International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 4 Issue 6, September-October 2020 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Jamming Attacks, Prevention and Detection

Ms. Pinki R. Jha[1], Prof. Shambhu Rai[2]

[1]Student, [2]Asistant Professor,

[1,2]Bharati Vidyapeeth's Institute of Management and Information Technology, Navi Mumbai, Maharashtra, India

ABSTRACT

The open nature of the wireless medium renders it weak to intentional inference attacks, typically known as jamming. Jamming attack is considered as a serious threat to the wireless communications. Reactive jamming amplifies the attack potency by jamming only when the targets are communicating, which can be easily implemented using software defined radio. The intentional intervention with wireless transmission can be used as a launch pad for increasing Denial-of-Service attacks on wireless networks. Jamming is well-known reliability threat for mass-market wireless networks. With the increase in safety-critical systems this will be possible to become a constraining issue in the future. Thus, the design of accurate jamming detection algorithms becomes critical to react to existing jamming attacks. With regards to experimental work, jamming detection has been mainly examined for sensor networks. Generally, jamming has been addressed as external threat model. However, adversary with internal knowledge of protocol condition and network secret can start low – effort jamming attacks that are hard to detect and counter. In this paper we discuss various methods of detecting the jamming attacks and methods to prevent them.

KEYWORDS: *Jamming; Attacks; Collision; Signal Strength; Packet Delivery Ratio*

How to cite this paper: Ms. Pinki R. Jha | Prof. Shambhu Rai "Jamming Attacks, Prevention and Detection" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-4 | Issue-6, October 2020, pp.89-92, URL: www.ijtsrd.com/papers/ijtsrd33214.pdf

IJTSRD33214

I. INTRODUCTION

Wireless networks are used for transmitting information of any kind between two or more nodes that are not physically connected. Wireless networks are vulnerable to various kinds of attacks because of its shared medium. It is needed to deal with numerous security issues. Attackers with a transceiver are able to interrupt wireless transmission, insert unwanted messages, or jam messages of high significance. Jamming can be considered as one of elemental ways of degrading network performance [1, 6]. Usually, jamming can be done in two forms. One is external threat model in which jammer will not be the part of network. Other one is internal threat model in which jammer will be part of network. In this paper, we will focus on external threat model where jammer with some confidential information about internal network can introduce jamming attacks.

In this paper, network model is considered where nodes are communicating with each other and there attack node also exist, which will jam messages going through network. As we are considering that jammer is using external threat model and jammer will not be a part of the network but jammer is aware of all the implementation details of network protocols. By using this knowledge, jammer targets the packets of high priority [1, 3 and 6].

II. LITERATURE REVIEW

There has been lot of research and development going on in this topic of wireless security, lots of articles, books, research and research papers have been published already. After reading handful of papers we have come to notice that there are various methods and techniques developed. First and foremost step is to identify the jamming attack which is the difficult part of that because if anyone is unaware that attack happening then, it is tough to avoid.

The steganography talks about security related to the data that travels from one node to another, which is new technique to hide the data inside images. The method is designed to hide all the data entered within the image to protect the secrecy of the data. This system provides an image platform for user to input image and a text box to insert texts. Steganography Imaging System (SIS) is a system that is capable of hiding the data inside the image [2].

Detecting jamming attacks is crucial because it is the first step towards creating a secure and dependable wireless network. It is challenging because jammers can employ different models, and it is often tough to differentiate a jamming scenario from legitimate scenarios, we need to differentiate a jamming scenario from various network conditions congestions that occur when the aggregated track load exceeds the network capacity so that the packet send ratio and delivery ratio are affected. Detection can be done by various methods like signal strength, carrier sensing time, packet delivery ratio [1].

Piggyback is a technique for the security of the data with the sequence ID and with the host name. Along with the piggybacking we also maintain a strong hiding scheme that

provides the packet from loss and stored in the buffer. The congestion control is mentioned in this paper by following the sequential number ID of the packets. In the wireless network, the confidentiality of the data is more crucial aspect and is mentioned in this paper by piggybacking the packets without loss. The RSA algorithm is used for the encryption and decryption purpose. The encrypted data will then be piggybacked by which the data is hidden and then moved to the destinations. Through this the congestion on the network can be controlled [3].

The analysis showed that collisions due to jamming attacks are not different from collisions due to hidden terminal and/or network congestion. To improve the detection accuracy, we utilized the channel utilization metric to evaluate network congestion state and then performed tests to classify whether collision is due to jamming or network traffic conditions. Evaluated effectiveness of the scheme through simulations and demonstrated that is can be used to detect attacks with enhanced reliability and accuracy [4].

WSNs are a rapidly growing field, with many opportunities and challenging. Strict architectural, economic and technological aspects of such networks give it its unique characteristics and traits. As more dependent we grow on WSN's, we cannot afford to compromise the availability and security of such networks. Since WSN hardware and software have many limitations, it allowed security issues to rise to the surface. In this paper, we have discussed the jamming attacks and sinkhole attacks. We discussed their main aspects and types, and how attackers utilize such techniques to launch their attacks. We have discussed through two major papers those pro-posed techniques to defend against jamming attacks [5].

III. METHODOLOGY

A. Collision Monitoring Process

Traditional detection mechanisms in wired networks consist of monitoring the network layer to analyze packet level transmissions. In wireless networks, such schemes cannot be used to detect DOS attacks such as jamming that occur at lower layers. In such cases it is necessary to monitor the wireless channel transmissions. Due to the broadcast nature of wireless channel, communication between nodes can be overheard by all points in their transmission range. We make use of this feature to our advantage and engage channel monitoring mechanism to detect collisions in wireless networks [3].

B. Congestion Estimation using Channel Utilization

In this, the cross-layer measurement of channel utilization to determine collisions due to network congestion. The possibility of packet loss due to hidden terminal collisions is a function of traffic load at the hidden terminal node. Heavy traffic load in the node's transmission or interference range can result in a congested network leading to packet collisions. Several metrics such as queue length, packet delivery ratio and throughput have been used to measure network congestion. Hence, congestion can be better characterized based on the amount of time the channel is utilized or reserved by nodes for transmission [3].

1. **Channel Busy Time:** Channel Busy Time is defined as the fraction of time interval during which the wireless channel is busy or occupied. Channel Busy Time measurement includes the time spent in packet transmission, reception and inter frame spacing delays preceding the transmission of control and data frames in wireless network [3].
2. **Channel Utilization:** Channel utilization in wireless networks is computed by adding the total time spent on transmission of all data and control frames, as governed by the Channel Busy Time. We define channel utilization as the fraction of time the channel is busy over the total duration [3].

C. Collision Detection

In this collision detection, we present the two phase detection mechanism employed at the monitor nodes to detect jamming attacks. We describe the detection mechanisms in detail below [3].

1. **Phase I Detection –** *Using passive monitoring:* In this Phase its monitors conducts preliminary tests to detect collision occurrences in the wireless channel [3].
2. **Phase II Detection-** *Using cross-layer measurement*: In Phase II detection, we address the challenge of differentiating the collisions in network occurred either due to jamming attacks or congested conditions. In this work, we propose a cross-layer based measurement driven approach where congestion estimation using physical, MAC and network layer measurements is used to identify collisions. The monitor runs jamming tests as well as evaluates the congestion status of the channel [3].

D. Detection of Jamming Attacks

1. **Signal Strength:** One natural measurement to detect jamming is signal strength, or ambient energy. Using this measurement is that the signal strength distribution is affected by the presence of jammer. By gathering enough amplitude measurements throughout a time period prior to jamming, network devices build statistical model that describe normal energy levels in the network.
2. **Basic Average and Energy Detection:** We can have two statistics from signal strength readings, they are, the average signal strength and the energy for detection. In both cases, the statistical hypothesis testing problem is binary and essentially involves deciding between signal absent and signal present hypothesis [1].
3. **Carrier Sensing Time:** A jammer can prevent a legitimate source from sending out packets because the channel might appear constantly busy to the source. In this case, it is very natural for one to keep track of the amount of time it spends waiting for the channel to become idle, i.e. the carrier sensing time, and compare it with the sensing time during normal track operations to determine whether it is jammed [1].
4. **Packet Delivery Ratio:** Jammer may not only prevent a wireless node from sending out packets, but can also corrupt a packet during transmission. As a result, we next evaluate the feasibility of using packet delivery ratio (PDR) as the means of detecting the presence of jamming. The packet delivery ratio can be measured by the sender as well as by receiver. At the sender side, the PDR can be calculated by keeping track of how many acknowledgements it receives from the receiver [1].

5. **Signal Strength Consistency Checks:** In this, we employ measurements of the PDR between a node and each of its neighbors. In order to combat false detections due to legitimate causes of link degradation, we use the signal strength as a consistency check. Specially, we check to see whether a low PDR value is consistent with the signal strength that is measured. If there are no interference or software faults, a high signal strength will corresponds to a high PDR [1].
6. **Piggybacking:** At the decryption end, the data in huge volume will be loss due to congestions. But by piggybacking the packets alongside the header and sequence ID and also the host name the information will be send directly to the selected host. Hence, the data will be buffered and after that process the data will be sent to all the clients that are alive on the network. Thus the piggybacking techniques the data will be directly sent to the client network, after the acknowledgement is received. The TCP protocol is responsible for the processing [4].

E. Defending against Jamming Attacks using Packet Hiding

1. **Strong Hiding Commitment Scheme (SHCS):** This is based on the symmetric cryptography method. Main motive is to satisfy the strong hiding property while keeping the computation and the communication overhead to a minimum. The proposed SHCS requires the point consideration of the MAC and PHY layers. To reduce the overhead the de-commitment value or the decryption key value is done in the same packet in which the encryption is taken place.
2. **Encryption of Data:** The data is encrypted by using the RSA algorithm. It is the public key algorithm that uses huge prime numbers in their factoring and their multiples as the code or key to encode the data given. Since the key size is large the intruders won't be easily able to hack the data. Through this RSA algorithm the data will be more secure. Cryptography is the process of transforming information (plain text / image) into incomprehensible form (Cipher text / Cipher image). The technology of encryption is called cryptology. The RSA algorithm is used to encrypt and decrypt the text, because it is considered as a better solution for encryption. In cryptography, RSA is an algorithm for public key cryptography. The RSA algorithm involves the use of two keys, a public key, which may be known to anybody and can be used to encrypt messages, a private key, known only by the recipient and used to decrypt messages [4, 5].
3. **Cryptographic Puzzle Hiding Scheme:** A sender sends a packet for transmission. Sender selects random key of desired length. Sender generates a puzzle (key and time), where puzzle denotes the function generator and it denotes the time required for solving the puzzle. After generating the puzzle, the sender broadcast the (C, P). At receiver side the receiver solve the puzzle to recover key and then computes the sender message [4, 5].
4. **All or Nothing Transformation:** The packets are pre-processed before transmission but are unencrypted. The jammer cannot perform packet classification till all pseudo message corresponding to original packet are received and inverse transformation have been applied [4, 5].

F. Prevention Techniques for Jamming Attacks

1. **Honeypots:** Honeypots are basically a great security measure which is used to fool attacker present in network. While deploying in a network, honeypot try to gain attention of attackers. Honeypots trap the attackers in a way that attacker attacks on honeypot by thinking that it is the important part of network and at the same time honeypot collects all the information about attacker such as attacking strategy, purpose and techniques. In this section, an approach is provided which will use honeypots to provide an efficient solution to jamming attacks. Architecture for Implementing HONEYPOTS consists of Base-station, Mobile nodes and Honeynodes (nodes where honeypots are deployed)

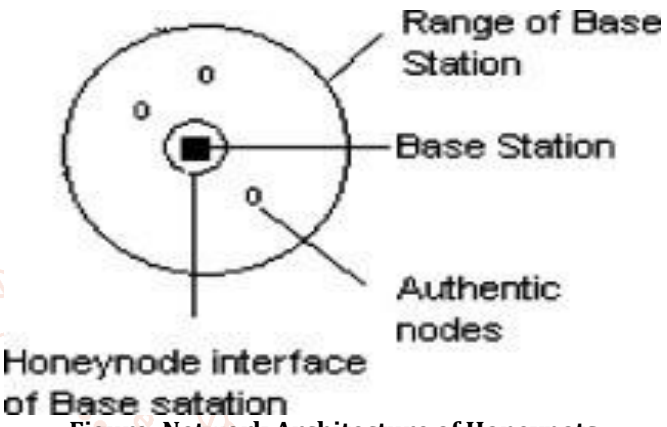

Figure: Network Architecture of Honeypots [Source adapted from [6]]

1. **Process:** In this process, if attack is detected then it checks for if, node is a honey node, then it informs base station of the attack and continues communication to deceive the jammer and change frequency of operation. If node is a base station then checks if honey node has informed of the attack then select frequency to jump using dynamic selection and inform associated node to switch to this frequency or else find the node that did not respond and if any node did not respond then broadcast frequency change command and change frequency of operation [6].
2. **Steganography:** In cryptography the protection of messages from being captured by non-legitimate entity is achieved using steganography. This technique depicts, the fact that a message is being sent, and, if not detected make the sender and receiver invisible. Thus, steganography provides not only security, but also anonymity and security during transmission process. Steganography techniques make the use of digital data such as audio, video, image, etc. to hide secret message [2].

IV. RESEARCH FINDINGS

By going through these papers, this methodology can be used for the future in detecting the jamming attacks in various fields where lots of data is transferred continuously. With the help of this we can secure the communication medium up to some extent. This concept can help us and give a prior intuition of the attacks by which we can detect as well as prevent jamming attacks. Many data center can also be benefited, as they store huge amount of data in their storage. While transferring the message or important documents we can also make use of the steganography as discussed above. Another interesting issue is to find alternatives for modelling

lack of knowledge for the attacker and the network. An idea would be to average over all strategies of the opponent. More enhanced versions of attacks can be considered, such as the one with dynamic control of jamming probability to extend detection time likewise, the network can adapt channel access probability. Finally the issue of multiple, potentially co-operating attackers give a whole new flavor to these problems and is worth further attention.

V. CONCLUSION

In this paper, researcher found that there are various jamming attacks and detection model in wireless networks. Different real-time packet classification is reviewed that are used to classify the packet before reaching at destination. Diverse prevention techniques based on cryptanalysis and steganography are used to reduce jamming attacks. Honey pot is another technique that has been used to reduce the effect of jamming as well as it uses some algorithm to fool jammer and decrease jamming rate. The conclusion is that there are various methods of prevention and detection of jamming attacks but, none can be 100% solution for the attacks. Still by using this methodology we can go one level up for preventing and detecting jamming attacks.

REFERENCES

[1] W. Xu, W. Trappe, Y. Zhang. The Feasibility of Launching and Detecting jamming attacks in Wireless Networks. In proceedings of MobiHoc, 2005.

[2] R. Ibrahim and Teoh Suk Kuan. "Steganography Algorithm to hide secret message inside an Image". Computer application and technology, February 2011.

[3] G. Thamilarasu, S. Mishra and R. Sridhar. "Improving reliability of Jamming Attack Detection in Ad-hoc Networks". In proceedings of IJCNIS, April 2011.

[4] N. Kavitha, A. Arun Joseph. "Piggybacking Method Combined With SHCS Technique for Spot Jamming Attacks in Wireless Networks". September 2013.

[5] Archana Patil, Prof. S. P. Pingat. "International Journal of Advanced Research in Computer Science and Software Engineering". June 2014.

[6] Neha Thakur, ArunaSankaralingam. "Introduction to Jamming Attacks and Prevention Techniques using Honey pots in Wireless Networks". In IRACST, April 2013.