Jamming DoS in IEEE 802.11 WLANs

Sunitha Azad[1], Eitan Altman[1], Majed Haddad[2]

[1]INRIA, Sophia-Antipolis, France
[2]LIA, University of Avignon, France
email: {sunitha.azad, eitan.altman, majed.haddad}@inria.fr

Abstract—**In this paper, we consider an intelligent malicious mobile that can send signals which would cause interference to the users that communicate with an Access Point (AP). The attack is based on the well known anomaly of IEEE 802.11 in which a single connection with low signal to noise ratio causes the throughputs of all connections to decrease [1]. The attacker tries to exploit this anomaly by jamming a single node in the cell. The rate of that particular node reduces and thus the throughput of all the hosts transmitting at higher rate is degraded below the level of the lower rate. The jammer tries to maximize the throughput degradation by driving the SINR below the SINR threshold reception and placing itself at its optimal position. We analyze the impact of jamming on the system throughput especially from the perspective of jammer's utility. Extensive simulations are conducted to analyze the performance of the jammer on 802.11 WLANs.**

I. Introduction

Today, wireless LANs (WLANs) are widely deployed throughout the world. The IEEE 802.11 technology is particularly attractive due to its low cost and ease of deployment, as well as need to support high bandwidth applications. However, since accessing wireless media is much easier than tapping a wired network, security becomes a serious concern when implementing any wireless network. There are hundreds of articles that deal mainly with confidentiality and authentication related security attacks. Wireless communication is exposed to various denial of services attacks at all protocol layers due to the open and shared nature of wireless medium. In wireless networks, Denial of Services (DoS) attacks are difficult to prevent and protect against. They can cause a severe degradation of network performance in terms of achieved throughput. The performance of a wireless network or a service degrades on DoS, depends on many factors such as location of malicious nodes, their traffic patterns, fairness provided in the network resources. Jamming is the most traditional technique to prevent wireless communication. In the jamming attack, an attacker injects a high level of noise into the wireless system which significantly reduces the signal to noise and interference ratio (SINR) and reducing the probability of successful message transmissions/receptions. Jamming and counter jamming measure techniques has gained more attention in recent research as well as industrial application due to the vulnerability of wireless medium and its potential damaging capability.

Our focus in this paper is on the jamming attacks on IEEE 802.11. In particular, we are concerned with the jamming attacks for establishing or maintaining the connectivity in the system. Jamming can be malicious, aiming at preventing wireless communication in an area. Jamming is any attack to deny service to legitimate users by generating noise or false protocol packets or legitimate packets but with spurious timing. This could lead to congestion due to data that is either retransmitted or transmitted on erroneous routes only to be dropped at a later time. Some of these issues are addressed in [2]. In [3], the authors propose the use of promiscuous mode wherein a node overhears the transmission of its neighbors and infers if the behavior and responses are normal. However, this overhearing may be very much dependent upon other transmissions in the vicinity and the MAC protocol in use.

II. System Model

Consider n active nodes in a single cell IEEE 802.11 WLAN contending to transmit data. The transmission buffer of each node is assumed to be saturated. We further assume that all nodes use the same backoff parameters. We assume the decoupling approximation [4] which says that from the point of view of a given node, the number of attempts by the other nodes in successive slots are i.i.d. binomial random variables with parameters $(n-1)$ and β. It is assumed that the decoupling approximation and the ensuing fixed point analysis in [4], yield an accurate estimate of the attempt rate. A single cell scenario in WLAN consists of an Access Point and a set of nodes operating at power level P. Node could also be the AP. We also assume that the length of the packets of all the nodes is also the same. The transmission rate of all the nodes is assumed to be same. Thus, the average throughput of a node i is considered for the case of absence and in the presence of the jammer and the results are compared and analyzed for various jamming attack scenarios.

We study the situation when one or more nodes are jammed (at most one node from a set). The jamming can refer to the entire network or only a specific node or link. We derive adequate throughput formulas based on the seminal work of [4]. These analytical models are used to quantify the impact of jamming on 802.11 WLANs.

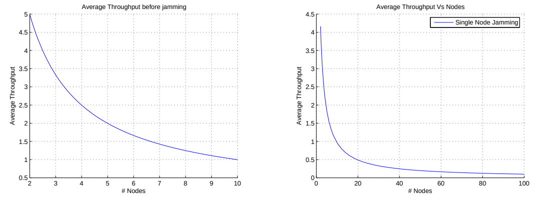
More specifically, consider two nodes in a single cell with a jammer in the same cell. Assume that the jammer wants to jam the two nodes in the cell and also the jammer to be positioned in between these two nodes. The distance between the two nodes is known. Assume that the jammer moves between these two nodes i.e., from one node to another.

VALUETOOLS 2012, October 09-12, Cargèse, France

DOI 10.4108/valuetools.2012.250348

III. Evaluation Results

As stated before, *the average throughput over an 802.11 LAN can be measured based on the amount of transferred data and the required transfer time*. If there is at least one host with a lower rate, a 802.11 cell presents a performance anomaly: the throughput of all the hosts transmitting at higher rate is degraded below the level of the lower rate. We compute the average throughput of a node without and with jamming. Due to the lack of space, these computations are omitted. The average throughput of a node i without and with jamming is shown in Fig. 1(a) and Fig. 1(b).



(a) Average throughput before jamming.

(b) Average throughput with single node jamming.

Fig. 1. Average throughput vs. Nodes

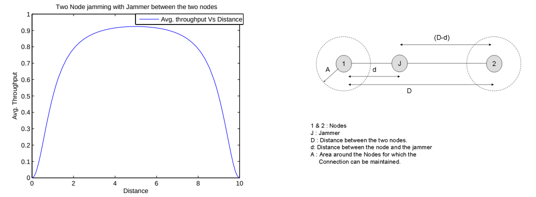
A. Optimal Jammer Location

The goal of the attacker is to maximize the degradation of throughput of the system. Hence it is indeed necessary to find the optimal jammer location in order to obtain maximum average throughput degradation. It was observed during evaluation that the optimal jammer location would be at a distance close to the node (almost d=0). Under such situation, the links of the node get corrupted and after some retries the node gets disassociated from the cell.

The objective of the attacker (jammer) is to drive the signal to noise ratio of the node below the threshold that is just sufficient to establish/maintain the connection. In order to find the optimal jammer position other than the origin of the node, we assume the SNR to be just below the threshold. The threshold depends on the type of service utilized. For the purpose of examination, we assume the threshold to be 1Mbps. With this threshold, the optimal position of the jammer is found. The jammer is located in between the two nodes. We assume the distance between the two nodes to be $D = 10$. The optimal jammer location is found by varying the jammer location between the two nodes. The system model is shown in Fig. 2(b). Fig. 2(a) below shows the results achieved for the considered throughput model.

B. Average throughput vs. distance

From Figs. 2(a) and 2(b), it is observed that the optimal jammer position would be at a distance close to the node (almost d=0). Under such situation, the links of the node get corrupted and after some retries the node get disassociated from the cell. It is seen that the average throughput is maximum when the jammer is exactly between the two nodes and the average throughput is minimum when the jammer is near to either of the two nodes.



(a) Average throughput vs. distance.

(b) Optimal jammer position with threshold 9.6Mbps.

Fig. 2. Two node jamming.

C. Optimal jammer location

Fig. 2(b) shows that the optimal position for the jammer for the 802.11b with threshold 1Mbps for n=5, is at 1.4 and 8.5m. With jammer being at these positions, the connectivity can be maintained. It is also observed during evaluation that for N=10, 20 and above, it is difficult to obtain the optimal location for the jammer because the average throughput of node is less than the threshold. This is because as the number of nodes in the cell increases, the average throughput of a node decreases.

IV. Conclusion

In this paper, we have investigated the impact of jamming under various scenarios on the basic model throughput, with a motivation to exploit the anomaly of IEEE 802.11 in which the node with low signal to noise ratio degrades the throughput of all the nodes transmitting at higher rate. From the numerical results, it was noticed that the node with lower bit rate degraded the throughput of all other nodes transmitting with higher bit rate. This is because the node with lower bit rate captures the channel for a long time and thus penalizing other nodes of higher bit rate. We have then investigated the optimal jammer position for establishing or maintaining the connectivity of the nodes in the cell/system. It was observed from the numerical results that the optimal location for the jammer to maintain the connection was at the threshold. Below the threshold, the links of the nodes get corrupted and finally the nodes get disconnected/disassociated.

References

[1] "M. Heusse, F. Rousseau, G. Berger-Sabbatel and A. Duda", *Performance Anomaly of 802.11b*, IEEE Infocom 2003, pp. 836-843.

[2] "P. Papadimitratos and Z. J. Haas", *Secure Routing for Mobile Ad Hoc Networks*, SCS Communication Networks and distributed Systems Modeling and simulation conference(CNDS 2002), San Antonio, TX, January 27-31, 2002.

[3] "S. Marti, T. Giuli, K. Lai and M. Baker", *Mitigating Routing Behavior in Mobile Ad Hoc Networks*, Proceedings of Mobicom 2001, Rome.

[4] "Ramaiyan, Venkatesh and Kumar, Anurag and Altman, Eitan", *Fixed point analysis of single cell IEEE 802.11e WLANs: uniqueness, multistability and throughput differentiation*, Proceedings of the ACM SIGMETRICS international conference on Measurement and modeling of computer systems, Banff, Alberta, Canada, 2005.