IOSR Journal of Electrical and Electronics Engineering (IOSR-JEEE)
e-ISSN: 2278-1676,p-ISSN: 2320-3331, Volume 11, Issue 4 Ver. II (Jul. – Aug. 2016), PP 48-52
www.iosrjournals.org

Jamming Attacks with its Various Techniques and AODV in Wireless Networks

Sneha A.Pandhre[1], Prof. Milind B.Tadwalkar[2]

[1]*Department of Electronics and Telecommunication Engineering JSPM's, Jayawantrao Sawant College of Engineering Pune, India*
[2]*Professor, Department of Electronics and Telecommunication Engineering JSPM's, Jayawantrao Sawant College of Engineering Pune, India*

Abstract: *Wireless sensor networks are built upon a shared medium that makes it easy for adversaries to conduct radio interference, or jamming, attacks that effectively cause a denial of service of either transmission or reception functionalities. These attacks can easily be accomplished by an adversary by either bypassing MAC-layer protocols or emitting a radio signal targeted at jamming a particular channel. Smart grids have been drawing increasing attention on physical infrastructures. It has broad application for time critical message delivery in wireless networking. In conventional data service networks, where communication traffic is more time-critical, we aim at evaluating and detecting jamming attacks against time critical wireless networks with application to smart grid. Based upon this, to achieve the robust jamming detection, we have implemented JADE (Jamming Attack Detection based on Estimation) system in smart grid for power substations in wireless networks using AODV (Ad-hoc on Demand Distance Vector Routing Protocol) in which number of nodes communicate with each other using On-demand communication link protocol considering the time critical factor.*

Keywords: *Time critical messages, Smart grid, Jamming attacks, Wireless networks*

I. Introduction

Wireless technologies have radio interference that target communication medium. Unlike Denial-of-services attacks, jamming attacks exploit the shared nature of wireless medium in order to prevent sending or receiving. In these systems jamming is addressed by spreading techniques whereas the interference can be resilience by using a wide bandwidth for e.g Code Division Multiple Access (CDMA).

A typical wireless sensor node has a protection against the radio jamming. In the data link layer the situation can become worst if the energy efficient jamming can be achieved. Based on the content of the packet encrypting the packet may help in preventing the jammer actions, but if the nature of the protocol can unravel pattern and the jammer can take advantage of this situation. Attacks are examined by analyzing the efficiency and effectiveness.

We consider a scenario in which a jammer jams an area in which a single-channel random-accessed-based wireless sensor network operates. In order to cause the maximal damage the jammer controls the transmission range. In order to optimized, the network defends itself by computing the channel access probability to minimize the jamming detection. To perform selective jamming, the adversary must be capable of classifying transmitted packets in real time, and corrupting them before the end of their transmission. Packet classification can be performed by receiving just a few bytes of a packet, for example, by decoding the frame control field of a MAC-layer frame. Resource efficient methods for preventing real-time packet classification has been developed and hence, mitigating selective jamming.

In a Mobile Ad Hoc Network (MANET), the network may experience rapid and unpredictable topology changes because of the presence of the mobile nodes. Every node in MANET has the responsibility to act as a router and routing paths in MANETs. These are easily exploited by various attacks due to the wireless nature of the channel and specific characteristics of MANETs. A malicious node can continually transmit a radio signal in order to block any type of legitimate access to the medium and/or infer with reception. This phenomenon is called as jamming and the malicious nodes are termed to as jammers.

For an adversary agnostic to the implementation details of the network, a typical jamming strategy is the continuous emission of high-power interference signals such as continuous wave tones, or FM modulated noise.

Wireless networks are sometimes exposed to jamming attacks because of the shared nature of the wireless channel that may degrade the performance of these time-critical networks. On physical infrastructures delivery of such messages is expected to be followed by a sequence of actions. Instability of the system operations due to overdue messages may lead to cascading failures. For example, a binary result of fault detection on power feeder can trigger subsequent operations of circuit breakers. The actions on the circuit breakers will get delayed if the message does not arrive on time or the result is missed, which can cause fault propagation along physical infrastructures and potential damage to power-equipments.

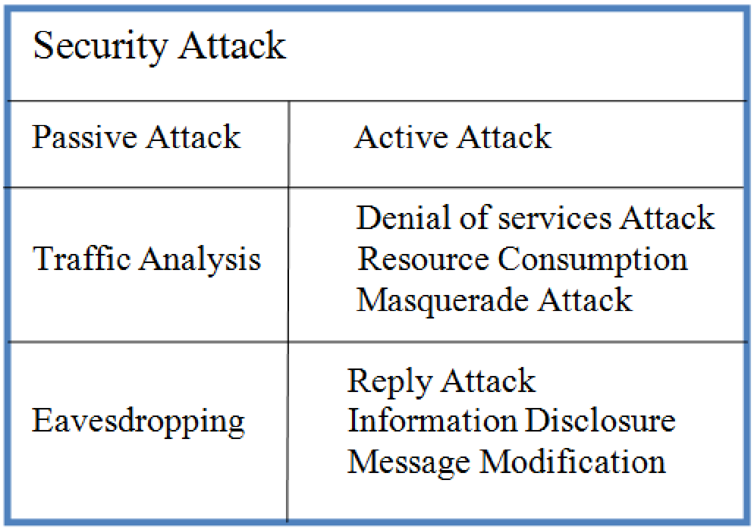
In the systems like Berkeley MICA2, the Zigbee (e.g. MICCAZ) and even 802.11 because of their use of carrier sensing approach for medium access control(MAC) they are likely to be susceptible to simple and severe jamming problem, an advisory can simply disregard the medium access and continue to transmit on the wireless channel. The objective of the jammer is to deny the reception at the receiver using as little power as possible. This prevents the user from being able to operate with the MAC (Medium Access control) or simply it can introduce a packet collision that creates repeated back-offs that results in jamming of the signal. Sensor networks will remain vulnerable to attacks that target their use of wireless medium.

Security Attacks: Mostly commonly seen in the wireless networks, they can be summarize in the Table no. 1 given below .Most attacks can be divided in two types one is active and other is passive. Passive attacks do not disrupt the network operation while the active attacks can interfere with the network. The advisory in the former part steal the transmitted information and the latter tries to alter network data.

Dos Attacks: Dos (Denial of service attacks) it attempts to exhaust the resources available to its legitimate users. An advisory uses the radio signal to make the attacked nodes suffer from the Dos in specific region.

Masquerade attacks: Here in this system the attacker pretends to be a user and deceives the authentication system so as to disrupt the system, that means it captures the authentication sequences and therefore it becomes an invalid user, and obtains an access to use the information illegally.

Eavesdropping and traffic analysis: Eavesdropping is a way for an attacker to intercept a message called as eavesdropper. We use the encryption technique in this so that the message that is needed to be transmitted, even if it get intercept, then the contents will not be retrieved.



Security Attack	
Passive Attack	Active Attack
Traffic Analysis	Denial of services Attack Resource Consumption Masquerade Attack
Eavesdropping	Reply Attack Information Disclosure Message Modification

Table 1 Classification of different security attacks in wireless communication

II. Motivation

As the “Active jammers” keep the channel busy all the time they are most effective. An alternative approach here that can be considered is reactive strategy in which we can see that there exits two systems or types one in which focus on the strategy that it stays quite when channel is idle, but starts a radio signal as soon as it senses any activity on the channel. And other one can be considered as just opposite of first one that means it does not reacts to the any suspicious activity going on in the network it remains or stays quite. In our system we are going to see a scenario in the networking field which considers a small scale network, in which a sender and receiver communicates using AODV protocol which decides the route to be specified for the required communication to happen or to take place. In this the receiver gets attack by the jammer by knowing the frequency on which the receiver is operating. Further detail operation can be considered in next session.

III. Literature Survey

Mario Strasser et al. (2008) considers the problem of how can two devices that do not share any secrets establish a shared secret key over a wireless radio channel in the presence of a communication jammer. An inherent challenge in solving this problem was that known anti-jamming techniques (e.g., frequency hopping or direct-sequence spread spectrum) which should support device communication during the key establishment required that the devices shared a secret spreading key (or code) prior to the start of their communication. This requirement created a circular dependency between anti jamming spread-spectrum communication and key establishment. The author proposed an Uncoordinated Frequency Hopping (UFH) scheme that breaks the dependency and enables key establishment in the presence of a communication jammer. The author performed a detailed analysis of UFH scheme and showed its feasibility, both in terms of execution time and resource requirements. Ali Hamieh et al. (2009) describes that the military tactical and other security sensitive operations are still the main applications of ad hoc networks. One main challenge in design (DoS) attacks.

In this paper, we consider a particular class of DoS attacks called Jamming. A new method of detection of such attack by the measurement of error distribution was proposed. To differentiate the jamming scenario from legitimate scenarios, the author measured the dependence among the periods of error and correct reception times. In order to measure this dependency, auhtor used the Correlation Coefficient which is a statistic measure of relation between two random variables. Zhuo Lu Wenye Wang et al. (2011) aims at modeling and detecting jamming attacks against time-critical traffic. The author introduced a new metric, message invalidation ratio, to quantify the performance of time-critical applications. The author claims that the behavior of a jammer who attempts to disrupt the delivery of a time-critical message can be exactly mapped to the behavior of a gambler who tends to win a gambling game.

In November 2001 the MANET (Mobile Ad-hoc Networks) Working Group for routing of the IEFT community has published the first version of the AODV Routing Protocol (Ad hoc On Demand Distance Vector).

AODV belongs to the class of Distance Vector Routing Protocols (DV). In a DV every node knows its neighbors and the costs to reach them. A node maintains its own.

IV. Discussions On Various Techniques In Jamming

Carrier sensing time and signal strength are sometimes not successful in detecting the presence of jamming attacks. Two devices that do not share any secrets establish a shared secret key over a wireless radio channel in the presence of communication jammer. Devices that share a secret spreading key prior to start of their communication should support device communication using the anti-jamming techniques (frequency hopping or direct sequence spread spectrum).A technique that enabled key establishment in presence of communication jammer and breaks the dependency created “uncoordinated frequency hopping (UFH)”.

The most important physical layer standard that can be used as IEEE 802.11 is having the highest well known recognition and is known as WLAN services. The main factor which is considered to be affected by the jamming attack is the “frequency”. There are certain other parameters or we can say we have few technical terms that could be considered to explain this in more deep manner and they are FHSS (Frequency Hopping), DSSS(Direct Sequence Spread Spectrum), Channel Surfing and smallest circle covering.

V. Methodology

The existing data services are based on packet-switched networks. So, in conventional wireless networks, the impact of jamming attacks is evaluated at the packet level such as packet send/delivery ratio and the number of jammed packets, or at the network level such as saturated network throughput. However, packet-level and network-level metrics do not directly reflect the latency constraints of message exchange in time-critical applications. For example, 100% packet delivery ratio does not necessarily mean that all messages can be delivered on time to ensure reliable operations in a cyber-physical system.

We design and implement the JADE system (Jamming Attack Detection based on Estimation) to achieve efficient and reliable jamming detection for power networks.

Figure 1 shows the block diagram of the JADE (jamming Atta) system. In the communication networking system there are sender and receiver who need to communicate to exchange data between each other. Firstly, the sender node decides the path to send the receiver node. It sends a REREQ (receiver request) to the receiver. The receiver gives the acknowledgement RERPL (receiver reply) that it is free to receive the data, if it is busy then it sends a busy signal to the sender. Sender starts sending the packet data in particular time interval period. While the transmission is going on the jammer detects the transmission frequency and starts the transmission on the same the path. As the jammer starts sending the data to the receiver, the packet data at the sender side will not be received by the receiver and it will starts dropping. As the receiver is unable to receive the packets send by the sender, so the receiver gives the acknowledgement to the sender that it is unable to receive the packets using AODV protocol, as soon as the sender receives such message, the sender will slow the packet sending rate.

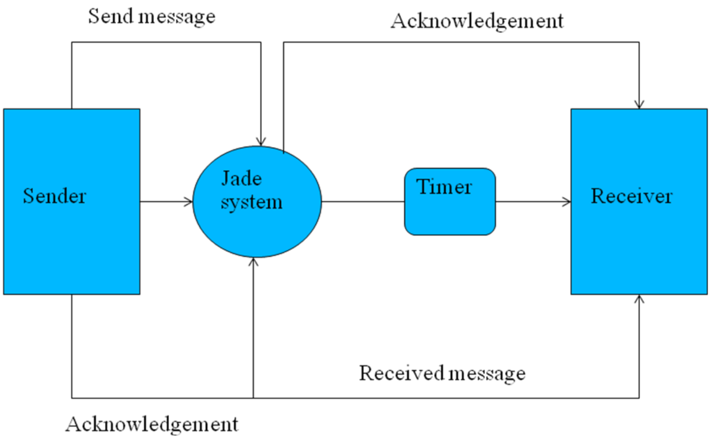


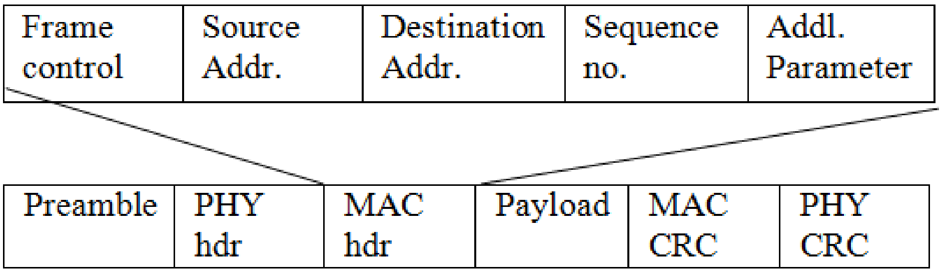
Figure 1 Block Diagram of JADE system

And till the time the packet sent by the sender reaches to the destination, the receiver has stops receiving the packets send by the sender and gets packet sent by the jammer as soon as the receiver realizes that the packets received are not correct or it has not been sent by the sender the receiver will stop receiving the packets and gets deactivated for particular time interval then the jammer stops sending the packet to the receiver, as it stops receiving the packets, as the jammer realizes that receiver has stop working so it also stops working. As soon as the jammer stops sending packets, the receiver node again gets activated and sends acknowledgment to the sender that it is again ready to receive the packet data. And the process continues till the time duration allotted to the particular path to execute the operation.

The scenario consists of 50 mobile nodes deployed randomly in 1000x1000 m. Nodes move in this area with the mobility speed of 10m/s. This is based on the virtual jamming; here the focus is on the jamming attack at the MAC layer. In virtual jamming malicious node send RTS packets continuously on the transmission with unlimited period of time. The Ad-hoc routing protocol is changed according to the requirement of the simulation in order to analyze the result under the AODV protocol. Here the packet size is set to 1000 and the packet inter-arrival time is 0.01 seconds.

Figure 2 shows the Fig.2 Generic frame format for wireless network.

The frame format consists of preamble, PHY-header followed by the payload, then MAC CRC and the PHY-trailer. The MAC header consists of source and the destination address of the packet. Then we are going to see in detail the use of each term. The first one is the preamble which is used for synchronizing the process at the receiver side. The transmission rate and the length of the frame is defined by PHY-layer header.



Frame control	Source Addr.	Destination Addr.	Sequence no.	Addl. Parameter

Preamble	PHY hdr	MAC hdr	Payload	MAC CRC	PHY CRC

Figure 2 A Generic Frame format for a wireless Network

The third term used is the frame is „MAC header‟. This header includes information such as source and destination address, the version of protocol used, sequence number and some additional fields. The next field is payload which typically contains either ARP packet or an IP datagram. At the last, the cyclic redundancy check (CRC) code is used to protect the MAC frame in order to achieve great security. To maintain the synchronization between sender and receiver the trailer may be appended, at PHY layer.

VI. AODV (Ad-Hoc On Demand Distance Vector Routing Protocol)

Our basic proposal can be called a pure on-demand route acquisition system nodes that do not lie on active paths neither maintain any routing information nor participate in any periodic routing table exchanges. Further, a node does not have to discover and maintain a route to another node until the two needs to communicate, unless the former node is offering its services as an intermediate forwarding station to maintain connectivity between two other nodes.

When the local connectivity of the mobile node is of interest, each mobile node can become aware of the other nodes in its neighborhood by the use of several techniques, including local (not system-wide) broadcasts known as hello messages. The routing tables of the nodes within the neighborhood are organized to optimize response time to local movements and provide quick response time for requests for establishment of new routes. The algorithm's primary objectives are:

1. To broadcast discovery packets only when necessary
2. To distinguish between local connectivity management (neighborhood detection) and general topology maintenance
3. To disseminate information about changes in lo-cal connectivity to those neighboring mobile nodes those are likely to need the information.

AODV uses a broadcast route discovery mechanism, as is also used (with modifications) in the Dynamic Source Routing (DSR) algorithm. Instead of source routing, however, AODV relies on dynamically establishing route table entries at intermediate nodes. This difference pays in networks with many nodes, where a larger overhead is incurred by carrying source routes in each data packet. To maintain the most recent routing information between nodes, we borrow the concept of destination sequence numbers from DSDV. Unlike in DSDV, however, each ad-hoc node maintains a monotonically increasing sequence number counter which is used to supersede stale cached routes. The combination of these techniques yields an algorithm that uses bandwidth efficiently (by minimizing the network load for control and data traffic), is responsive to changes in topology, and ensures loop-free routing.

VII. Conclusion

In this paper, jamming attacks in wireless networks and their significant changes and benefit in people’s life have been discussed. Modeling Systems such as Reactive and Non-reactive jammers constitute the majority of jamming attacks widely adopted in existing data communication networks. They can serve as more intelligent jamming strategies against the time-critical traffic. Also we have discussed different types of security attacks in wireless communication system. AODV uses a broadcast route discovery mechanism. Instead of source routing, however, AODV relies on dynamically establishing route table entries at intermediate nodes. This difference pays in networks with many nodes, where a larger overhead is incurred by carrying source routes in each data packet. AODV maintains the most recent routing information between nodes; we borrow this concept from destination sequence numbers from DSDV. Unlike in DSDV, however, each ad-hoc node maintains a monotonically increasing sequence number counter which is used to supersede stale cached routes. The combination of these techniques yields an algorithm that uses bandwidth efficiently by minimizing the network load for control and data traffic and ensures loop-free routing i.e. AODV.

References

[1] P. Sudha , K.Durairaj, “From Jammer to Gambler: Modeling and Detection of Jamming Attacks against time Critical Traffic ”IEEE, March 2015.

[2] Prakash J.Parmar, Sachin D. Babar, “Survey of jamming Attacks and Techniques in wireless sensor Networks ”,IJOAR,Aug 2014.

[3] Gavali S.B, Gavali A.B, Patil D.S, “Review on Packet Hiding : A new Paradigm for Avoiding Jamming Attack over Wireless Network”, 2014.

[4] Divya S. Manoher Gosul, “Jamming Attack Prevention in Wireless Networks using Packet Hiding Methods”, IOSCJCE, September 2014.

[5] Upma Goyal, Mansi Gupta and Karanveer Kaur, “Meliorated Detection Mechanism for the Detection of Physical Jamming Attacks under AODV and DSR Protocol in MANETS ”, Oct 2014