Detection and Prevention of various types of Jamming Attacks in Wireless Networks

Mr. Pushphas Chaturvedi
Dept. Of Computer Science
Amity University
Noida, India

Mr. Kunal Gupta
Dept. Of Computer science
Amity University
Noida India

***Abstract* - Basic characteristic of wireless networks that makes it vulnerable to attacks is its broadcast nature. Attacks are of various types that effect confidentiality and integrity of wireless network and in this paper we are discussing about Jamming attacks. Jamming can stop or disrupt wireless transmission. It is interference, noise or collision at the receiver end. Jamming may happen unintentionally by network load or intentionally in form of attack. No specific hardware is used for executing it, it can be easily implemented by listening to the open medium and broadcasting in the frequency band same as network. If it is executed successfully it gives significant advantages to the attacker at very low cost. That is the reason why it is effective.**

So in this paper we are giving detailed overview of Jamming attacks and their types with its detection and prevention techniques.

***Keywords* - Jamming attacks, Commitment scheme, Physical jamming, Virtual jamming, Rate adaptation scheme**.

I. INTRODUCTION

In modern era the accommodations provided by the 802.11 based wireless access network led to its deployment in various sectors such as defence, consumer and industrial sector. Openness of wireless network makes it vulnerable to various types of attacks. Out of various types of attacks, Denial-of-service (DoS) attack is one of the most troublesome threat which prevent legitimate users from accessing the network. It is executed in many ways such as intentional interference or jamming. Jamming is one of many exploits used compromise the wireless environment. It works by denying service to authorized users as legitimate traffic is jammed by the overwhelming frequencies of illegitimate traffic. If an attacker truly wanted to compromise your LAN and wireless security, the most effective approach would be to send random unauthenticated packets to every wireless station in the network. To minimize the impact of an unintentional disruption, it is important to identify its presence. Jamming makes itself known at the physical layer of the network, more commonly known as the MAC (Media Access Control) layer. The increased noise floor results in a faltered noise-to-signal ratio, which will be indicated at the client. It may also be measurable from the access point where network management features should able to effectively report noise floor levels that exceed a predetermined threshold. From there the access points must be dynamically reconfigured to transmit channel in reaction to the disruption as identified by changes at the physical layer.

II. TYPER OF JAMMING

A. Physical Jamming (Physical Layer)

Physical or Radio jamming in a wireless medium is a simple but disruptive form of DoS attack. These attacks are launched by either continuous emission of radio signals or by sending random bits onto the channel. The jammers causing these attacks can deny complete access to the channel by monopolizing the wireless medium. The no destroying to communicate have an unusually large carrier sensing time waiting for the channel to become idle. This has an adverse propagating effect as the nodes enter into large exponential back-off periods.

B. Virtual Jamming (MAC Layer)

In IEEE 802.11 based MAC protocols, virtual carrier sensing is used at the MAC layer to determine the availability of the
wireless medium. Jamming can be launched at the MAC layer through attacks on the RTS/CTS frames or DATA frames. A significant advantage of MAC layer jamming is that the adversary node consumes less power in targeting these attacks as compared to the physical radio jamming. Here, we focus on DoS attacks at the MAC layer resulting in

collision of RTS/CTS control frames or the DATA frames.

C. Synchronization Signal Jamming (SSJ)

When a UE wants to connect to an Node, it has to first go through a series of synchronization steps. First, it detects the Primary Synchronization Signal (PSS) which allows the UE to synchronize to each slot and gives it the cell ID. Next, it detects the Secondary Synchronization Signal (SSS) which tells the UE the cell ID group, which method of duplexing is used, and the cyclic prefix length. The SSS also allows the UE to detect when each radio frame starts. Both the PSS and SSS are mapped to the central 62 subcarriers (not including the DC subcarrier). After synchronizing with the PSS and SSS, the UE receives more information about the cell by decoding the Master Information Block (MIB). The MIB contains information essential for initial access to a cell. It consists of 14 bits that contain the downlink system bandwidth, the Physical Control Format Indicator Channel (PHICH) size, and information allowing frame synchronization. It is mapped to the central 72 subcarriers, and appears in slot 1 of each frame. The three signals are not present in all ten subframes, but they are always mapped to the same subcarriers.

The Synchronization Signal Jamming (SSJ) attack is designed to deny the UE access to the PSS, SSS, and MIB. The jamming waveform used for the SSJ attack is noise that spans the center 73 subcarriers. The DC subcarrier is included for the sake of complexity, even though it does not contain information. The SSJ attack does not involve jamming specific symbols (it uses a 100% duty cycle), so the jammer does not have to be synchronized to the Node. The SSJ attack is simply a brute force method of denying the UE three different mechanisms that it needs to access a cell. The act of only jamming certain subcarriers allows the SSJ attack to have roughly a 3 dB gain over traditional barrage jamming, which can be thought of as an increase in jamming radius for a jammer that is power constrained.

D. Primary Synchronization Signal Jamming

Detecting the PSS is the first step a UE takes in accessing a cell. The PSS uses a sequence length of 63, and the center element is nulled because the downlink DC subcarrier is never used for transmission. There are three PSS sequences used in LTE, and each one corresponds to one of the three sectors. The UE must detect the PSS without any knowledge of the channel, so it finds the timing offset that corresponds to the maximum cross-correlation for each of the three sequences, and uses it to synchronize in the time domain. For FDD, the PSS only occurs in slots 0 and 10 (there are 20 total slots per frame).

The SSJ attack discussed previously injects noise into the subcarriers that contain the PSS. An attack that only targets the PSS can be realized by only jamming the symbols that contain the PSS. However, the jammer would have to cause a fairly high jammer-to-signal ratio, because the PSS is designed to be detected at high interference levels, so that the UE can also detect neighbouring cells.

A more effective method of causing a PSS attack would be to simply transmit one of the three PSS sequences, and thus create a bogus PSS. If the jammers received power at the UE is greater than the Node's, then the UE is most likely going to synchronize to the bogus PSS. This is because a cross-correlation process is used to detect the PSS non-coherently. A jammer using this method would not need receiving capability, because it would simply start the bogus PSS transmission at a random time, leading to uniformly distributed timing relative to the correct PSS signal. If the UE synchronized to the bogus PSS, then is not synchronized in time to the Node, and it will not know when each OFDM symbol starts, and hence will not be able to detect the SSS or decode the MIB.

This attack appears to work, until considering the cell reselection procedure. If a cell does not provide a certain level of quality, then the UE begins the cell reselection procedure, where it tries to access the cell with the next strongest signal. The solution is to spoof all three PSS sequences. A jammer transmitting three bogus PSSs only has to transmit six symbols in every frame, on 62 subcarriers. A downside to PSS jamming is that it will not immediately cause Denial of Service (DOS). It will prevent new UEs from accessing the cell(s), and cause UEs in idle mode to reselect a bogus cell. Therefore PSS jamming is not effective for an attack intended on causing immediate DOS. However, it is sufficient for an attack that will last a long period of time. Because the jammer barely has to transmit anything, the PSS jamming attack offers roughly 20 dB of gain relative to the barrage jamming attack. This results in an extremely efficient jammer.

Fortunately, this type of attack can be prevented by employing a cell reselection implementation that is able to blacklist “bogus synchronization signals”, by keeping track of the time-delay in the cross-correlation.

E. Physical Uplink Control Channel Jamming

The Physical Uplink Control Channel (PUCCH) is used to send the Node a variety of control information, including scheduling requests, Hybrid Automatic Repeat Request (HARQ) acknowledgements, and channel quality indicators.

The PUCCH is mapped to the resource blocks on the edges of the system bandwidth. These resource blocks are evenly split between the two edges of the system bandwidth, and the UE rapidly alternates between the two sets of resource blocks, for the purpose of frequency diversity. When a UE is transmitting on the PUCCH it is not transmitting anything else. This allows PUCCH jamming to be feasible, even with SC-FDMA in use. PUCCH jamming is possible when the only a priori knowledge is the system bandwidth and location in the uplink signal in the frequency domain.

The signal sent on the PUCCH by the UE depends on the type of information it wants to send. For scheduling requests, all the UE has to do is transmit energy in its assigned slot. This causes the Node to assign the specific UE additional uplink resources. This means PUCCH jamming will cause the Node to assign every active UE additional uplink resources (which they probably do not need), and cause degradation of service. The signal transmitted by the UE for ACK and NACK responses is not as straightforward; it involves modulating the ACK or NACK indicator onto a predefined sequence which is then cyclically shifted and scrambled. This system is meant to allow multiple PUCCH transmissions to exist in the same time and frequency slot. Successful PUCCH jamming will cause ACKs to not reach the eNodeB, resulting in retransmissions and further degradation of service. The last type of control information sent on the PUCCH is channel state information, which is used by the UEs to send the Node information about the channel quality. The Node uses this information to assign subcarriers to users that experience better channel conditions on the corresponding frequencies, as well as choose which modulation scheme to use. As in the ACK indicators, the information is sent to the Node through modulation with a UE-specific sequence, which is then scrambled and cyclically shifted. The corruption of channel quality information is not as detrimental to the LTE service as missed ACKs, but it is likely to help accelerate the process of causing DOS. PUCCH jamming offers roughly 5 dB of gain compared to barrage jamming, because the jammer can focus its energy into the control channel subcarriers.

III. DETECTION OF JAMMING

The network employs a monitoring mechanism for detecting potential malicious activity by a jammer. The monitoring mechanism consists of the following: (i) determination of a subset of nodes *M* that will act as network monitors, and (ii) employment of a detection algorithm at each monitor node. The assignment of the role of monitor to a node can be affected by energy limitations and detection performance specifications.

In this work, we fix *M* and formulate optimization problems for one or more monitor nodes. We now fix attention to detection at one monitor node. First, we define the quantity to be observed at each monitor node. In our case, the readily available metric is probability of collision that a monitor node experiences, namely the percentage of packets that are erroneously received. During normal network operation, and in the absence of a jammer, we consider a large enough training period in which the monitor node "learns" the percentage of collisions it experiences as the long-term average of the ratio of number of slots in which there was a collision over total number of slots of the training period. Assume now the network operates in the open after the training period and fix attention to a time window much smaller than the training period. An increased percentage of collisions over this time window compared to the learned long-term average may be an indication of an ongoing jamming attack or only a temporary increase of percentage of collisions compared to the average during normal network operation. A detection algorithm takes observation samples obtained at the monitor node (i.e, collision or not collision) and decides whether there exists an attack. On one hand, the observation window should be small enough, such that the attack is detected on time and appropriate countermeasures are initiated. On the other hand, this window should be sufficiently large, such that the chance of a false alarm notification is minimized.

IV. PREVENTION OF JAMMING

A. Rate Adaptation Scheme

Most of widely used jamming attack solutions have some limitations. Those solutions use spatial or spectrum diversity to cope with the jamming attack. These schemes do not utilize the jammed channels, though they have enough bandwidth for the data transmission. Rate adaptation scheme to overcome problems in previous works. The most important goal of the proposed scheme is to achieve high link utilization by adjusting the transmission mode based on the expected maximum throughput. The expected maximum throughput must consider the successful transmission probability.

Suppose that L is the length of data frame and Tm is the transmission time of data frame in a specific transmission mode, m. Each transmission mode specifies the transmission rate appropriately adapted to network condition. The successful transmission probability can be calculated using error probabilities for a data frame and ACK frame. An ACK frame which is usually much shorter than the data frame is transmitted at the rate equal to or

lowers than the data frame rate. Therefore, the error probability of the ACK frame is much lower than that of the data frame. Hence we can approximate the successful transmission probability.
The error probability for a data frame can be calculated using error probability of the PLCP (Physical Layer Convergence Procedure) scheme selects the transmission mode based on the expected maximum throughput. Each node is able to calculate the expected maximum throughput for each transmission mode m from a set of available transmission modes, *M*. Finally we can choose the optimal transmission mode.

B. Mapping to Commitment Scheme for Selective Jamming attack prevention

For Countering selective jamming, the goal of this scheme is to transform a selective jammer to a random one. This can be achieved by overwhelming the adversary's computational ability to perform real-time packet classification. It first show that our problem can be mapped to the hiding property of commitment schemes
Commitment schemes are fundamental cryptographic primitives that allow a committer *P*, commit to a value *m* to a verifier *V* while keeping *m* hidden. Initially, *P* provides *V* with a commitment $C = commit(m, r)$, where *commit* is some commitment operation, and *r* is a random number. At a later stage, *P* can release additional information that reveals *m.* A scheme that does not allow the computation of *m* from *C* without additional information from *P* is called *perfect* or *hiding*, while a scheme that does not allow *P* to change *m* to a value *m_* once *C* is released, is called *binding*.
The role of the committer is assumed by the transmitting node *S*. The role of the verifier *V* is assumed by any receiver *R* within the communication range of *S*, including the jammer *J*. Note that *S* has no particular interest in modifying *m* after he has committed to it, since its primary goal is to communicate *m*. However, satisfying the binding property ensures that, (a) only *S* can release information that reveals *m*, and (b) the only value that *R* can accept is *m.*
To prevent selective jamming, *S* first transmits *C* that hides *m* from any receiver, including *J*. Once the transmission of *C* is completed, *S* reveals additional information that "opens" *C*. Intended receivers are able to read *m*. We now provide a scheme that prevents packet classification based on the idea
of commitments.

V. CONCLUION

We addressed the problem of jamming in wireless networks and illustrated the effectiveness of jamming attacks, such as attacks against the TCP protocol. We showed that an adversary can exploit its knowledge of the protocol implementation to increase the impact of his attack at a significantly lower energy cost. We illustrated the feasibility of jamming attacks by performing real time packet classification, we have discussed two methods which are Rate adaptation technique and Mapping to commitment scheme for selective jamming attacks. Packet hiding methods can also be used for jamming prevention.

ACKNOLEDGEMENT

I Would like to acknowledge and extend my heartfelt gratitude to following persons who made the completion of this paper possible.
Dr. Ashok Chouhan, Chairman Amity University
Dr. Abhay Bansal, HOD, Dept. of CSE, ASET
and also to my family and friends.

REFERENCES

[1] Stefania Sesia, Issam Toufik, and Matthew Baker, editors, LTE, The UMTS Long Term Evolution: From Theory to Practice, chapter 9. John Wiley & Sons Ltd, Chichester, West Sussex, United Kingdom, second edition, 2011.

[2] Mingyan Li, Iordanis Koutsopoulos and Radha Poovendran, Optimal Jamming Attacks and Network Defense Policies in Wireless Sensor Networks,infocom,2007

[3] Geethapriya Thamilarasu, Sumita Mishra and Ramalingam Sridhar, Improving Reliability of Jamming Attack Detection in Ad hoc Networks, International Journal of Communication Networks and Information Security (IJCNIS) Vol. 3, No. 1, April 2011

[4] Kwangsung Ju and Kwangsue Chung, Jamming Attack Detection and Rate Adaptation Scheme for IEEE 802.11 Multi-hop Tactical Networks, International Journal of Security and Its Applications Vol. 6, No. 2, April, 2012

[5] Alejandro Proa˜no and Loukas Lazos, Selective Jamming Attacks in Wireless Networks, Dept. of Electrical and Computer Engineering University of Arizona, Tucson, Arizona

[6] OPNET http://www.opnet.com/solutions/network rd/modeler.html.

[7] IEEE802.11standard http://standards.ieee.org/getieee802/download/802.11-2007.pdf, 2007.

[8] Shabnam Sodagari and T. Charles Clancy, Efficient Jamming Attacks on MIMO Channels, Bradley Dept of Electrical and Computer Engineering Virginia Tech, Arlington, VA,USA

[9] S. Jiang and Y. Xue (Eds.), Optimal Wireless Network Restoration under Jamming Attack, Proceedings of 18th International Conference on Computer Communications and Networks, (2009) August 3-9; Francisco, California.

[10] Tao Peng Christopher Leckie Kotagiri Ramamohanarao, Detecting Distributed Denial of

Service Attacks Using Source IP Address Monitoring, ARC Special Research Center for Ultra-Broadband Information Networks.

AUTHORS PROFILE

PUSHPHAS CHATURVEDI has received B.E. Degree in Information technology from RGTU MP and pursuing M.Tech in CSE from Amity university UP. His interested research areas are Network security, Mobile Computing and Wireless sensor network.

KUNAL GUPTA is Assistant Professor in Amity university UP and received M.Tech Degree from Punjabi University Patiala also he is pursuing Ph.D from Dr. C.V. Raman University CG. His areas of research are wireless networking and computer networking.