Impact Factor (SJIF): 3.632

International Journal of Advance Research in Engineering, Science & Technology

e-ISSN: 2393-9877, p-ISSN: 2394-2444

(Special Issue for ITECE 2016)

DDRS algorithm over DoS Attack in Wireless Communication Due to Jammers

Prof. Bhaumik Machhi[1]

[1]Computer Science & Engineering, SLTIET

Abstract. Jamming attacks in wireless communication are subset of denial of service (DoS) attacks in which malicious nodes block legitimate communication by causing intentional interference in networks. To better understand this problem, we need to discuss and analyze, in detail, various techniques for jamming and anti-jamming in wireless networks. There are two main aspects of jamming techniques in wireless ad hoc networks: types of jammers and placement of jammers for effective jamming. To address jamming problem, various jamming localization, detection and countermeasure mechanisms are studied. Finally, we describe the open issues in this field, such as energy efficient detection scheme and jammer classification. Main objective of this paper to overcome the effect of DoS in wireless communication by improving packet delivery ratio, throughput, Control Packet Overhead. Here DDRS algorithm provides detection as well as recovery from DoS attack. this system provides variation in energy consumption, delay variation, throughput variation on node. DDRS provides protection against Jamming techniques vary from simple ones based on the continual transmission of interference signals.

Introduction

Security is one of the critical attributes of any communication network. Various attacks have been reported over the last many years. Most of them, however, target wired networks. Wireless networks have only recently been gaining widespread deployment. At the present time, with the advances in technology, wireless networks are becoming more affordable and easier to build. Many metropolitan areas deploy public WMANs for people to use freely. Moreover, the prevalence of WLANs as the basic edge access solution to the Internet is rapidly becoming the reality. However, wireless networks are accompanied with an important security flaw; they are much easier to attack than any wired network. The shared and easy to access medium is undoubtedly the biggest advantage of wireless networks, while at the same time is its Achilles' heel. In particular, it makes it extremely easy for an adversary to launch an attack. The goal of traditional DoS attacks is to overflow user and kernel domain buffers. However, such "brute-force" jamming techniques, which mainly exploit PHY and MAC layer vulnerabilities, can be detected easily. Jammers have responded by employing more intelligent ways to accomplish jamming task in order to evade detection. They exploit vulnerabilities at the higher layers of the network stack.

DoS

As DoS attacks become one of the most threatening security issues, the need to detect this type of attack is increasing. DoS is not just a "game" played for fun by some attackers, it has become an effective weapon for cyber war or for so called "hacktivist" groups. In general, detection is required before the spread of a DoS attack. DoS detection is often part of a wider intrusion detection system (IDS). An IDS is best defined as software or hardware used to detect unauthorized traffic or activities that are against the allowed policy of a given network. Intrusion detection is not a new research field, with one of the earliest published IDS papers in 1980 by Anderson in 1987, Denning provided a structure for researchers working on IDS. IDS can be classified based on the serving component (the audit source location) as either host-based, network-based or a combination of both. In a host-based IDS the audit information, such as application and operating system log files, are monitored while the network traffic is monitored in a network-based IDS. The host-based is usually located in a single host while the network-based system is usually located on machine separate from the hosts that it protects. Hybrid intrusion detection systems combine both the network and host-based systems. The rest of this paper is organized as follows. We focus on DoS attacks in wireless ad hoc networks. More specifically, we investigate attacks at the medium access control layer. An attacker causes congestion in the network by either generating an excessive amount of by itself, or by having other nodes generate excessive amounts of traffic. In wireless networks, DoS attacks are difficult to prevent and protect against. They can cause a severe degradation of network performance in terms of the achieved throughput and latency.

Challenges

We start out with listing possible DoS attacks and identifying possible methods to alleviate these attacks. Next, we investigate in detail the vulnerabilities of the IEEE 802.11 MAC protocol that make DoS attacks easy. We identify that the capture effect and the lack of fairness that arise when this MAC protocol is used may be especially exploited to cause disruptions in accessing important services. To our knowledge this work is one of the first attempts to characterize and quantify the effects of DoS attacks at the MAC layer in ad hoc networks. To gain an understanding of how fairness may prevent some of the DoS attacks, we emulate a perfectly Fair MAC protocol1. We simulate various scenarios to understand the local and global effects of various types of DoS attacks with both the IEEE 802.11 MAC protocol discuss possible solutions to overcome or alleviate these effects. Our results show that the extent to which 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. we provide the background in terms of prior work in the areas of security and intrusion detection in ad hoc networks. We also provide a description of the IEEE 802.11 MAC protocol and briefly describe some of the fairly well known problems that arise when it is deployed in ad hoc networks. We identify possible DoS attacks and suggest methods that may be used to overcome them.

Objective

- Detecting jammers
- Reduce the effect of DOS attack
- Improve wireless communication

We describe some of the most harmful attacks that can be launched by a jammer. We develop such as one system, to show the effect of the dos attack. In our proposed system, the normal client and server process is initially depicted, then the attack is launched manually to show how the dos attack affect the normal client/server process.

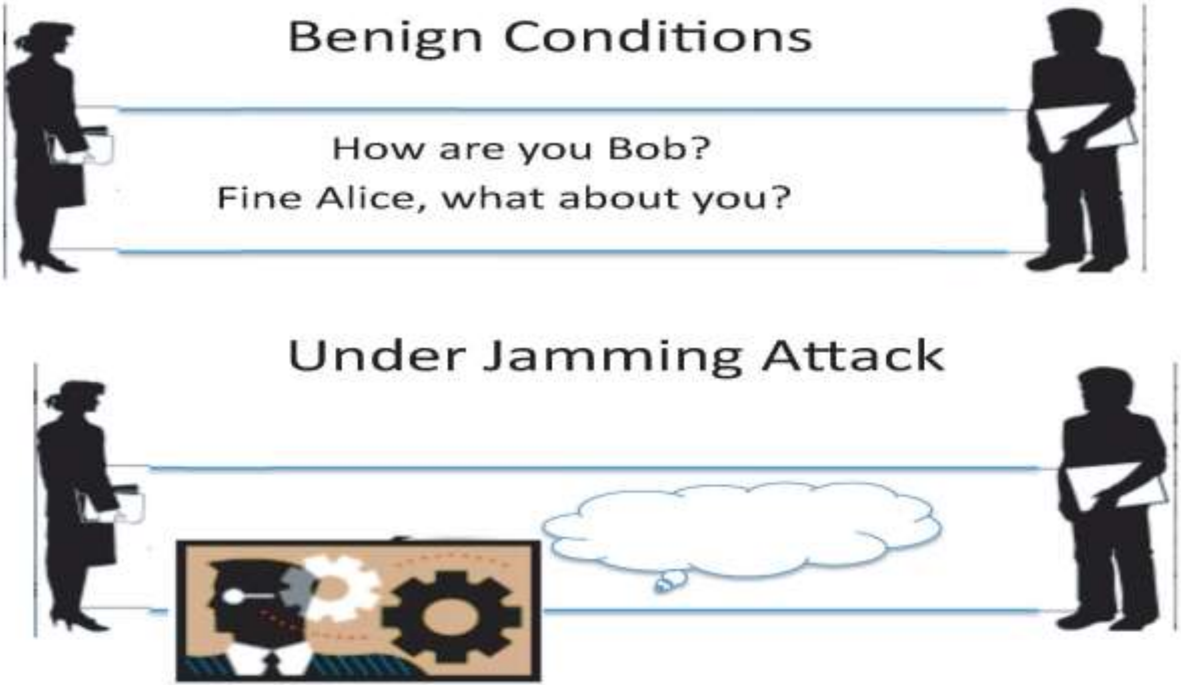

Figure 1.1 Pictorial representation of a jamming entity.

First, we start by formally defining jammers. We will adopt the definition given by Xu : “We define a jammer to be an entity who is purposefully trying to interfere with the physical transmission and reception of wireless communications”. A pictorial representation of the jammer is given in Figure 1.Before describing the various jamming models, it is important to refer to some criteria and metrics that are used to characterize the attack model.

Jammers: Constant jammer

Emits radio signals all the time at the wireless medium. The signals that he/she emits are totally random. They don’t follow any underlying MAC protocol and are just random bits. The goal of this type of jammer is either for a legitimate user to sense all the time the channel busy and as a result the sender will never get access to the channel to send data or to pose interference to a node that has send out data and as a result to corrupt the packets sent out. Similar in some way to the constant jammer is the deceptive jammer. Its similarity lays in the fact that deceptive jammer also sends out constantly bits, however this time the bits are not random.

dXA(inch)	**PSR (%)**	**PDR (%)**
38.6	74.37	0.43
72.0	99.57	93.57

Table 2.1 Effect of constant jammer

Deceptive jammer

Continually injects regular packets to the channel without any gap between the transmissions. This has as a result a legitimate user to believe that there is an legitimate transmission going on and as a result this node will remain at the receive state even if it has data to send out. One problem that the previously described jammers can face is this of energy failure. They emit signals to the wireless medium all the time so their life time is restricted.

dXA(inch)	**PSR (%)**	**PDR (%)**
38.6	**0.0**	**0.0**
54.0	0.0	0.0

Table 2.2 Effect of deceptive jammer

Random jammer

Jams for tj seconds and sleeps for ts seconds. At the jamming period the jammer can follow any of the models that we have described since now or any of the models that we will describe in following sections. By changing tj and ts we can achieve different levels of effectiveness and power saving. All those jamming models that we mentioned and can be found with more details at target mostly at the transmission of a packet. They try to avoid the transmission of a packet from the sender.

dXA(inch)	**PSR (%)**	**PDR (%)**
38.6	**79.45**	**0.26**
54.0	80.43	99.00

Table 2.3 Effect of random jammer

Reactive jammer

On the other hand a jammer can target the reception of the a packet. So a reactive jammer is sensing the channel all the time and when he/she senses a packet to be sent, transmits a radio signal in order to cause collision and as a result corruption of the data that the packet transfers.

dXA(inch)	**PSR (%)**	**PDR (%)**
38.6	**99.00**	**0.00**
54.0	100.0	99.24

Table 2.4 Effect of Reactive jammer

The effectiveness of those types of jammers is being augmented by the current standards for wireless data communications . The PHY of IEEE 802.11 or Bluetooth makes them an easy target for DoS. These PHY layers don't support error correction. This has as a result even if a jammer sends as less bits as it cans in order to corrupt one bit, the whole packet will not pass the CRC check as there is no error correction scheme. The reason for this is that wireless systems had been designed in order to be resilient to non-malicious interference and to noise. But as we can see a jammer can use efficiently low power in order to jam a whole communication.

We have reviewed some recent research paper for wireless communication. It is clear from the papers reviewed below that currently the area of wireless communication has already been well studied by many researchers and several algorithms are used for wireless communication.

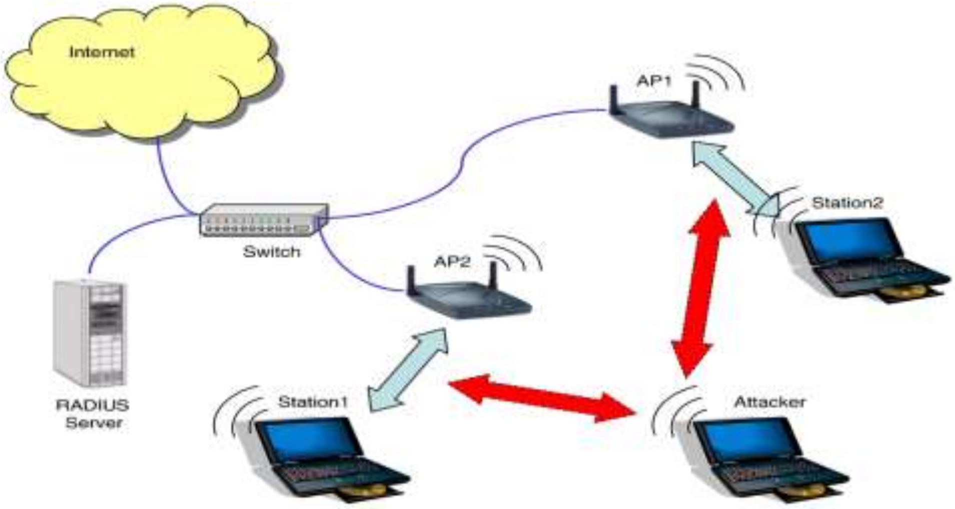

Fig 2.1 Wireless Communication

Intrusion Detection Schemes

As per[11] Traditional techniques directly borrowed from Intrusion Detection Systems (IDS) for wire line networks, face practical limitations when considered for wireless networks. For example, signature based IDSs will not be efficient, since many WDoS attacks take place at the MAC layer. Thus, it is difficult to isolate sequences of packets and feed them as an input is such systems. In addition, the power constraints of a mobile user are such that make it relatively difficult to build such an IDS, which is required to store a great number of attack signatures. The rest of this section presents studies related to intrusion detection in wireless networks.

PHY layer Intrusion Detection

The PHY layer jamming is the most easy to implement jamming technique. The basic idea for detecting such attacks is very simple: *the presence of jamming radio signals at the receiver can affect the received signal strength*. Along these lines, the authors in and propose a series of basic detection methods. Signal Strength Measurements show that simple statistical metrics, such as the average received signal power, are not useful in discriminating between the jamming scenarios and the normal states of the network. In particular, it is hard to select a threshold that can distinguish between jamming and normal network conditions (e.g., congestion). Use spectral discrimination techniques in order to enhance detection. However, as shown in the paper, their scheme can detect only some types of jammers. In particular, it can detect the constant and the deceptive jammers, but it fails to detect the reactive and the random jammers.

Carrier Sensing Time In a CSMA network - e.g.802.11 - the MAC protocol requires a node to first sense the channel to be idle for a specific amount of time prior to transmitting. Under normal conditions and for a specific network, the distribution of this *carrier sensing time* is known and can be acquired either theoretically or empirically. Monitoring for deviations from the *benign* distribution, can be used for jamming detection. However, the effectiveness of this scheme is similar to that of the scheme that relies on signal strength measurements; it can detect a constant and a deceptive jammer, but not a random or a reactive jammer. The random jammer spends time sleeping without affecting the carrier sensing time (during these periods), while the reactive jammer is not affecting transmissions at all.

Measuring the PDR In and show that PDR measurements can help detect all types of PHY layer jammers. It is shown that even in a highly congested network the PDR remains as high as 78%. On the other hand, under a jamming attack, the PDR drops significantly. Therefore, a simple threshold can be set to distinguish between a congested network state and a state induced by a PHY layer jammer. However, there are still situations where PDR measurements can lead to false alarms. For example, such scenarios may arise when there is a network failure (such as a battery failure); the node under consideration stops sending packets and PDR drops to 0. In addition, poor link quality at the receiver (i.e. low SNR) can drastically reduce PDR.

Intrusion Prevention Schemes

As per[16] their name suggests, Intrusion Prevention Systems try to prevent jamming by either *avoiding* or *fighting* against the malicious entities.

Frequency Hopping

Frequency hopping has been traditionally employed in order to overcome the presence of a jammer. Frequency hopping can be either reactive or proactive. In the reactive case, when a node detects that it is jammed it switches to a different channel and sends a beacon message on the new channel, announcing its presence. Its non-jammed neighbors will sense its absence and will change their bands of operation to check if their lost neighbor has sent beacons announcing its presence on a different channel. If not, then they assume that the node just moved away. Conversely, if they sense a beacon, they will inform the other nodes in the network to change channels. At this point, there are two possible approaches. The first approach would be for the entire network to eventually migrate to the new, non-jammed channel.

Spatial Retreats

Mobile nodes affected by the jammer can move away from their initial positions to avoid jamming signals. In brief, when a node detects that it is being jammed, it tries to (a)*escape* from the jammed area (*evasion phase*) and (b) *stay connected* with the rest of the network (avoiding partition with the rest of the network - *reconstruction phase*).In particular, when a node senses that it is being jammed, it starts moving out of the jammed region; at the same time it executes a detection algorithm trying to stay connected with its previous neighbors

Fighting Reservation Based DoS attacks

As mentioned earlier, an adversary can send an RTS packet, requesting the medium for a period of M slots, while it does not have actual data to send. This results in the under utilization of the medium; no packets are on the air but the legitimate users cannot access it.

Securing our Network from a Layered Jamming Attack

This model tries to exploit existing patterns in protocols related to the size, the interface time periods and the sequence of the packets being exchanged. A simple way to make a network resilient against such intelligent jamming attacks is to obfuscate these patterns when possible. As an example, for obfuscating the packet size consistencies a simple padding technique can be used; every control packet can be made to be of the same size, making it more difficult for a jammer to recognize such packets. This padding only has a very small impact on throughput as explained in.

Simple PHY Layer Techniques:

The jamming-to-signal ratio, captured by Equation 3, provides various insights on possible ways to fight against jammers. For instance a legitimate transmitter can increase its transmission power. As another example the distance between the transmitter and the receiver ,i.e., the length of the link, can be reduced, thus boosting the received signal strength. Both of this approaches are brute force techniques. They result in a decreased jamming-to-signal ratio and hence, can be expected to improve performance.

Directional Antennas:

This results in an increased antenna gain from the transmitter to the receiver and vice versa, decreasing as a consequence the jamming to signal ratio. The same effect can also be achieved by using sectored antennas, or other types of smart antennas that focus the beam's power on the receiver. Using directional antennas, can also help at mitigating jamming effects at a CSMA/CA transmitter. In particular, based on the radiation patterns of the antenna used, jamming interference coming from directions other than the direction of transmission does not stimulate transmission deferrals due to carrier sensing; in other words packets can still be transmitted despite the presence of a jammer.

Spread Spectrum:

The above methods do not perform any processing of the transmitted signals; they just change the transmission parameters of the signals (e.g. power, directionality, etc.). However, there are PHY layer signal processing techniques used as jamming countermeasures. The most well known techniques are based on the use of Spread Spectrum communications.

Characteristics of various jamming models

Jamming Model	Implementation Complexity	Energy Efficiency	Stealth Efficiency	Level of DoS	Anti−Jamming Resistance
Constant [10]	Low	Low	Low	High	Medium
Deceptive [10]	Low	Low	Low	High	Medium
Random [10]	Low	Adjustable	Medium	Adjustable	Medium
Reactive [10]	High	High	Medium	High	Low
Packet Corruption [11], [21]	Average	High	Average	High	Low
Narrow-band [20]	High	High	High	High	Average
DIFS Waiting [11], [21]	Medium	Medium	Medium	High	Low
Identity Attacks [22]	Medium	Average	Average	High	High
Layered Attacks [18]	High	Low	Average	High	Medium

Table 2.5 Characteristics of various jamming models

Jamming Efficiency Metrics

In order to quantify the extent to which the jammer satisfies the above criteria, we need to define metrics that capture the jammer's behavior. For describing these metrics, we will use simple scenarios with one transmitter (*Tx*) and one receiver(*Rx*).Introduce the following two, widely used, metrics (PSR and PDR). Packet Send Ratio (PSR):Lets assume that the MAC layer of *Tx* has n packets for transmission. Due to jamming interference, only m (n ≥ m) of these packets can eventually be transmitted. PSR is then defined to be:

$$PSR = \frac{m}{n} = \frac{Packets\ Sent}{Packets\ Intended\ To\ Be\ Sent} \qquad (1)$$

PSR is an easily computed measure which intuitively captures the effectiveness of the jammer towards a transmitter employing carrier sensing as its medium access policy. The jamming signals can render the medium busy due to carrier sensing and as a result the transmission queues of *Tx* will get filled up quickly. Packets arriving at a full queue will be dropped. Moreover, depending on the semantics of the MAC protocol employed, transmissions for packets at the head of the queue can eventually expire and the packets themselves get discarded. The PSR metric can quantify such jamming effects.

Packet Delivery Ratio (PDR):Lets suppose that Rx receives m packets sent out from *Tx*. However, from these m packets only q were successfully delivered to the higher layers of *Rx*. A successful reception means that the packet successfully passed the CRC (Cyclic Redundancy Codes) check. In contrast to PSR, PDR captures the effectiveness of the jamming attack towards *Rx*. The PDR is defined as follows (note that if *m*= 0then PDR is defined to be zero):

$$PDR = \frac{q}{m} = \frac{Packets\ That\ Pass\ The\ CRC}{Packets\ Received} \qquad (2)$$

Jamming-to-Signal Ratio**:** Traditionally, jamming strength(mostly referring to PHY layer jamming) is measured by the jamming-to-signal ratio given by the following equation.

$$\frac{J}{R} = \frac{P_j G_{jr} G_{rj} R_{tr}^2 L_r B_r}{P_t G_{tr} G_{rt} R_{jr}^2 L_j B_j} \qquad (3)$$

Where with the subscript j we refer to the jammer, with r to the receiver and with t to the transmitter. *Px*is the transmission power of node *x*, *Gxy* is the antenna gain from node *x*to *y*, *Rxy* is the distance between nodes *x* and *y*, *Lr* is the communication link's signal loss, *Lj* is the jamming signal loss and *Bx* is node's *x* bandwidth. Connectivity index: The presence of jammers in an ad hoc wireless network can hurt connectivity (i.e., disrupt the existence of routes between all wireless nodes in the network).To capture the effect of jamming on the connectivity of a wireless ad hoc network. introduce the connectivity index.

Let *G = (V,E)* be the directed connectivity graph representing the multi-hop ad hoc network after removing the jammed links. Let *G*= (*V*,*E*) be the transitive closure of *G*. The connectivity index of *G* is defined to be:

$$Connectivity\ Index = \frac{|E'|}{\frac{|V|(|V|-1)}{2}} \qquad (4)$$

From the definition of the transitive closure, E contains all the pair of nodes of the graph for which, there exists a path that connects them. The connectivity index is simply the ratio of the number of such pairs to the number of all possible pairs of nodes in the network. As a result, a connected graph has a connectivity index of 1, while a graph partitioned in two connected graphs of equal size, has a connectivity index 0.5.

Proposed System

Dynamic Detecting & Recovery System (DDRS) algorithm

- Detect the number of packets coming from a particular source to a particular destination
- Keep a track on the number of packets
- If the number of packets given to a particular destination by a particular source exceed a particular threshold then discard the packets from that particular connection
- Repeat this for all the nodes in the network
- Jammers would be avoided because any connection which is used by a jammer would pass and waste lot of packets at runtime.

DDoS attacks detection algorithm:

1. Set the sampling frequency as *f*, the sampling period as *T*, and the grouping thresholds as GT_T and GT_S.

2. In the router after aggregation of traffic, sampling the network flows come from the upstream routers.

3. Calculate the numbers of packet which has various recognizable characteristics (such as the source IP address or the packet's size, etc.) in each sampling time interval.

4. Calculate in parallel the probability distributions of the sampled network flows.

5. Calculate in parallel the values of the total variation and the similarity coefficient among each of the pair.

6. If the value of the total variation of any two distributions is more than the lower bound of the grouping threshold GT_T (1.1045) and the value of the similarity coefficient is less than the upper bound of GT_S (0.7220), then the system detected the DDoS attacks from Flash crowds, and begins to raise alarms and discard attack packets.

7. If the value of total variation is located in the grouping threshold GT_T (the lower bound: 0.5921, and the upper bound: 1.1045) and the value of the similarity coefficient is located in GT_S (the lower bound: 0.7220, and the upper bound: 0.8708), then the system detected the DDoS attacks from Normal network flow, and begins to raise alarms and discard attack packets.

8. If the value of the total variation of any two distributions is less than the upper bound of the grouping threshold GT_T (0.5921) and the value of the similarity coefficient is more than the lower bound of GT_S (0.8708), then the system detected the Flash crowds from Normal network flow, and begins to raise alarms.

9. Otherwise the router forwards the packets to the destination or the downstream routers.

10. Return to step 2.

Conclusion.

Here in DDRS algorithm for improving the effect of DoS attack in case of jammers. Other prevention schemes require properties that might not be applicable in realistic scenarios. Given the already widespread deployment of wireless systems, solutions that require large scale changes(and cannot be applied for example through a software patch) are unrealistic. DoS is one of the main security threats in the Internet. Defending against DoS becomes a necessary step that must be considered by the companies and ISPs. IDS is used to detect different types of intruders including DoS/DDoS attacks. By using hybrid probability metrics to detect DDoS attacks, and through experiment and simulation gives that the proposed metric can not only detect DDoS attacks from the normal flows, but also can recover from DoS attack. In future work Dynamic Detecting & Recovery System (DDRS) which have dynamic algorithm which will detect packets from source to destination & keep track on the number of packets. DDRS discard the packets from that particular connection & adjust their channel settings of APs to avoid RF interferers. Establishment of system that effectively works against each jammers & graph system.

REFERENCES

[1] Q.Huang, H.Kobayashi, and B.Liu. “Modeling of distributed denial of service attacks in wireless networks,” in *IEEE Pacific Rim Conf.Commun., Computers and Signal Process., vol. 1, pp. 113-127, 2003.*

[2] Y.Zhang and W.Lee, “Intrusion detection in wireless ad hoc networks,” in *ACM MobiCom 00*, Boston, MA.

[3] S.Bhargava and D.P.Agrawal, “Security enhancements in AODV protocol for wireless ad hoc networks,” in *VTC 2001 Fall*, vol. 4, Oct. 7-11,2001.

[4] Y.Zhang, W.Lee, and Y.-A.Huang, “Intrusion Detection Techniques for Mobile Wireless Networks,” *in ACM J. Wireless Net., vol. 9, no. 5, Sept.2003, pp. 545-56.*

[5] R. Gummadi, D. Wetheral, B. Greenstein, and S. Seshan, “Understanding and mitigating the impact of RF interference on 802.11 networks,”in*ACM SIGCOMM, 2007.*

[6] J.Bellardo and S.Savage, “802.11 denial-of-service attacks: Real vulnerabilities and practical solutions,” in *Proc. USENIX Security Symposium03*,Aug. 03.

[7] M.Raya, I.Aad, J-P.Hubaux, and A. El Fawal, “DOMINO: Detecting MAC layer greedy behavior in IEEE 802.11 hotspots,” in *Proc. ACMMobiSys, Boston (MA), USA, 2004.*

[8] P.Kyasanur and N.Vaidya, “Detection and handling of MAC layer misbehavior in wireless netwoks,” in *Proc. International Conf. DependableSyst. Netw.*, June 2003.

[9] P.Kyasanur and N.Vaidya, “Selfish MAC layer misbehavior in wireless networks,” in *IEEE Trans. Mobile Comput.*, vol. 4, no. 5, Sept./Oct.2005.

[10] K. Pelechrinis, G. Yan, S. Eidenbenz and S.V. Krishnamurthy, “Detectionselfish exploitation of carrier sensing in 802.11 networks,” in *IEEEINFOCOM 2009*, Apr. 2009.

[11] M. Li, I. Koutsopoulos, and R. Pooverdan, “Optimal jamming attacks and network defenses policies in wireless sensor networks,” in *Proc.IEEE INFOCOM* 2007.

[12] A. Wald, “Sequential Analysis,” Wiley 1947.

[13] M.D.Aime, G.Calandriello, and A.Lioy, “A wireless distributed Intrusion Detection System and a new attack model,” in *Proc. 11th Symp. Comput.Commun.*, 2006, ISCC 06.

[14] V.Chatzigiannakis, G. Androulidakis, K. Pelechrinis, S. Papavassiliou,and V. Maglaris, “Data fusion algorithms for network anomaly detection: classification and evaluation,” in *ICNS 2007,* Athens, Greece.

[15] W.Xu et al, “Channel surfing and spatial retreats: Defenses against wireless denial of service,” in *Proc. 2004 ACM Wksp. Wireless Security*,2004, pp.80-89.

[16] Denial of Service Attacks in Wireless Networks:The Case of Jammers Konstantinos Pelechrinis, Marios Iliofotou and Srikanth V. Krishnamurthy