A Review on Types of Jamming Attack In Mobile Ad-Hoc Network

R.Maheswari.
M.Phil. Research Scholar – Computer Science, SreeSaraswathiThyagaraja College,
Email ID:ramarajmahes106@gmail.com

Ms.S.Rajeswari. MCA., M.PHIL
HOD of PG Computer science, SreeSaraswathiThyagaraja College
Email ID:rajeswari75_gopal@ yahoo.co.in

----------**ABSTRACT**----------

The works in this paper is about to MANET and classify jamming attacks in 802.11b wireless networks. The number of jamming attack and classification techniques are used. Majority of them model individual parameters like signal strength,carrier sensing time, and packet delivery ratio to detect the presence of a jammer and to classify the jamming attacks. We investigate a multi-modal scheme that models different jamming attacks by discovering the correlation between three parameters: packet delivery ratio, signal strength variation, and pulse width of the received signal. Based on that, profiles are generated in normal scenarios during training sessions which are then compared with test sessions to detect and classify jamming attacks.

Keywords: Attacks, Jamming, MANET, Wireless networks.

---

1. INTRODUCTION

Wireless networks make use of shared transmission medium; therefore, they are open to several malicious attacks. An attacker with a radio transceiver intercepts a transmission, injects spurious packets, and blocks or jams the legitimate transmission. Jammers disrupt the wireless communication by generating high-power noise across the entire bandwidth near the transmitting and receiving nodes. Since jamming attacks extremely damage the performance of wireless networks, some effective mechanisms are required to detect their presence and to avoid them. Constant, deceptive, reactive, intelligent, and random jammers are few jamming techniques used in wireless medium. All of them can partially or fully jam the link at varying level of detection probabilities. Some of them either produce high false alarm rates or do partial detection of jamming attacks. Moreover, the results are based on simulations.

2. MOBILE AD HOC NETWORK

An ad-hoc network is formed when more stations come together form an independent network. Ad-hoc networks do not require any prior infrastructure; therefore, they are also termed as infrastructure-less networks consisting of both fixed node and mobile nodes exchange data with each other without any centralised infrastructure or base station. The transitional node behaves like router to transmit data to nodes not in range. Each node in the MANET having its own processing capability and energy resources and the mobile nodes are moving rapidly. MANET can be easily established in any emergency situations which can be used in disaster recovery, conferences, emergency situation in hospitals, meetings, lectures. Mobile Ad-hoc network has a number of protocols which are classified as reactive, proactive and hybrid for difference types of MANET such as (AODV, DSR, OLSR, TORA and GRP)

3. SECURITY ISSUES IN MANET

In a MANET, nodes within ranges of each other's wireless transmission can communicate directly; however, nodes outside that range will depend on some other nodes to relay messages. An essential set of security mechanism must be encapsulated for any routing protocol to detect, prevent, and respond to security attacks. In order to investigate a reliable and secure ad-hoc network environment there are five major security goals. They are mainly Authentication, Integrity, Confidentiality, Non-repudiation and Availability.

4. MANET ATTACKS

The threats for MANETs are classified as shown in Figure. Types of MANET Attacks.

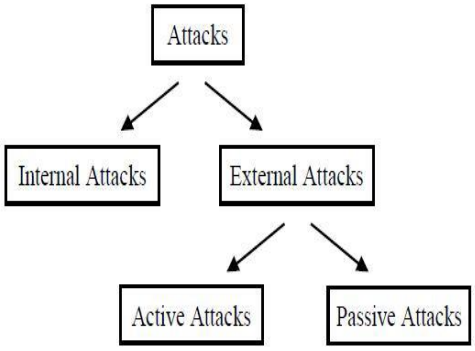

Figure1: Types of Attack.

Among attacks that are considered more of the nodes on the network which can Result in denial-of-service and hence network collapses completely.

5. JAMMING ATTACKS

Firstly one should know what jammer is. Jammer is defined as an individual who is intentionally obstructing the methods of legal wireless communication. It is treated as an active attacker depending upon its intentions and actions. Jamming is a DoS attack's special category used in wireless networks. Handling of Jamming attacks much harder than other attacks. The attacker disrespects the medium access control (MAC) protocol and transmits on the shared channel; A radio signal can be interfered or jammed, which causes the message to be corrupted or lost. The attacker with a powerful transmitter causes that the generated signal will be strong enough to crush the targeted signals and damage communications.

5.1 Types of Jamming Attacks

There are many different attack strategies an adversary can use to jam wireless communications. While it is impractical to cover all the possible attack models that might exist, in this article we review a wide range of jammers that have proven to be effective.

5.1.1 Constant jammers

A constant jammer continuously produces high-power noise that represents random bits. The bit generator does not follow any media access control (MAC) protocol and operates independent of the channel sensing or traffic on the channel.

5.1.2 Random jammers

A random jammer operates randomly in both sleep and jam intervals. During sleep interval, it sleeps irrespective of any traffic on the network, and during jam interval, it acts as a constant reactive jammer. That jammer does not follow any MAC protocol. The PDR increases when the sleep interval increases and the packet size decreases.

5.1.3Deceptive jammers

These jammers continuously send illegitimate packets so that the channel appears busy to the legitimate nodes. They are protocol aware and increase carrier. They are protocols aware and increase carrier They are protocols aware and increase carrier sensing time for the legitimate nodes indefinitely. The difference between a deceptive and a constant jammer is that constant jammer send Random bits continuously while ad adaptive jammer sends packets which appear legitimate to the receiver.

5.1.4 Reactive jammers

A reactive jammer activates when it senses the transmission on the channel. If the channel is idle, it remains dormant and keeps sensing the channel. On sensing the transmission, it transmits enough noise resulting some sufficient number of bits corrupted in the legitimate packet so that packet checksum is not recovered by the receiver and the packet is discarded.

.

5.1.5 Shot noise-based intelligent jammers

Shot noise-based intelligent jammers are protocol-aware jammers that just beat forward error correction (FEC) scheme used at physical and MAC layers. IEEE 802.11bnetworks use convolution coding at the physical layer. Single continuous pulse interfering legitimate packet can completely drop it if it is able to beat the FEC scheme used in the packet.

5.1.6 Nonstop Jamming:

Constant jammers continuously emit electromagnetic energy on a channel. Nowadays, constant jammers are commercially available and easy to obtain. While constant jammers emit non decipherable messages, *deceptive* jammerstransmit seemingly legitimate back-to-back dummy data packets. Hence, they can mislead other nodes and monitoring systems into believing that legitimate traffic is being sent.

5.1.7 Intermittent Jamming:

As the name suggests, these jammers are active intermittently; the primary goal is to conserve battery life. A *random* jammer typically alternates between uniformly distributed jamming and sleeping periods. It jams for Tj s, and then it sleeps for Ts s. A *reactive* jammer starts emitting energy only if it detects traffic on the medium. This makes the jammer difficult to detect. However, implementing reactive jammers can be a challenge.

6. CHARACTERIZING JAMMING ATTACKS

A jamming attack can be detected easily, less effective, energy efficient, or protocol aware. There are a few commonly used metrics characterizing the jamming attacks

- Least detection probability
- Stealthy against detectors
- Completely denial of service like constant jammers
- Protocol aware so that they are less likely to detect
- Authentication of users
- Strength against FEC codes
- Strength at physical layer to beat channel coding techniques

Energy conservation is to get highest jamming efficiency with least energy used the type of metrics also

depends on the application in consideration. Energy efficiency is an important metric for for all the jammers specifically in jamming the sensor networks for a long time. Strong denial of service is critical in war situations. Least probability of detection is desired for jammers if they have to keep for a long time in opponent areas safely. FEC schemes increase resilience of packet against errors. Strong FEC codes can be compromised with constant or intelligent jamming. Similarly, metrics to efficient and accurate detection of jamming attacks are as follows

• Low false alarm rate
• Proactive detection
• Least computational cost
• Quick detection

7.CONCLUSION

In this paper we have described about Fast change infrastructure MANET, different types of jamming attacks and Characterizing jamming attacks in wireless sensor network.The major contribution of the work is the classification of jamming attacks with accuracy and low false alarm rate. Jammer will reduce the performance of the network by decreasing the throughput and increasing delay.

REFERENCES

[1] S.Rajeswari. "*Optimization of an Error Minimizing or Localizing Jammers in Wireless Networks"* International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064.

[2] R. Anderson, Security Engineering: *"A Guide to BuildingDependable Distributed Systems".*John Wiley & Sons, Inc., 2001.

[3] J. Bellardo and S. Savage, *"802.11 denial-of-service attacks:Real vulnerabilities and practical solutions,"* in Proc. USENIXSecurity Symposium, Washington, DC, Aug. 2003, pp. 15–28.

[4] MithunAcharya, David Thuente, "*Intelligent Jamming Attacks, Counterattacks and (Counter)2 Attacks in 802.11b Wireless Networks"*, in Proceedings of the OPNETWORK-2005 Conference, Washington DC,
USA, August 2005.

[5] Abhay Kumar Rai, Rajiv RanjanTewari, Saurabh Kant Upadhyay, *"Different Types of Attacks on Integrated MANET-Internet Communication",* International Journal of Computer Science and Security (IJCSS) Volume (4): Issue (3), 2010, pp. 265-274.

[6] Ali Hamieh, Jalel Ben-Othman, "*Detection of Jamming Attacks in Wireless Ad Hoc Networks using Error Distribution"*, 978-1-4244-3435-0/09 IEEE, 2009.

[7] FarazAhsan, Ali Zahir, SajjadMohsi, Khalid Hussain, *"Survey on survival approaches in wireless network against jamming attack",* Journal of Theoretical and Applied Information Technology, 15th.Vol. 30 No.1, August 2011, pp. 55 – 67.