievable between the legitimate transmitter-receiver pair subject to constraints on information attainable by the unauthorized receiver. This methodology provides a tutorial on several existing prevalent methods to enhance security at the physical layer in wireless networks. Those methods are classified into five major categories based on their characteristic features.

Each of these methods is evaluated and compared in terms of two performance metrics that is their secret channel capacities and computational complexities [5]. In channel approaches, three methods have been proposed: radio frequency (RF) fingerprinting, algebraic channel decomposition multiplexing (ACDM) pre-coding, and randomization of MIMO transmission coefficients. In case of code approaches the main objective is to improve resilience jamming and eavesdropping. The code approaches include use of error correction coding and spread spectrum coding. Power approaches include the employment of directional antennas and the injection of artificial noise [2].

The existing lower/physical layer signature schemes can be broadly classified into three categories: software based, hardware based and channel/location based. Most of the schemes proposed in the literature are applicable only to static networks. Limited work has considered mobile scenarios. So here Non-Cryptographic authentication and identification methodology has reviewed the existing and ongoing research on non-Cryptographic authentication/ identification in both static and mobile wireless networks [10]. Also, two more RSS-based authentication systems have been proposed. The two RSS-based authentication systems are: RSS Similarity-Based authentication and Temporal RSS Variation authentication. In RSS similarity based authentication, in order to authenticate *n*th frame $DATA_n$, one person in communication compares its RSS with that if the $DATA_{n-1}$. If the difference is within a certain range, Bob assumes the signal comes from Alice. Otherwise, he generates alarm. When the time interval between two consecutive frames is larger than some threshold, or the sender has already moved to another location, the RSS of the received data becomes uncorrelated with the previous one. In such situation, Temporal RSS variation authentication is applied. This is motivated by the wireless channel reciprocity principle. This principle indicates that the channel state between two transceivers should be identical at any instant of time [3].

III. Previous Work Done

W. Xu proposed a system for defense strategies against attacks in sensor networks. Brown proposed a system for jamming and sensing of encrypted wireless ad hoc networks. Pelechrinis proposed a system for detection selfish exploitation of carrier sensing in 802.11 networks. Aime proposed a wireless distributed intrusion detection system and a new attack model. Chatzigiannakis proposed data fission algorithms for network anomaly detection [1]. Kshiti proposed a system for secure transmission with multiple antennas. Barros proposed a system for secrecy capacity of wireless channels. Li proposed a system for secret communication via multi-antenna transmission. Tomko proposed system for physical layer intrusion detection in wireless networks [2].

V. Brik proposed wireless device identification with radio metric signatures. L. Xiao proposed a physical layer technique to enhance authentication for mobile terminals. B. Danev proposed a system for identification of attacks on physical layer. J. Yang proposed a system for determining the number of attackers and localizing multiple adversaries in wireless spoofing attacks [3].

An introduction to the first wireless standard based upon CRNs is presented in the work by Cordeiro. The work demonstrated the prospect of CRN-based wireless communication by using the IEEE 802.22 WRAN technology. A detailed overview of the WRAN specifications, topology, service requirements, capacity, and applications were presented in the work. Most importantly, it specified the 802.22 system to comprise a fixed point-to-multipoint wireless air interface, in which a base station manages its own cell and all associated consumer premise equipment (CPE). It was an early time for considering any of the CRN security issues. Major security threats against CRN are PUE attacks, objective function attack and jamming attack [9].

This paper introduces various methods which can be used for preventing jamming attacks in the networks. **Section 1** Introduction. **Section 2** discusses Background. **Section 3** discusses Previous Work Done. **Section 4** discusses various methodologies. **Section 5** discusses attributes and parameters. **Section 6** proposed Method and possible outcome result. Finally **section 7** concludes this paper.

IV. Existing Methodologies

The various intrusion prevention scheme given by K. Pelechrinis are frequency hopping, spatial retreats, and fighting reservation based DoS attacks, security network from a layered jamming attack, PHY layer anti-jamming techniques, wormholes, and protocol mechanism hopping. Frequency hopping has been traditionally employed in order to overcome the presence of jammer. It can be either proactive or reactive. In reactive case, when a node detects that it is jammed it switches to a different channel and sends a beacon message on the new channel, announcing its presence. Its non-jammed neighbours will sense its absence and will change their bands of operation to check if their lost neighbour has sent beacons announcing its presence on a different channel. If not, they assume that the node just move away. In case of proactive hopping, a proactive frequency hopping protocol with pseudo-random channel switching is used [1].

This methodology given by Yi-sheng Shiu presents a tutorial on several existing prevalent methods to enhance security at the physical layer in wireless networks. Those methods are classified into five major categories base on their characteristic features. The various physical layer security approaches are theoretical secure capacity, channel, and coding, power and signal detection. In channel approaches, three methods have been proposed: radio frequency (RF) fingerprinting, algebraic channel decomposition multiplexing (ACDM) pre-coding, and randomization of MIMO transmission coefficients. In case of code approaches the main objective is to improve resilience jamming and eavesdropping. The code approaches include use of error correction coding and spread spectrum coding. Power approaches include the employment of directional antennas and the injection of artificial noise [2].

Non-Cryptographic authentication and identification methodology has reviewed the existing and ongoing research on Non-Cryptographic authentication/identification in both static and mobile wireless networks. In addition two RSS-based authentication schemes in mobile networks are proposed. Non-Cryptographic wireless user authentication and device identification consist of: Software-based fingerprinting, hardware-based fingerprinting and channel/location-based fingerprinting [6]. Each of these has their own merits and

demerits. Software-based mechanism consists of MAC behavior, frame sequence number, traffic pattern. Hardware-based consist of clock skew, physical unclonable function, radiometric identification. Channel/location basic mechanism consists of channel state information, signal strength. The two RSS-based authentication systems, proposed here are: RSS Similarity-Based authentication and Temporal RSS Variation authentication. In RSS similarity based authentication, in order to authenticate *n*th frame $DATA_n$, one person in communication compares its RSS with that if the $DATA_{n-1}$. If the difference is within a certain range, Bob assumes the signal comes from authenticate user. Otherwise, he generates alarm. When the time interval between two consecutive frames is larger than some threshold, or the sender has already moved to another location, the RSS of the received data becomes uncorrelated with the previous one. In such situation, Temporal RSS variation authentication is applied. This is motivated by the wireless channel reciprocity principle. This principle indicates that the channel state between two transceivers should be identical at any instant of time [3].

V. ANALYSIS AND DISCUSSION

K. Pelechrinis has suggested to use proactive frequency hopping protocol with pseudo-random channel switching by Navda. For this, there is need to compute the optimal frequency hopping parameters, assuming that the jammer is aware of the frequency hopping procedure that is followed. This scheme can retain up to 60% of the throughput, under benign conditions. A jammer exploiting vulnerability, can cause a significant number of packets to be corrupted with even a 1000 times weaker signal than that of the legitimate transceivers [1]. There are some advantages of this methodology as follows: throughput can be retained up to 60% of the throughput achieved under benign conditions. Also, there is no significant degradation when there is no jammer. Also it has a disadvantage that this system can retain only 60% throughput which can be improved.

Full channel state information (CSI) is considered where the transmitter has access to the channel gains of the legitimate receiver and the eavesdropper. The secrecy capacity under this full CSI assumption is adopted as an upper bound for the secrecy capacity when only the CSI of the legitimate receiver is known at the transmitter. A low-complexity on/off power allocation strategy that achieves near optical performance with only the main channel CSI can also be used [7]. The channel fading has the positive impact on secrecy capacity and rate adaptation based on channel CSI. Based on an information-theoretic formulation of the problem, in which two legitimate partners communicate over a quasi-static fading channel and an eavesdropper observes their transmissions through a second independent quasi-static fading channel, the important role of fading was characterized in terms of the average secure communication rates and outage probability. A secure communication protocol that adopts the following four step procedure to ensure wireless information-theoretic security: common randomness via opportunistic transmission, message reconciliation, common key generation via privacy amplification and message protection with a secrecy key. Finally, a set of security measures for assessing average secure key generation rates was established and it was shown that the protocol is effective in secure key renewal even in presence of imperfect CSI. The use of multiple antennas has drawn a lot of attention in wireless communication research [2]. The advantages of this system are: By using this system message can be protected by using secret key and this system is effective in secure key renewal even in the presence of imperfect CSI. If jamming is detected, transmitting nodes switch to a PN code known only to a subset of nodes. The compromised node is uniquely identified in a number of a step that is logarithmic to the number of nodes within a cluster [8].
The two schemes proposed here by Kai Zeng are: RSS similarity-based authentication and temporal RSS variation authentication. In RSS similarity based authentication (SA), in order to authenticate n^{th} frame $DATA_n$ legitimate user compares its RSS with that of the $DATA_{n-1}$. If difference is within a range, user assumes the signal comes from another legitimate user. Otherwise he generates an alarm. When the time interval between two consecutive frames is larger than some threshold, or the sender has already moved to another location, the RSS of the received data becomes uncorrelated with previous one. In such situation, Temporal RSS variation authentication is applied. It has an advantage that non-Cryptographic authentication and identification schemes can be used to augment or enhance existing cryptography-based mechanisms. Also, this scheme exploits the inherent defects/characteristics of the devices or wireless channel to extract fingerprints. This system has a disadvantage that although these schemes can be used to detect, identify spoofing attacks or authenticate/identify a particular user, they cannot achieve a 100 percent detection rate without introducing false alarms [3].

VI. PROPOSED METHODOLOGY

Various systems are available which detects and prevents the jamming attack in networks. They are not able to achieve maximum throughput as well as to maintain the energy in the network. So with the help of the proposed methodology throughput can be improved with less or no delay. Also the energy in the network can be maintained. The proposed methodology is consists of Network Formation, Jamming attack creation, Jamming attack prevention, Result evaluation and System optimization. Proposed methodology uses network simulator 2 for simulation.
Network Formation module will create the network with some nodes. After network formation, with the help of a node in the network, jamming attack will be created. Later, in jamming attack prevention scheme, the jamming attack prevention algorithm will be applied, which will first detect the malicious node in the network and then it will prevent that particular malicious node from sending or receiving the packets in the network. Result evaluation will show the graphs for various parameters like delay, energy and throughput. If in case some parameters need to change then system optimization would be used for that purpose.

The diagram below shows the various steps in jamming attack prevention scheme.

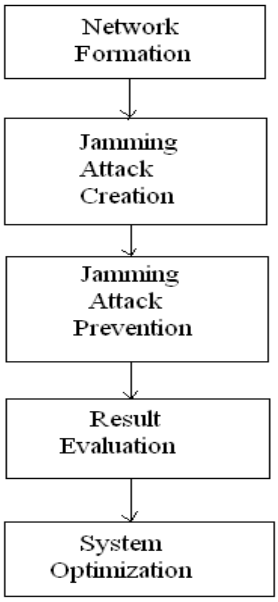

Fig. 2: Steps for jamming attack prevention

VII. Possible Outcomes And Result

Better results can be obtained in terms of parameters like reducing the delay, achieving maximum throughput with high energy. The throughput can be achieved up to 80% or may be larger than that in some cases. An individual can work in more secure networking environment.

VIII. Conclusion

This paper addresses the problem of jamming attacks in the computer network. A novel approach for the jamming attack prevention is given here in this paper. Better results can be obtained in terms of energy, throughput by using this methodology. Also, delay in the communication can be reduced to a greater extent.

IX. Future Scope

For prevention of various attacks rather than Denial of Service only, cross layer security can be designed.

References

[1] K. Pelechrinis, M. Iliofotou and S. V. Krishnamurthy, "Denial of Service attacks in wireless networks: The Case of Jammers", IEEE communication surveys and tutorials, 1553-877X, VOL. 13, NO. 2, pp. 245-257, Aug 2011.
[2] Yi sheng shiu, Shih Yu Chang and Hsiao-Chun Wu "Physical layer security in wireless networks: A tutorial," IEEE wireless communications, 1536-1284, VOL. 18, NO.2, pp. 66-74, April 2011.
[3] Kai Zeng, Kannan Govindan and Prasant Mohapatra, "Non-cryptographic authentication and identification in wireless networks", IEEE wireless Communications , 1536-1284, Vol. 17, No. 5, pp. 56-62, Oct 2010.
[4] Alejandro Proano and Loukas Lazos, "Packet hiding methods for preventing selective jamming attacks", IEEE Transactions On Dependable And Secure Computing, 1545-5971, VOL. 9, NO. 1, pp. 101-114, Jan-Feb 2012.
[5] Faheem Fayyaz and Hamza Rasheed, "Using JPCAP to prevent man-in-the-middle attacks in a local area network environment", IEEE potentials, 0278-6648, VOL. 31, NO. 4, pp. 35-37, July-Aug 2012.
[6] Ashish Kumar, Sachin Kumar Gupta and Shubham Singh, "Packet hiding methods for preventing selective jamming attacks", International Journal Of Computational Engineering Research, 2250-3005, Vol. 3, No. 1, PP. 148-153, Jan 2013.
[7] Ali Hamieh, Jalel Ben-Othman, "Detection of jamming attacks in wireless Ad hoc networks using error distribution", IEEE communications, Dresden, pp. 1-6, 14-18 June 2009.
[8] L. Lazos and M. Krunz, "Selective jamming/dropping insider attacks in wireless mesh networks," IEEE network, 0890-8044, VOL. 25, NO.1, pp. 30-34, Jan/Feb 2011.
[9] K. Gill, S. H. Yang and W. Wang, "Scheme for preventing low-level denial-of-service attacks on wireless sensor network-based home automation systems", IET wireless systems , 2043-6386, Vol. 2, No. 4, pp. 361-368, Dec 2012.
[10] Z. M. Fadlullah, H. Nishiyama, N. Kato and M. M. Fouda, "Intrusion detection system for combating attacks against cognitive radio networks", IEEE network, 0890-8044, Vol. 27, No. 3, pp. 51-56, May/June 2013.