IJournals: International Journal of Software & Hardware Research in Engineering
ISSN-2347-4890
Volume 4 Issue 7 July, 2016

A System to Analyze Detection of Jamming Attacks in Time Critical Wireless Applications

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

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

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

E-mail: pandhre.sneha@gmail.com[1] , mbtadwalkar@yahoo.com[2]

ABSTRACT

In time critical wireless applications there exits number of applications in networking field such as smart grid and E-Health care system. The broadcast nature of the wireless networks however sometimes needs to face the jamming attacks. Based on the idea of the JADE (Jamming Attack Detection based on Estimation) system to achieve efficient and robust jamming detection for time critical wireless networks we have designed a wireless network using AODV (Ad-hoc on Demand Distance Vector Routing Protocol) in which number of nodes present in the network communicate with other using On-demand communication link feature of the AODV protocol considering the time critical factor.

Keywords: Time critical factor, JADE (Jamming attack detection based on estimation), AODV, Smart Grid.

1. INTRODUCTION

Wireless networks are susceptible to numerous security threats due to the open nature of the wireless medium. Anyone with a transceiver can eavesdrop on ongoing transmissions, inject spurious messages, or block the transmission of legitimate ones. One of the fundamental ways for degrading the network performance is by jamming wireless transmissions. In the simplest form of jamming, the adversary corrupts transmitted messages by causing electromagnetic interference in the network's operational frequencies, and in proximity to the targeted receivers.

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. However, adopting an "always-on" jamming strategy has several disadvantages. First, the adversary has to expend a significant amount of energy to jam frequency bands of interest. Second, the continuous presence of high interference levels makes this type of jamming easy to detect. Third, these attacks are easy to mitigate either by spread spectrum communications, spatial retreats, or localization and removal of the jamming nodes.

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. Due to the wireless nature of the channel and specific characteristics of MANETs, these are easily exploited by various attacks. 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.

An ad-hoc network is the cooperative engagement of a collection of mobile nodes without the required intervention of any centralized access point or existing infrastructure. In this paper we present Ad-hoc On Demand Distance Vector Routing (AODV), a novel algorithm for the operation of such ad-hoc networks. Each Mobile

Host operates as a specialized router, and routes are obtained as needed (i.e., on-demand) with little or no reliance on periodic advertisements. Our new routing algorithm is quite suitable for a dynamic self-starting network, as required by users wishing to utilize ad-hoc networks. AODV provides loop-free routes even while repairing broken links. Because the protocol does not require global periodic routing advertisements, the demand on the overall bandwidth available to the mo-bile nodes is substantially less than in those protocols that do necessitate such advertisements. Nevertheless we can still maintain most of the advantages of basic distance-vector routing mechanisms. We show that our algorithm scales to large populations of mobile nodes wishing to form ad-hoc networks. We also include an evaluation methodology and simulation results to verify the operation of our algorithm.

Although AODV does not depend specially on particular aspects of the physical medium across which packets are disseminated, its development has been largely motivated by limited range broadcast media such as those utilized by infrared or radio frequency wireless communications adapters. Using such media, a mobile node can have neighbors which hear its broad-casts and yet do not detect each other (the hidden terminal problem). We do not make any attempt to use specific characteristics of the physical medium in our algorithm, nor to handle specific problems posed by channelization needs of radio frequency transmitters. Nodes that need to operate over multiple channels are presumed to be able to do so. The algorithm works on wired media as well as wireless media, as long as links along which packets may be transmitted are available. The only requirement placed on the broad-cast medium is that neighboring nodes can detect each others' broadcasts.

2. 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, the author considers 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, author 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 routing table, storing all nodes in the network, the distance and the next hop to them. If a node is not reachable the distance to it is set to infinity. Every node sends its neighbors periodically its whole routing table. So they can check if there is a useful route to another node using this neighbor as next hop. When a link breaks a Count-To-Infinity could happen.

3. 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.

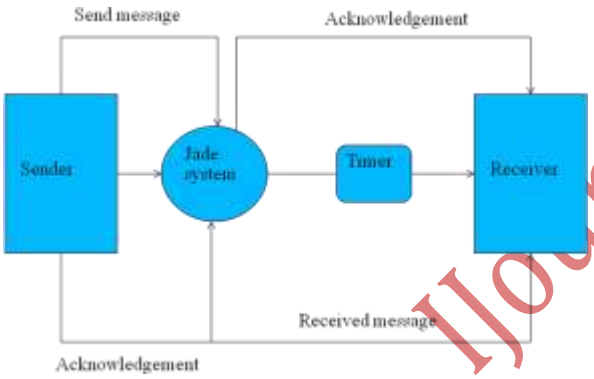

Figure 1 Block Diagram of JADE system

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 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, as soon as the sender receives such message, the sender will slow the packet sending rate. And till the time the packet sent by the sender reaches to the destination 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.

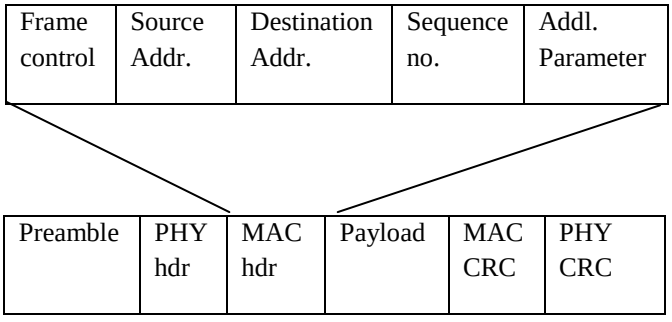

Figure 2 A Generic Frame format for a wireless Network

Figure 2 shows the 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.

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.

4. 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) broad-casts 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 local 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.

5. CONCLUSION

Here an internal threat model is considered in which the jammer is part of the network, thus being aware of the protocol specifications and network secrets. Jammer can classify transmitted packet in real time by decoding the first few symbols of an ongoing transmission or packet.

Although AODV does not depend specially on particular aspects of the physical medium across which packets are disseminated, its development has been largely motivated by limited range broadcast media such as those utilized by infrared or radio frequency wireless communications adapters. Using such media, a mobile node can have neighbors which hear its broad-casts and yet do not detect each other (the hidden terminal problem.

6. DISCUSSIONS

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).

AODV uses symmetric links between neighboring nodes. It does not attempt to follow paths between nodes when one of the nodes cannot hear the other one however we may include the use of such links in future enhancements.

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 o_ 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 i.e. AODV.

7. REFERENCES

[1]. Gavali S.B, Gavali A.B, Patil D.S, "Review on Packet Hiding : A new paradigm for Avoiding Jamming Attack over Wireless Network", 2014.

[2]. P. Sudha1, K. Durairaj, "From Jammer to Gambler: Modeling and Detection of Jamming Attacks against Time Critical Traffic.",IEEE, March 2015.

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

[4]. Upma Goyal, Mansi Gupta and Kiranveer Kaur , "Meliorated Detection Mechanism for the detection of Physical Jamming Attacks under AODV and DSR protocols in MANETs.",October 2014

