On the MAC Layer Jamming Techniques for IEEE 802.11e based Wireless Ad-hoc Networks

Deepak Nadig Anantha, Kushal S.P, Pradeep A.S
Research Technology Division (RTD)
SOLUTT Corporation
Bangalore, INDIA
deepak@solutt.com, pradeep@solutt.com

***Abstract*— Security forms an important part of wireless network communication systems. A wide variety of attacks can be performed on IEEE 802.11 MAC thereby compromising the security of the system and also leading to degradation of the system performance. The security attacks can be classified into different categories based on criteria/nature of the attack, domain or attack techniques used. In this work we study the performance of IEEE 802.11 MAC with CSMA/CA systems under various jamming attacks. The study will comprise of simulation of jamming attacks and its effect on various system parameters like throughput, latency, offered load, etc.**

Keywords-IEEE 802.11 DCF, IEEE 802.11 EDCA, Jamming attacks.

I. INTRODUCTION

Security forms an integral part of a wireless local area network communication. IEEE 802.11e MAC Layer standard is responsible for the coordination of transmissions between different nodes in a wireless local area network (WLAN). Since radio transmissions are broadcast, the implication is that transmissions with same frequency signals will interfere with each other and lead to collisions which result in data loss for both sources. IEEE 802.11 based systems use distributed coordination mechanisms to facilitate channel sharing among users. Two contention resolution algorithms are important in this regard, Distributed Coordination Function (DCF) and Point Coordination Function. It can be noted that PCF requires a centralized authority such as an Access Point (AP) or a Base Station (BS) to make decisions, where as DCF uses a carrier sensing mechanism like Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) in contention resolution among multiple wireless nodes. DCF defines three interframe spacing (IFS) values to accommodate priority based access to the radio propagation channel, DCF IFS, Short IFS and Arbitration IFS.

II. MAC LAYER FUNCTIONALITY OF IEEE 802.11E

IEEE 802.11e standard was designed to provide Quality of Service (QoS) provisioning at the MAC layer of the protocol stack. The QoS provisioning is achieved by a new distributed channel access mechanism called the Enhanced Distributed Channel Access (EDCA). EDCA defines four access categories with different levels of priorities. Each Access Category is differentiated using it own parameter set, particularly, Congestion window sizes and AIFS spacings. The categories are Voice, Video, Background and Best Effort, with Voice traffic assigned the highest priority. Each Access category is defined to use its own set of parameters namely: Congestion window sizes, Arbitration Inter Frame Spacing (AIFS) and Transmission Opportunity (TXOP) Limit. The table below presents the parameter specification for each access category.

TABLE I. VARIOUS MAC PARAMETERS FOR IEEE 802.11E EDCA

IEEE 802.11e EDCA Parameters			
AC	***CWMin***	***CWMax***	***AIFS***
Voice	7	15	2
Video	15	31	2
Background	31	1023	3
Best Effort	31	1023	7

The contention handling mechanism for EDCA is similar to IEEE 802.11 DCF. In EDCA, each channel access is prioritized and therefore every frame arriving at the MAC layer is distributed according to its priority. Four priority queues, each defined for a particular access category is used to provide service differentiation. There are four transmission queues, one for each AC. AIFS[AC] is the parameter which replaces the DIFS of DCF. Collisions can still occur if two or more nodes start simultaneous transmissions. The AIFS is determined by an AIFS Number called AIFSN. The AIFSN parameter is specified for each access categories in the IEEE 802.11e standard. The idea is to let the higher priority traffic access the medium using a lower backoff compared to the lower priority traffic. We can also use Contention window sizes to control and affect a service differentiation. As the duration of backoff for a particular station is a function of congestion window size, CW values can be used to provide service differentiation. The CW is doubled until it reaches a specified maximum value. In IEEE 802.11e, the minimum and maximum values for the CW are lower for high priority Access Categories. Therefore higher priority access categories are able to transmit more frequently, on average, than lower priorities

978-1-4244-9243-5/11/$26.00 © 2011 IEEE

since a backoff is always performed after a successful transmission.

III. RELATED WORK

[1] Employs contention window misbehavior to analyze the impact on QoS provisioning, to find if the user's gains are dependent in terms of transport protocol used and network size and to understand the gains for uplink and downlink traffic. One misbehaving node is used for each uplink scenario with the background priority being used by all nodes. In the downlink scenario, there is one misbehaving node and well-behaved nodes, all within hearing range of each other. TCP-ACK packets sent by the misbehaving node are used to influence on the rate of the received data. The achievable throughput of the misbehaving node with respect to well behaved nodes is analyzed. The main conclusion is that the misbehaving node can easily dominate the network in terms of throughput and delay. This occurs once the network reaches congestion, until which point the bad node's presence is not harmful. After reaching congestion, the bad node increases its throughput at the cost of the good nodes until saturation is achieved, in which the bad node has much more throughput than the average throughput of the good nodes. The type of transport protocol used having no influence on this type of behavior. Here, the total number of nodes in the network acts only to limit the maximum achievable throughput of the misbehaving nodes.

In [2] four parameters for jamming are used, namely, Priority distribution of packets generated, AIFSN, Minimum CW size and Maximum CW size. Staggering of AIFS times is used to create different priority levels. The first technique is aimed at causing packet collisions between nodes. This would cause greater backoff time which would leave the medium free for longer periods of time. In this way, it was hoped to make the network attack itself by reaching a point where the load was so great that collisions would be unavoidable. Collisions are ensured by transmitting only high priority packets while performing no backoff, CWmin = CWmax = 0, or even a negative backoff by additionally setting the AIFSN ≠ 2. The staggered AIFS times are combined with the backoff timers to create several priority levels which have the different opportunities to transmit. For example, a Best Effort packet with a backoff timer of 1 will attempt to transmit at the same time as a Video or Voice packet with a backoff timer of 2. The next technique used is the distribution of ACs (35% Voice, 35% Video, 20% Best Effort, and 10% Background). Negative backoff was ineffective as the jamming node was the only node always transmitting, so there was no chance of collision. But the use of no-backoff scenario leads to a reduction in the throughput. Both of these techniques are also highly visible to any node and easy to detect. Jamming nodes transmitting at higher priorities will have better chance at reduction of network throughput than jamming nodes transmitting at lower priority.

In [3], selecting backoff values from a different distribution with a smaller average backoff value is used, than the distribution specified by DCF (e.g., by selecting backoff values from the range[0, CW/4] instead of [0, CW] or by always selecting a fixed backoff of one slot). Using a different retransmission strategy that does not double the CW value after collision. In IEEE 802.11 protocol, a sender transmits an RTS (Request to Send) after waiting for a randomly selected number of slots in the range [0, CW]. Consequently, the time interval between consecutive transmissions by the sender can be any value within the above range. Hence, a receiver that observes the time interval between consecutive transmissions from the sender cannot distinguish a well behaved sender that legitimately selected a small random backoff from a misbehaving sender that maliciously selected a non-random small backoff. The idea is that two hosts may obtain the same throughput share over the long term, but one host may achieve significantly lower delay by misbehaving (the misbehaving host may immediately access the channel, but the well-behaved host may have a significant contention resolution delay, especially at higher loads). Two models are used, Persistent Misbehavior Model, captures the behavior of a misbehaving host that always misbehaves using a fixed strategy, and Adaptive Misbehavior Model, captures the behavior of a misbehaving host which changes the magnitude of misbehavior based on the magnitude of penalty assigned by the receiver.

The performance of the system in terms of achievable throughput as a function of increasing number of nodes is analyzed to calculate average throughput of well-behaved hosts and the misbehaving host throughput. The proposed solution assumes that the IEEE 802.11 access points (receivers) are well behaved. Misbehavior occurs when a sender deviates from the assigned backoff, with the penalty of higher backoff in the next transmission. However it is unsuitable as it requires changes to the widely deployed IEEE 802.11 standard which is not feasible.

The work in [4] analyzes how IEEE 802.11 throughput varies as a function of jammer rate. Various models are developed for jamming. Jammers are classified into four categories, based on sensing capabilities and their ability to react to a medium state. The four categories are (i) *Channel-Oblivious & memoryless*: make jamming decisions without sensing the channel, (ii) *Channel-Oblivious & stateful jammers*: do not have access to the channel state, (iii) *Channel-Aware & memoryless jammers*: one jamming rate for each possible state of the channel and (iv) *Channel-Aware & stateful jammers*: which senses the medium and transmits a jamming pulse with a specified probability. The authors perform prototype experiments using different jamming parameters and different payload sizes. The jammer is implemented on a software radio platform. Experiments are carried out under saturated throughput conditions using varying packet sizes and varying jamming rates. The impact of jamming rate, packet size and network size on saturation throughput is analyzed and it is found that the above jammer models perform better than simple continuous jammer.

IV. MOTIVATION

While the performance of MAC under ideal conditions and cooperative behavior of nodes is very good, situations where security of the data transfer has a greater priority might generate malicious users who wish to hamper or severely jeopardize the communication. Such malicious user nodes are called jammer nodes and the effect of jamming in IEEE 802.11 networks can pose significant issues relating to security as well as network performance. As IEEE 802.11e standard allows for easy modification of the Access Category parameters, a malicious user can exploit these features and reduce the network performance or exhibit greedy behavior. CSMA/CA relies on random deferrals and cooperative node behavior for contention resolution. As IEEE 802.11e provides incentives to users exhibiting cooperative behavior, a malicious user on the other hand need not conform to the standards and thus attempt to increase individual gain. Selfish behavior among nodes can be detected, if the objective is to increase personal gain. Detection of nodes deviating from the standard node protocol operation is necessary to ensure fairness in the allocation of resources. Selfish nodes can therefore result in resource exploitation which can eventually lead to disruption of the network system operation. Unlike Physical layer jamming attacks, the MAC layer attacks can be performed in an energy efficient manner. This can be achieved in a number of ways, for example, a jammer can selectively disrupt control packets continuously during a transmission. This not only leads to packet loss, but the effect is far more serious leading to significant reduction in overall network throughput. Also, working in an energy efficient manner ensures that a malicious node can perform attacks for a longer period of time and simultaneously operate in a stealthy manner, thereby making the detection process more complex. The volatile nature of the wireless access medium and the random nature of operation of the CSMA/CA protocols, can lead to creation of different network conditions for different stations. This is a serious problem, because the number of collisions in the network can be caused by either:

- Sudden increase in the number of nodes leading to increased network load
- A Jamming node exhibiting selfish behavior as a cause for collisions.

This makes the detecting process complex. Also due to the random nature of the backoff mechanism, it is harder to differentiate between the choice of a random backoff value and a manipulation as part of a misbehavior strategy.

V. PROBLEM FORMULATION

The Vulnerability of 802.11e to jamming attacks can be analyzed through the following methods:

A. *Attacks based on the manipulation of Medium Access Parameters*

These attacks can be performed in two ways:

1) Misbehavior in basic access methods based on contention:

Here, a two-way handshake mechanism is used by the stations. Terminals sense the channel and transmit only if it is idle. If the channel appears to be busy, terminals enter the CA mode by generating a random backoff interval. The backoff time is randomly chosen to minimize the probability of a collision and is called the contention window CW, where CW = [CWmin, CWmax], where CWmin and CWmax are called the maximum and minimum contention window sizes. After the backoff timer expires, the terminals try again and if the medium is still busy, the contention window is doubled and the terminal continues the deferrals until a maximum of $CWmax = 2m*CWmin$, where 'm' is the maximum backoff stage. By setting the CW window size lower than the specified ranges for each access category for a jamming node, we can increase backoff period for normal nodes, reducing access time and thus bringing about a reduction in throughput.

$$\text{AvgBackoff} = (\text{Avg.CW} + 1) * 1/2 \quad (1)$$

$$\text{AvgCW} = \text{Fn}(\text{CWmin}, \#\text{activestations}) \quad (2)$$

$$\text{AIF S[AC]} = \text{SIF S} + \text{AIF SN [AC]} * T_{slst} \quad (3)$$

Therefore, variation of CWmin and CWmax along with AIFS values for each access category can lead to bad behavior among nodes. Also, since collisions are directly proportional to CWmin sizes, and since an active station contends with at least one other station, the problem can be severe in a network with large number of active stations.

2) Misbehavior in RTS/CTS based access methods:

This method is similar to the above, except that a four way handshake mechanism is used. Corruption of RTS and CTS frames can affect stations by increasing the random deferral period and thus reducing medium access time, resulting in the reduction of achievable throughput. Also since RTS/CTS messages are control messages and hence smaller in size, corruption of these messages requires smaller packets to be transmitted by the jammer, making the jamming process more energy efficient.

B. *Network Scenarios*

The network consists of eight nodes and an access point in the center. The nodes are placed at equidistant locations from the access point. All the nodes are placed well within the transmission range and therefore there is no hidden terminal problem in this scenario.

All the nodes are operating within a grid of 500m by 500m. The channel propagation model used is the two ray ground model. RTS/CTS is enabled and the RTS Threshold is set to 128 bytes. All the nodes use a UDP agent at the transport layer and a Constant Bit Rate generator traffic source which is transmitting packets of size 1472 bytes at a constant interval of 0.0001 seconds. The data rate and the basic rate are both set to 54Mbps conforming to the 802.11g standard.

1) Variation of AIFS to reduce Backoff times:

Access categories for each node can be assigned through the use of four priority queues which use the standard parameter values defined in Table1. Modifications are made in the AIFS values of each AC to reduce backoff times. The Table 2 shows the variation of AIFS for each AC used to achieve throughput gain. This staggering of AIFS values to change backoff timers can cause different priorities to use different transmission opportunities. For example, AC[3] with a Backoff timer of 1 will transmit at the same time as AC[0] or AC[1] thereby creating more contention among access categories, causing more collisions and thereby reducing network throughput. The above scenario can then be repeated with two jamming nodes to further reduce the throughput of the system.

TABLE II. VARIATION OF AIFS FOR EACH ACS IN 802.11E

AC	*AIFS (Actual)*	*AIFS (Jammer)*
Voice	2	0 – 1
Video	1	0 – 1
Background	3	0 – 2
Best Effort	7	0 – 6

2) Misbehavior using Contention Window Cheating:

Since Contention window sizes affect the backoff times for a particular access category, Reduction in CW sizes for higher ACs can have drastic effects on the network throughput. This is a serious issue as use of two jammer nodes with reduced contention windows can cause the starvation of lower priority traffic.

3) Misbehavior using RTS/CTS:

A jamming node can continuously send RTS frames to the AP. The AP replies with a CTS Packet, which is heard by neighboring nodes. The jammer therefore gains continuous access to the channel. Also RTS/CTS frames can be damaged by using a jamming node which can transmit packets of smaller sizes during the contention period. The Jammer can resort to two techniques in this regard, first being transmission of uniform sized packets both continuously and at periodic intervals, and second being the transmission of variable sized packets both continuously and at periodic intervals. Therefore the optimal packet sizes for transmissions by well-behaved nodes in the presence of jammers need to be explored.

VI. SIMULATION RESULTS

We analyze the effects of variation in AIFS values for each Access Category. The AIFS value for each category is varied as per the ranges given in Table 2. For AC[0], we find that any reduction in AIFS values to one from the standard specification can result in significant reduction in throughput by upto 50% as seen in figure 1. Use of two jammer nodes can further reduce the achievable throughput as seen in figure 2. It is to be noted that a setting of AIFS value to zero can result in further degradation of achievable throughput in the network. Next we look at the AC[1], and the effect of variation in AIFS values. First we set the AIFS value to '1' and then to '0' Here we note that, for AIFS = 1, although the variation causes the degradation in throughput for Video traffic, it does not however significantly impact the highest Access Category, AC[0]. But AIFS = 0 causes reduction in achievable throughput across all access categories.

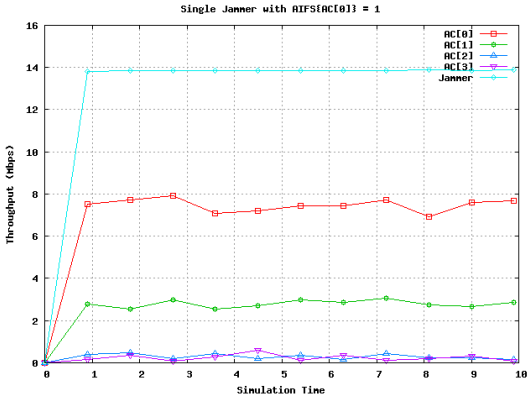

Figure 1. Variation in achievable throughput for a jammer with AIFS{AC[0]}=1

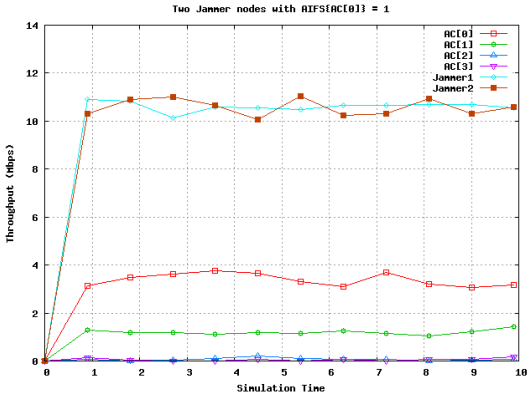

Figure 2. Variation in achievable throughput for two jammers with AIFS{AC[0]}=1

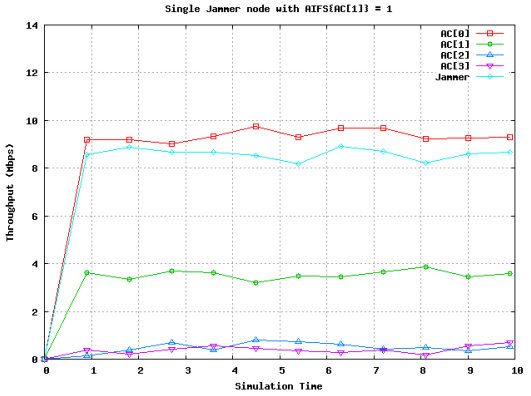

Figure 3. Variation in achievable throughput for a jammer with AIFS{AC[1]}=1

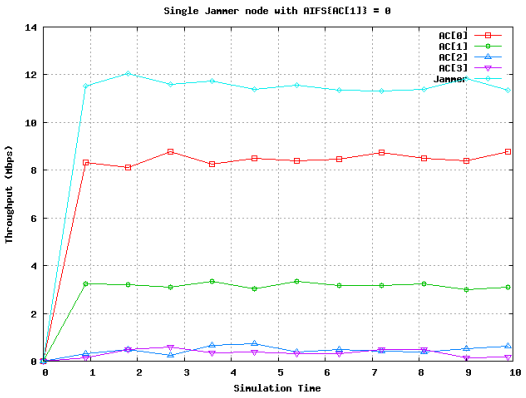

Figure 4. Variation in achievable throughput for two jammers with AIFS{AC[1]}=0

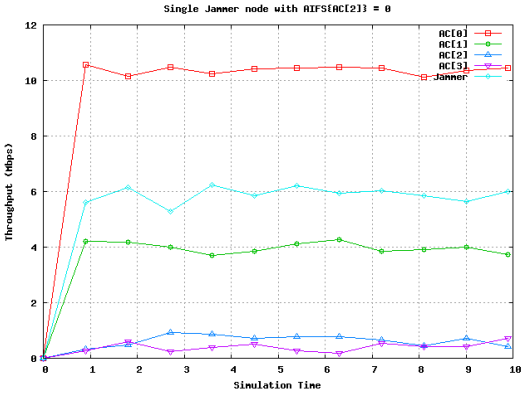

Figure 5. Variation in achievable throughput for a jammer with AIFS{AC[2]}=0

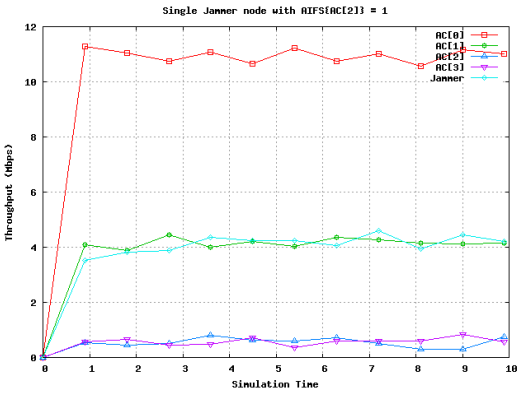

Figure 6. Variation in achievable throughput for a jammer with AIFS{AC[2]}=1

The results for a network with one jammer are shown in figures 3 and 4. The same procedure is repeated for AC[2]=0,1 and 2, and results are shown in figures 5, 6 and 7. We see that, any variation in lower AC categories will mostly impact the throughput of well behaved nodes in the same category. However, it does not have any impact on the achievable throughput of the highest access category.

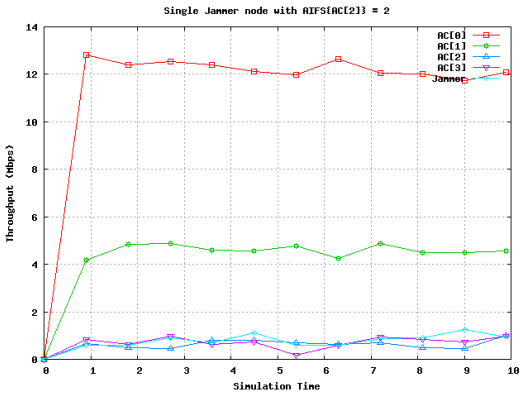

Figure 7. Variation in achievable throughput for a jammer with AIFS{AC[2]}=2

VII. CONCLUSIONS

The performance of Single Jammer node and two jammer nodes are analyzed for an IEEE 802.11e system in a single hop ad-hoc configuration. We find that jammers accessing the network at higher priority levels have the ability to significantly affect the maximum achievable throughput for the network and eventually lead the non misbehaving nodes in the network to starvation. However the effect is reduced for jammers accessing the network at lower priority levels.

REFERENCES

[1] Szott, S.; Natkaniec, M.; Canonico, R.; Pach, A.R., "Impact of Contention Window Cheating on Single-Hop IEEE 802.11e MANETs," Wireless Communications and Networking Conference, 2008. WCNC 2008. IEEE , vol., no., pp.1356-1361, March 31 2008-April 3 2008

[2] Thuente, David J.; Newlin, Benjamin; Acharya, Mithun, "Jamming Vulnerabilities of IEEE 802.11e," Military Communications Conference, 2007. MILCOM 2007. IEEE, vol., no., pp.1-7, 29-31 Oct. 2007

[3] P. Kyasanur and N.H. Vaidya, "Selfish MAC Layer Misbehavior in Wireless networks", IEEE Transactions on Mobile Computing, Volume 4, Number 5, September/October 2005.

[4] Bayraktaroglu, E.; King, C.; Liu, X.; Noubir, G.; Rajaraman, R.; Thapa, B, "On the Performance of IEEE 802.11 under Jamming" INFOCOM 2008. The 27th Conference on Computer Communications. IEEE , vol., no., pp.1265-1273, 13-18 April 2008

[5] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," presented at the ACM MobiHoc, Urbana-Champaign, IL, May 2005.

[6] Raya, M.; Aad, I.; Hubaux, J.-P.; El Fawal, A. DOMINO: Detecting MAC Layer Greedy Behavior in IEEE 802.11 Hotspots Mobile Computing, IEEE Transactions on , vol.5, no.12, pp.1691-1705, Dec. 2006

[7] Sun, H., Hsu, S., and Chen, C Mobile Jamming Attack and its Countermeasure in Wireless Sensor Networks In Proceedings of the 21st international Conference on Advanced information Networking and Applications Workshops - Volume 01 (May 21 - 23, 2007).

[8] Wei Chen, Danwei Chen, Guozi Sun, Yingzhou Zhang Defending Against Jamming Attacks in Wireless Local Area Networks Autonomic and Trusted Computing, Springer 2007