ISSN: 2277-9655
Impact Factor: 1.852

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

A Survey on the Defense Mechanisms of Jamming Attacks in Wireless Networks

T.Ramesh[*1], S.S.Meenatchi[2]
meenuvanu@gmail.com

Abstract

Wireless Networks is the most vital and emerging technology. It contains lots of sensor nodes comprised in it. This provides us global and local views. It has a numerous potential applications like Residence, Military, Industry, Environmental monitoring and many more. As it is ad-hoc in nature it is subjected to several security threats. This paper defines Jamming attack and focuses on various defense mechanisms of Jamming attack in Wireless Networks.

Keywords: Jamming attack, Wireless Networks.

Introduction

Wireless Networks is a rapidly growing technology, which provides lot of opportunities. At first Wireless Networks was only used in military purposes but nowadays we are using it in most of our day to day things. Wireless Networks suffer from so many constraints such as energy efficiency, several security breaches, limited memory power, limited processing speed and many more. Among these constraint security is a major concern. Securing a Wireless Network from several attacks is not an easier job, as the security breaches are diverse. This paper focuses on an important attack in the Physical layer and in the MAC sub layer, which is jamming attack. One of the fundamental ways to degrade a network performance is achieved by jamming attack. The remainder of this paper is organized as follows: Section 2 focus on Security Threat categories of Wireless Networks. Section 3 focuses on Physical, MAC Layer and its Security threats. Section 4 defines Jamming attack and its types. Section 5 focuses on the Several Defense mechanisms, of various Jamming Attacks. Finally all the discussions are summed up in section 6.

Security Threat Catagories

Unlike Wired Networks, Wireless Network is not reliable so it is subjected to several security threats. Attacks on the wireless networks are classified as:

- Interruption – It can halt a node or any process can be stopped abruptly for that matter.
- Interception – This is an attack which is based on the confidentiality. The Node can be comprised by the attacker and gain un-authorized access.
- Modification – This is an attack based on candor. By gaining the unauthorized access from the node it modifies the data present in it.
- Fabrication – This is an attack authentication. It modifies the data present in the nodes and creates compromises the trustiness of the information relayed [1].
- Spoofing - This is an attempt to gain access of a system using false identity. This can be achieved by using stolen user credentials or a false IP address. After the hacker successfully gains access as a legitimate user, unauthorized access begins.
- Repudiation - This is the ability of users to deny the performed specific actions. Without adequate monitoring, repudiation attacks are difficult to identify.
- Information disclosure - This is the unwanted exposure of private data. An authorized file is being displayed to unauthorized users.
- Denial of service – This is making a network services unavailable to a legitimate users.
- Elevation of privilege – This is making limited privilege users to gain control on highly privileged account [2].

Physical Layer, MAC Layer and Its Security Threats

Physical Layer is the first layer of the OSI Model. The physical layer consists of the basic networking hardware transmission technologies in a network. It is the lowest layer nevertheless very complexedone. It transmits raw bits.The bit stream is combined into code words or any symbols and converted as signals.

The physical layer has 5 major responsibilities they are [5]:

- Frequency selection
- Carrier frequency generation
- Signal detection
- Modulation
- Data encryption.

The functions and services performed by the physical layer are:

- Bit-by-bit delivery
- Providing a standardized interface
- Modulation
- Line coding
- Bit synchronization
- Signaling
- Flow control
- Circuit switching
- Multiplexing
- Carrier sense
- Collision detection
- Forward error correction
- Bit-interleaving and
- Channel coding
- Bit rate
- Point-to-point, multipoint or point-to-multipoint line configuration
- Physical network topology
- Serial or parallel communication
- Transmission mode
- Autonegotiation

The Physical layer is subjected to several security threats they are

PHYSICAL LAYER	ATTACKS
	Sniffing (Or) Eaves Dropping
	Spoofing
	Tampering
	Jamming

Table-1: Physical layer Attacks

MAC Layer is the sub Layer of the Data Link Layer (DLL).DLL is the Second Layer of the OSI Model. Every System has a unique MAC address. This Layer is responsible for sharing physical connection to the network among several nodes. It uses MAC Protocols to ensure a signal sent from a system does not collide with the other. Different Protocols are used for different layers.

- TheMAC Layer has two primary responsibilities they are:
  1) Data Encapsulation with frame assembly before transmission.
  2) Error Detection during or after Transmission.
- The MAC sub-layer provides two services they are:
  1) The MAC data service – This enables the transmission and reception of MAC protocol data units(MPDUs) across the Physical data service.
  2) The MAC management service – This interfaces to the MAC sub-layer management entity (MLME) service access point (SAP) (MLME-SAP).

- The peculiarities of the MAC sub-layer are:
  1) Beacon management.
  2) Channel access.
  3) GTS management.
  4) Framevalidation.
  5) Acknowledged frame delivery.
  6) Association.
  7) Disassociation.
  8) Provides hooks for implementing application-appropriate security mechanisms [3].

All the layers of the OSI model are subject to several vulnerabilities. This paper focuses on MAC Layer's Security issues. Someof the attacks are listed below:

MAC SUB-LAYER	ATTACKS
	1. JAMMING
	2. SCRAMBLING
	3. MASQUERADING
	4. DATA TRAFFIC MODIFICATION
	5. DOS

Table-2: MAC Sub-layer Attacks

Jamming Attack and Its Types

The fundamental way to degrade a network performance is achieved by jamming. It is achieved by overhearing the first few bits of a packet or any classification of transmissions based on the Protocol semantics. These attacks can easily be accomplished by an adversary by intruding MAC-layer protocols or emitting a radio signal targeted at jamming in a specific channel. The jammer controls the probability of jamming and transmission range to cause maximal damage to the network in the way of corrupted communication links.

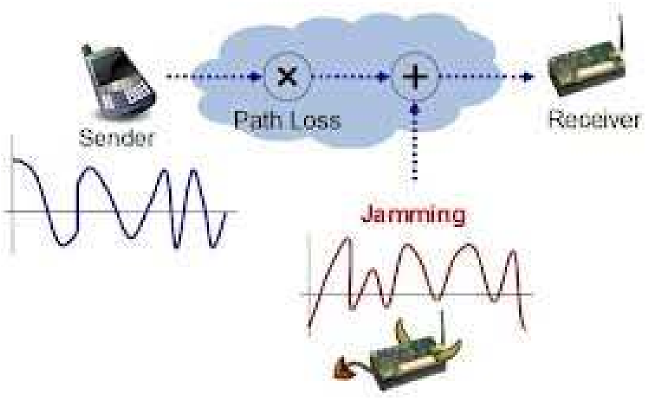

Fig-1:Jammer

Wireless Networks is subjected to several attacks. One of the major issues is Jamming Attack. The jamming attack is classified broadly into types they are:

1) Internal Jamming Attack and
2) External Jamming Attack.

External jamming can be prevented easily when compared to internal attack. The internal attack is classified into a type called Selective Jamming. This is unable to find that much easier. The jammer decides where the attack should happen.The External Jamming is classified into four types [4]. They are:

- **Constant Jammer**– This emits aradio signal continuously by implementing a waveformgenerator that continuously sends a radio signal or a normalwireless device that continuously sends out random bits tothe channel without following any MAC-layer decorum. Usually, the underlying MAC protocol allows legitimatenodes to send out packets only if the channel is idle. So a constant jammer can effectively prevent legitimate trafficsources from getting hold of a channel and sending packets.
- **Deceptive Jammer** – Instead of sending random bits, the deceptive jammer constantly injects regular packets to the channel without any gap between subsequent packet transmissions. So a normal communicator will be deceived into believing that there is a legitimate packet and be duped to remain in the receiving state. Even if a node has packets to send, it cannot switch to the sending state because a constant stream of incoming packets will be detected.
- **Random Jammer** – Instead of continuously sending out a radio signal, a random jammer switches between sleeping and jamming. Especially, after jamming for sometime it turns off its radio and enters a sleeping mode. It will reinstitute jamming after sleeping for some time. During jamming phase,it can behave like a constant jammer or a deceptivejammer. This jammer model is much concerned about energy efficiency, which is more important for a jammer as it does not have an unlimited power supply.
- **Reactive jammer** – The above three models are active jammers, this is a reactive model. This method is hard to detect. Active jammers are easier to detect as they always keep the channel engaged. Whereas reactive method keeps idle when channel is idle.

Defence Mechanisms of Various Jamming Attack

A Jammer blocks or gives Denial of Services to the legitimate users.Jamming attack is one of the vulnerability in MAC Layer. The Jammers are prevented using several techniques some of the techniques are as follows:

Using Honey Nodes for Defense against Jamming Attacks

Jamming attacks cause frequent noise and signal interferences which lead to congestion in network [6]. In this approach, a pre-emptive detection strategy using honey nodes and a response mechanism based on the existing Channel Surfing Algorithm to protect wireless nodes from a jammer is being proposed. In both Physical layer and MAC Layer a Jamming attack can occur. This paper focuses on both Physical Layer and MAC Layer jamming. Most of the Approaches have problems in attack detection, because most of the time the attacks detected generates false alarms. This is because network congestion is sometimes misunderstood as DOS. To get rid of this problem, in this approach a Honey node is introduced.

A Honey node is secondary interface present in the base station. It guards the nodes from attacks by creating a fake frequency range near by the actual interface. And also it deceives the attacking entity to the honey node so that the actual node gets time to switch to the new frequency.When a honey node is under attack, other nodes function properly.As they are operate in a separatefrequency. As soon as the honey node detects an attack, it alerts the base-station. On reception of this alert, the base-station selects a frequency using the reactive channel selection algorithm and alerts all its associated nodes to jump to that frequency. In this scenario, normal communication is not disrupted as the access point and all mobile nodes switch their frequency synchronously.

This method is a cost efficient and easily adaptable to the existing network architecture. Even when the attacker performance is low, the algorithm gives high performance in detection of jamming.

Using Alibi Framework for Defense against Insider Based Jamming Attack

Insider based jammer is a jamming technique which has knowledge about the frequency hopping pattern [7]. To identify this kind of jammer this method is being proposed. ALIBI means it is a form of defense whereby a defendant attempts to prove that he or she was elsewhere when the crime inquestion was committed. This is not a process of detection. Detection means there a jamming prevails whereas identification means finds the jammer.In the context of jamming attacks,honest nodes try to obtain alibis showing that they did legitimate actions observed by some witnesses while thejamming action took place. From this concept ALIBI frame work is developed.

In this approach, the defendant cannot claim an alibi by himself. So other nodes should be the witness, this is to create a trustworthiness. Here 2 alibi nodes are present one is S-alibi and R-alibi. S-alibi is referred as sending based alibi this sends an uncorrupted packet over one wholetime slot in one channel at a time the jamming actiontook place in another channel it is also observed by several otherwitnesses. So that a jammer cannot jamone channel and send an uncorrupted packet of one time slotin another channel simultaneously.

R-alibi is referred asareceiving basedalibi; this shows thatthe defendant was receiving a jammed packet, by showinga packet content that matches with the packet content received by other witnesses.So that node cannot send and receive a packet simultaneously.

Using these two alibis a normal node gets alibi to prove that they are not faulty. Whereas the faulty nodes does not gets alibi. Thus we can identify insider based jamming attack. This alibi framework works in various challenging scenarios such as lossychannels, non-colluding multiple attackers, and colluding multipleattackers.

Using Delaying Real Time Packet Classification Method for Defense against Selective Insider Jamming Attack

The jammer has the ability to classify the transmitted packets in real time by decoding the first few symbols of an ongoing transmission [8]. The attacker can easily launch internal attacks with data alteration, message dropping, selective forwarding, jamming, etc. The insider attackers are severely destructive to the functioning of a network. As the jammer is from within the network, jammer has access to shared cryptographic keys, aware of protocol semantics and the network topologies. It may be equipped with advanced hardware like multiple radios, multiple directional antennas and high computational power. The adversary can launch a denial of service attack from within the network. Moreover, the adversary is not only insider but also selective.

Attacker With internal knowledge, targets a specific message of high importance. A message which exceeds the threshold limit of a header size is the important packet. Those packets are the targets of the selective insider jammer. These packets are encoded and sent to the destination that alone is not enough. In order to secure it this approach uses Cryptographic puzzle which has to be solved within a timeslot by the receiver to get the key and decrypt the message.

This method delays the packet classification as the jammer will take considerable time to solve the puzzle, get the key, decrypt the message and then read the header information to classify the packet.

Conclusion

A wireless network is subjected to several security adversaries .Jamming attack is a crucial one, in the Physical Layer and MAC-Sub layer. In this paper first we have discussed the Security threat categories, Jamming and the existing methods to detect the Jamming attack in Wireless Networks.

References

[1] AnithaS Sastry, ShaziaSulthana, Dr. S Vagdevi, “*Security Threats in Wireless Sensor Networks in Each Layer*”, Int. J. Advanced Networking and ApplicationsVolume: 04 Issue: 04 Pages:1657-1661 (2013) ISSN : 0975-0290

[2] J.D. Meier, Alex Mackman, Michael Dunner, SrinathVasireddy, Ray Escamilla and AnandhaMurukan, ” *Improving Web Application Security: Threats and Countermeasures*” Microsoft Corporation, Published: June 2003 Last Revised: January 2006.

[3] “*WIRELESS MAC AND PHY SPECIFICATIONS FOR LR-WPANS*” IEEE Std 802.15.4-2006.

[4] WenyuanXu, Wade Trappe, Yanyong Zhang,” *Jamming Sensor Networks: Attack and Defense Strategies*” Published in IEEE Network, Volume 20, Issue 3, Spring 2006, pages 41-47. http://ieeexplore.ieee.org/servlet/opac?punumber=65 © 2006 by the Institute of Electrical and Electronics Engineers (IEEE)

[5] Yong Wang, GarhanAttebury, Byrav Ramamurthy, “*A Survey of Security Issues In Wireless Sensor Networks*”IEEE

Communications Surveys & Tutorials , 2nd Quarter 2006

[6] SudipMisra , Sanjay K. Dhurandher , AvanishRayankula , DeepanshAgrawal , "*Using honeynodes for defense against jamming attacks in wireless infrastructure-based networks*", Elsevier,Computers& Electrical Engineering, pg. 367-382,Vol. 36, Issue 2, March 2010.

[7] Hoang Nguyen, ThadpongPongthawornkamol and KlaraNahrstedt, "*Alibi: A framework for identifying insider-based jamming attacks in multi-channel wireless networks*" Published in: Proceeding MILCOM'09 Proceedings of the 28th IEEE conference on Military communications Pages 2646-2652 IEEE Press Piscataway, NJ, USA ©2009 ISBN: 978-1-4244-5238-5

[8] LEKSHMI.M.R, N. NITYANANDAM, "*Thwarting Selective Insider Jamming Attacks in Wireless Network by Delaying Real Time Packet Classification*" Indian Journal of Computer Science and Engineering (IJCSE)Vol. 4 No.3 Jun-Jul 2013