Classification of Jamming Attacks and Detection and Prevention Techniques in Local Wireless Networks

Darko Pajkovski, Nikola Rendevski, Zoran Kotevski, Tome Dimovski

***Abstract*— This study focuses on the detection techniques and classification of jamming attacks in wireless networks. This is more difficult, because open nature of this medium leaves vulnerability to multiple threats. Jamming attacks often appear at physical and MAC layer but sometimes cross-layer and involves different methods and techniques. Some of these jamming techniques are surveyed to understand the problem of blocking legitimate communication by causing intentional interference in the network. In this case, there are two main aspects of jamming techniques in wireless network: types of jammers and placement of jammers for effective jamming. Various jamming detection, and localization mechanisms are studied towards detection and jamming classification. Basically, a jammer can be elementary or advanced depending by functionality. Both of these are divided into two sub-groups.**

Keywords: Jamming, wireless networks, placement of jammers, detection jammers, localizing jammers.

I. INTRODUCTION

With the rapid development of WLAN over the last decade WiFi technology and communications have evolved rapidly and have been widely deployed and utilized in both residential and enterprise networks. The growth of wireless technologies and networks over recent years have created more security vulnerabilities and resulted with more incidents and security attacks to both enterprise and customers. This type of various security threats such as jamming, flooding, collisions due to dynamic nature and node characteristics become critical issue [1]. While WiFi brings brilliant convenience to the social life, some kinds of criminal activities and attacks in wireless communication protocols and devices have significantly increased. The WiFi forensics technology has become a significant problem to be solved both in WiFi and in computer forensics.

Jamming attack is the most efficient way to stop services, disrupt the wireless communication and it is very difficult and complex to be appropriately detected. Any interferences at the transmissions on wireless networks are due to jamming attack. A jammer can easily listening the shared medium and transmitting in the same bandwidth as network, without particular hardware. Usually, attacks occur a physical layer such as radio jamming (RF) however at MAC layer; an attacker in 802.1x protocol manipulates with increasing the delay time or sending false data [2].

Jamming detection has become an important issue with main goal to improve security in wireless networks. Signal-to-noise ratio has been used to detect jamming. Jamming in wireless networks represents disruption of existing wireless communications with changing the intensity of the signal-to-noise ratio at receiver sides through the transmission of interfering wireless signals.

Figure 1 Example of wireless network

One of the key issues that make jamming a big threat is that they are easy to launch, but difficult to detect. In the case of WiFi even special devices not be needed as computers can be turned into jammers. There are several cases of jamming incidents that indicate the criticality of the issue like; cars parked near a store could not be unlocked remotely using key fobs, that showing presence of jammer attack that interrupted the key fob signals [3]. Another case involves an explosion of an oil pipeline, cyber-attacks that involved jamming of satellite communications to prevent transmission of alerts in Baku-Tbilisi. It appears that jamming will remain to be a major issue, with the growing up of the Internet of Things devices, the use of wireless communications is rapidly increasing in many fields and jamming attacks is becoming an important threat. Jamming can be done at different levels, from interfering transmission to blocking legitimate communications.

To understand how a jammer works and how to avoid jamming in wireless network, we will describe some different aspects of wireless network jamming. First, types of existing jammers and how network can be jammed in various ways using different types of jammers. We discuss in details different types of jammers, the optimal placements of jammers in order to achieve their affects. Then, it's necessary to use existing technologies to localize jammers in wireless networks. Finally, the most challenging issue is how to deal with the jamming attacks when we cannot know exactly when may start/end.

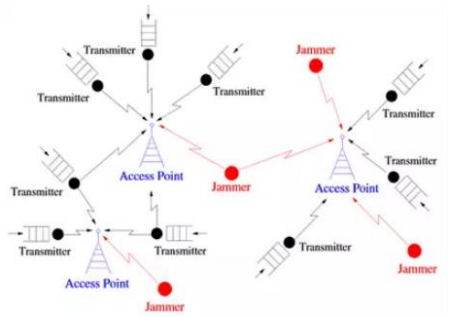

Figure 2 Jamming attacks on wireless network

In this paper we discuss for different types of jammers and their optimal placements also classification to identify the type of a particular jammer. This paper is organized as follows: Section 2 shows the security layer in wireless networks. In Section 3 we discuss different measurements that might be used to detect a radio interference attack. Section 4 describes the definition of jamming attacks and classifications of jammers. In Section 5 we give some details of how to localize jammers in wireless networks. Section 6 describes various protocols for detection and prevention of jamming attacks.

II. NETWORK LAYER IN WIRELESS NETWORKS

Network layer in wireless networks is divided into 5 layers as shown in Figure 3. Jammers launch attacks in both lower layer because it's easier to generate there, their characteristics and nature of wireless networks allow it. Characteristics are with open medium, dynamic topology and hidden terminal.

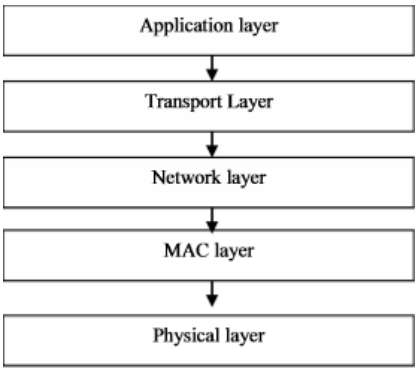

Figure 3 TCP/IP Stack

III. JAMMING CHARACTERISTICS AND METRICS

In this section, we define the characteristic of a jammer's behavior, and then we describe metrics that can be used to measure the effectiveness of a jamming attack. In this case, the metrics are strongly related to the ability of a radio device to either send or receive packets.

After numerous studies for jamming attacks, the exact definition of this type of attack remains unclear. A common conjecture is that a jammer continuously emits RF signals to fill a wireless channel, and legitimate traffic will be completely blocked [4, 5]. They may start interference as soon as it detect a transmission on the channel, and may remain quiet when the channel is idle. A jammer is purposefully trying to interfere with the physical transmission and reception of WiFi communications because all jamming attacks and their communications aren't compliant with MAC protocols. A jammer can achieve the main goal to interfere the legitimate WiFi communications by preventing a real traffic source from sending out packet, or by preventing the reception of packets. If X and Y is two legitimate participants, and Z denote a jammer, for many reasons X and Y may be unable to send out packets. One of them is that Z can continuously emit a signal on the channel so that X can never sense the channel as idle. The other one can be keep sending out packets from Z and force X to receive as junk all the time. If X successfully sends out packets to Y, but Z blast a radio transmission to corrupt the message that Y receives. The following metrics is to measure the effectiveness of a jammer:

- **Packet Send Ratio** (PSR): The ratio of packets that are successfully sent out by a legitimate traffic source to the total number of packets received. PSR is measured at the transmitter side. MAC sub-layer acts as an interface between two sides and some of the wireless networks employ some form of carrier-sensing multiple access control before transmission packets. That means that the channel must be sensed as being in an idle state for some random time before X can send out a packet. Different MAC protocols have different definitions on an idle channel, some of them compare the signal strength measured with fixed threshold, others may base threshold on the noise level on the channel. If we have many packets buffered in the MAC layer, the newly arrived must be dropped. Also, the time for staying in MAC layer is limited and packets that are too long will be discarded. If X intends to send out *n* messages but only *m* of them go through, the PSR is *m/n*.

- **Packet Delivery Ratio (PDR):** It is a ratio of packets that are successfully delivered compared to the number of packets that have been send out by the sender. We have unsuccessful delivery, if the packet that is send out by X, Y may not be able to decode it correctly. The PDR can be compute on multiple ways such as measuring at the receiver Y by calculating the radio of the number of packets that pass the CRC check with respect to the number of packets received. The other way to calculate at the sender X by having Y send back acknowledge packet. Also PDR is defined to be 0, if no packets are received.

- **Carrier sensing time:** The time a station has to wait for the channel to get idle and then start the transmission.

- **Signal strength:** The signal power that is measured on the receiver end and can be used as a detection parameter [6]. Also, there are two approaches that are used to characterize the variation in signal strength: 1) average value of signal strength in time window; 2) spectral discrimination technique.

IV. JAMMING TECHNIQUES AND FUNCTIONALITY

As we describe before, jamming attacks makes intentional radio interferences to harm WiFi communications in various ways like corrupting signal received at receivers, keeping communicating medium busy, causing a transmitter to back-off whenever it senses busy WiFi medium. Jamming attacks are mostly at the physical or MAC layer but sometimes cross-layer are possible too. In this section we describe various types of jammers and their functionality. Also, jamming effect of jammers depends on its radio transmitter power, location and influence on the network. The main goal of a jammer is to make the jamming as effective as possible. Basically, a jammer can be elementary or advanced depending upon its functionality. The elementary jammers are divided into two sub-groups: proactive and reactive. In other hand, advanced jammers are also classified into two sub-groups: function-specific and smart-hybrid.

A. Proactive jammer

There are three basic types of proactive jammers: constant jammer, deceptive jammer and random jammer. All of them transmits jamming signals all time whether or not there is data communication in WiFi network. They sends packets on the channel it is operating on or some random bits, putting all the others nodes on that channel in non-operating modes, because they doesn't switch channels, operates and performing jams on only one channel until its energy wasted.

1) Constant jammer: continuosly produces high-power noise that represents random bits without following CSMA (Carrier Sense Multiple Access) protocol. According to this mechanism, a legitimate node has to sense the status of the WiFi medium before transmitting. Specifically, the constant jammer doesn't wait for the channel to become idle before transmitting, because prevents legitimate nodes from communicating with each other by causing the WiFi media to be constantly busy. This type of attacks are easy to detect, easy to launch but can damage network commnunications to the point that no one can communicate at any time,

Identify applicable sponsor/s here. If no sponsors, delete this text box (*sponsors).*

2) Deceptive jammer: continuosly send illegitimate packets so that the channel appears busy to the legitimate nodes. The difference between this jammer and a constant jammer is that a constant jammer sends random bits continuously while a deceptive jammer sends regular packets which appear legitimate to the receiver. The other advantage compared to a constant jammer it is more difficult to detect because it sends legitimate packets instead of random bits. Deceptive jammer is also energy inefficient due to the continuous transmission like constant jammer.

3) Random jammer: intermittenly sends either random bits or regular packets into WiFi networks. Opposite to the above constant jammer and deceptive jammer it aims at saving energy. It operates randomly in both sleep and jam intervals. It sleeps for a certain time of period and then becomes active for jamming, it acts as a constant or reactive jammer. The both sleeping and jamming time periods are either fixed or random. This jammer doesn't follow any MAC protocol. The PDR increases when the sleep interval increases and packet size decreases. The ratios between sleeping and jamming time can be manipulated to adjust tradeoff between efficiency and effectiveness.

B. Reactive jammer: The three models described above are active jammers and they try to block the channel irrespective of the traffic pattern on the channel. As we decribe before active jammers are usually effective and keep te channel busy all the time, but its also easy ti detect. An alternative approach to jamming WiFi communications is to employ reactive method. In this type of jammer is not necessary to jam the channel all time when nobody is communicating. In other words a jammer stays quiet when the channel is idle but starts transmitting radio signal when it sense activity on the channel. A reactive jammer targets on compromising the reception of a message. It is less energy efficient than random jammer because the jammer's radio must continuously be on in order to sense the channel. The primary advantage on reactive jammer is that it is much more difficult to detect than proactive jammer because the PDR cannot be determined accurately in practice. There are two different ways to implement a reactive jammer.

1) Reactive RTS/CST jammer: jams the WiFi network when it senses a request-to-send (RTS) message is received by receiver. RTS/CST jammer starts jamming the channel when RTS is sent. When the RTS message is sent from a sender, receiver will not send back clear-to-send (CST) reply because the RTS message is distorted. In this way, the sender will not send any packets beacause it belives the other side is busy with another transmission. In other way, the jammer can wait the CTS reply to be sent by the receiver and jams them. The result will also be the same because the sender not sending data and the receiver always waiting for data.

2) Reactive Data/ACK jammer: jams the WiFi network by corrupting the transmissions packets or acknowledgement (ACK) packets. This jammer starts jamming the channel when sense a data transmission at the transmitter end. In this case, the jammer can corrupt data packets, or it will waiting the data packets reach the receiver and then corrupt the acknowledgement packets. The result of both corruptions data transmissions and ACK messages will lead to re-trasnsmissions at the sender end. In the first way when the data packets are not received correctly at the receiver side, data packets have to be re-transmitted. In the second way, if the sender doesn't receive the ACK message it believes that something is wrong at the other side like buffer overflow and it will re-transmit the data packets.

C. Function-specific jammers

Function-specific jammers are implemented by having a pre-determined function. They can work as proactive and reactive jammers on a single channel to conserve energy or sometimes to jam multiple channels and maximize the jamming throughput irrespective of the energy usage. At one moment in time a jammer can jam a single channel not fixed to that channel, can change their channels according to their specific functionality. There are three basic types of specific-functionality jammers: follow-on jammer, channel-hopping jammer and pulsed-noise jammer.

1) *Follow-on jammer:* hops over all available channels very frequently about thousand times per second and jams all channels for a short period of time. The jammers in modern systems do not know the frequency of next hop. These jammers are able to follow even a pseudo-random frequency hopping sequence, because after the transmitter hops away from the previous frequency, the jammer scans the entire band in search for the new frequency and starts to jam there. Increases hopping rate doesn't change the bit-error-rate of the communications signal and that is an advantage on follow-on jammers. Due to its high frequency, hopping rate is more effective against same anti-jamming techniques.

2) *Channel-hopping jammer:* can listen to and jam a single channel at a time and hops between different channels proactively. The jammer can determine instantaneously when it has hopped to some channel on which legitimate communication exists and then immediately jams this channel. This type of jammer has directly accessed to channels by overriding the CSMA method provided by the MAC layer. Characteristically for this type of jammers is that it can jam multiple channels at the same time. The jammer can check j channels in time $t\,j$. If we have a total of L channels the probability that the jammer has hit the right pseudo-random sequence after checking j channels is j/L for all $0 \leq j \leq L$.

3) *Pulsed-noise jammer:* is similar to the elementary proactive random jammer because can switch channels and jam on different bandwidths at different periods of time. Another advantage and similarity with random jammer is saving energy by turning off/on according to the programmed schedule. This jammer just like previous one can attack multiple channels and it can be implemented to simultaneously jam them.

D. Smart-hybrid jammers

The main goal of these jammers is to expand their congestion effect in the network they mean to jam. The name smart-hybrid comes from their power efficient and effective jamming nature. They also pay attention of themselves by conserving their energy. Additionally, they spend significant energy in the right place to hinder the communication bandwidth for the complete network or a major part of network in enormous systems. Every of this kind of jammer can be implemented as both proactive and reactive jammers.

1) *Control-channel jammers:* work in multi-channel networks by targeting the control channel to coordinate network activity [6]. If the jammer captures the hopping sequence of a compromised node, then by design this node can be identified. In this case the effectiveness of a jammer who gets knowledge from compromised node becomes unique to the effectiveness of a jammer who hops randomly between channels. Furthermore, future control channel can be obtained from the compromised nodes.

2) *Implicit jamming attacks:* are used the rate adaptation algorithm in WiFi networks, where the AP (Access Point) worries to the weak node by reducing its rate. During to this process the current AP spends much more time communicating with this weak node than the other nodes. When the jammers of these types jams a node which is communicating with the AP, the focus from the rate adaptation effect falls down on the jammed node while causing other clients to wait and suffer.

3) *Flow-jamming attacks:* can involve several jammers throughout the network to jams packets with purpose to reduce traffic flow. These attacks are launched by using information from the network layer [7]. There are two jammer models with centralized control and non-centralized model. The first model with centralized control, minimum power to jam a packet is computed then the jammer acts accordingly. The second model a non-centralized, where each jammer shares some

information with neighbor jammers to increase efficiency. In Table 1 we summarize the features of all the above jamming technique. We represent every type of jammer in this table, is it a proactive or reactive, energy efficient or not, and their ability of jamming single or multiple channels. Also, there are some jamming approaches that combine multiple of these techniques such as implementation of a single-tone reactive jamming [8], using the variations of jammers to analyze the performance of the best jamming approach in 802.11 networks [9]. In other hand, the [10] are using combination od jammers (reactive/random and multi-channel/pulsed-noise) and resulted with obtaining interrupt jamming, pulse jamming and scan jamming.

Jammer	*Proactive*	*Reactive*	*Energy efficient*	*Single channel*	*Multiple channels*
Constant	×			×	
Deceptive	×			×	
Random	×		×	×	
RTS/CTS jammer		×		×	
Data/ACK jammer		×		×	
Follow-on	×		×	×	
Channel hopping		×		×	×
Pulsed noise	×			×	×
Control channel	×	×	×	×	
Implicit	×	×	×	×	
Flow-jamming	×	×	×	×	×

Table 1 Classification of jammers

V. LOCALIZING JAMMERS

In this section the focus falls down on localization approaches and positioning of jammers. The localization approaches are divided into two groups: range-based and range-free. There is few work in this area because is very difficult to locate a jammer. Current techniques are described below:

- **Centroid-based schemes** [11] estimate the position of a jammer by averaging the coordinates of the jammed nodes. If the jamming has been detected, all affected nodes are marked as jammed and these nodes have information about their coordinates. In distributed network, better estimation can be obtained with increasing the network density. In this case if we increase network density the most probably is that jammed nodes are evenly distributed around the jammer.

- **Virtual force iterative approach** starts with a coarse estimation build upon the centroid scheme [11] and then re-estimate the jammer's position until is closely to the true location by computing the push and pull virtual forces. The real jammed region contains all jammed nodes but none of the boundary nodes. The virtual-force iterative approach will stop computing when the estimated jammed region covers all jammed nodes and all boundary nodes fall outside of the region.

- **Geometry covering based localization** is similar to centroid approach because computes the convex hull instead of the centroid. Then, uses the computed geometry to estimate jammer location from the convex hull [12]. Technique of finding the smallest circle completely contains a set of points given by the convex hull is to approximate the location of the jammer with high accuracy.

- **Light weight jammer localization** is gradient-based scheme with computing the PDR value [13] of two sides (sender and receiver) as a product of probability. The first computed probability is that the sender sensing the medium idle, then second is probability that the receiver will receive the data sent to it, and the third is probability that the sender will receive the ACK message. All third probabilities are computed independently by sending messages to its neighbors in order to obtain PDR.

- **Exploiting neighbor changes** [14] are using the least-squares (LSQ)-based algorithm to locate the jammer. The jammer's location is computed from the initial hearing range of the node and changes of node's hearing range. The assumption is that the initial value is known before the jammer starts computing. The equations of the algorithm are equal to the number of nodes whose hearing range changes and they are computed simultaneously.

VI. DETECTION AND PREVENTION OF JAMMING

Jamming is a very harmful and destructive attack, it is essential to have operative detection and recognition and necessary countermeasure against it. In this section we discuss some of existing schemes for detection and recognition jamming of basic types of jammers. For methods of detection and recognition we investigate the operational form specific, metric, overhead, charge, cost and implementation difficulty. Moreover, for this types of detection, countermeasure we examine the condition of network type and whether is knowledge required.

- **Ant system –** an evolutionary algorithm for recognition jamming [15] at the PHY layer and redirects communications to an appropriate destination node. It communicates a suggestion to test whether a DoS attack is true or not. By creating an agent traverse the network iteratively, the Ant system collects the information for multiple routes to a destination. The information collected is then stored in a list and will be used for redirection. Also, the information on energy and expanse are used to be sure of whether jamming is identified or not. The detection of jamming is true or not is based on checking the metrics like SNR, PDR, BER, energy, expanse, packet loss and putting them into a decision model. Then the system calculates the values between two given nodes and check probability is within a certain threshold, otherwise the network is jammed.

- **Channel searching and spatial retreat** provides migration to alternative channel when a jammer within range and lumps communication on a particular channel [16]. On other hand, spatial retreat moves mobile nodes from the location where they involve jamming to another safe location. The authors [16] investigate three situations: two-party communication, organization and networks. Here, the detection may be conducted at MAC layer using CSMA. On the validation of a jamming recognition channel changing or spatial retreat process is accomplished.

- **Hybrid system** is a mixture of anti-jamming defense techniques: base station repetition, base station evasion and multipath routing between origin paths [17]. The base station repetition implies that multiple simulated base stations are existed in the network. Evasion scheme denotes to the spatial retreat of a base station when jamming is detected. Multipath systems occur when there are multiple data paths between a node and a base station.

- **Game theoretic modeling** uses a clustering algorithm to recognize whether a node belongs to non-jammed cluster or jammed cluster based on the RTS, data, carrier sensing failure count or network allocator significance [18]. Game theory necessitates two players: the jammer and the display nodes. The determination of jammers is to maximize the denial of wireless channel to access the appropriate users while sincere nodes try to exploit their communication output. Display nodes use cross layer features for recognition of constant jammers by sensing the medium and for detecting of reactive jammers by typical retransmission rate of RTS/Data packets. This kind of nodes can act continuously or periodically.

- **Channel hopping** or switching from one station to another is the most popular countermeasure to jamming. Proactive channel hopping is the modest implementation. Multiple variations of channel hopping are present in [19]. The authors improve the effectiveness and efficiency of channel hopping by creating it sensitive, adaptive and code-controlled. In proactive channel hopping the present communication channel is altered after certain duration of time. This happens regardless of whether or not there is jamming.

- **Control channel attack prevention** in a wireless network manages channel custom where multiple channels are used to increase the network ability. To avoid jamming the authors in [6] purpose several bunch whereby each of them preserves its own control channel with a single hopping structure. At the advanced network level a jammer can jam the control channel by enchanting data from a compromised node about the protocol mechanism and cryptographic quantities. A jammer's capability to positively regulate the upcoming control channel from previously detected information is measured in evasion entropy.

- **Cross-layer jamming detection and migration –** can be completed either at the PHY layer or MAC layer; very infrequently it is done on the higher layers. There are certain circumstances where jamming detection is done using cross-layer approaches. The algorithm is created on PHY layer but usually uses the upper-layer security devices. A three-based approach is used to form the irregular hopping pattern. Any user can interpret the message the message transmitted by the sender using accurately one hopping pattern. When the jamming is detected the cover is detached and both the children of that root are added to the shield. The detection of jamming will be done when the source uses additional test designs during its transmission.

REFERENCES

[1] G. Thamilarasu, S. Mishra, R. Sridhar, "A Cross-layer approach to Detect Jamming Attacks in Wireless Ad Hoc Networks", IEEE Military Communications Conference 2006, Washington, D.C., October 2006

[2] Le Wang, Alexander M. Wyglinski. "A Combined Approach for Distinguishing Different Types of Jamming Attacks Against Wireless Networks." Proceedings of the 2011 IEEE Pacific Rim Conference on Communications, Computers, and Signal Processing (Victoria, BC, Canada), August 2011.

[3] https://www.techrepublic.com/article/wireless-jammers-cast-a-dark-shadow-on-iot-security/

[4] A. Wood, J. Stankovic, and S. Son. JAM: A jammed-area mapping service for sensor networks. In 24th IEEE Real-Time Systems Symposium, pages 286 – 297, 2003.

[5] W. Xu, T. Wood, W. Trappe, and Y. Zhang. Channel surfing and spatial retreats: defenses against wireless denial of service. In Proceedings of the 2004 ACM workshop on Wireless security, pages 80 – 89, 2004.

[6] Lazos L, Liu S, Krunz M (2009) Mitigating controlchannel jamming attacks in multi-channel ad hoc networks. In: Proceedings of the 2nd ACM Conference on Wireless Network Security, pp 169–180.

[7] Tague P, Slater D, Poovendran R, Noubir G (2008) Linear programming models for jamming attacks on network traffic flows. 6th International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks and Workshops pp 207–216.

[8] Wilhelm M, Martinovic I, Schmitt JB, Lenders V (2011) Short paper: reactive jamming in wireless networks: how realistic is the threat? In: Proceedings of the fourth ACM Conference on Wireless Network Security, pp 47–52.

[9] Bayraktaroglu E, King C, Liu X, Noubir G, Rajaraman R, Thapa B (2008) On the performance of IEEE 802.11 under jamming. In: IEEE the 27th Conference on Computer Communications, pp 1265–1273.

[10] Wood A, Stankovic J, Zhou G (2007) DEEJAM: Defeating energy-efficient jamming in IEEE 802.15.4based wireless networks. In: 4th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks, pp 60–69.

[11] Liu H, Liu Z, Chen Y, Xu W (2011a) Determining the position of a jammer using a virtual-force iterative approach. Wireless Networks 17(2):531–547.

[12] Sun Y, Wang X (2009) Jammer localization in wireless sensor networks. In: 5th International Conference on Wireless Communications, Networking and Mobile Computing, pp 1–4

[13] Pelechrinis K, Koutsopoulos I, Broustis I, Krishnamurthy S (2009b) Lightweight jammer localization in wireless networks: System design and implementation. In: IEEE Global Telecommunications Conference, pp 1–6.

[14] Liu Z, Liu H, Xu W, Chen Y (2011b) Exploiting jamming-caused neighbor changes for jammer localization. IEEE Transactions on Parallel and Distributed Systems To Appear

[15] Muraleedharan R, Osadciw LA (2006) Jamming attack detection and countermeasures in wireless sensor network using ant system. In: SPIE the International Society for Optical Engineering, vol 6248, p 62480G.

[16] Xu W, Wood T, Trappe W, Zhang Y (2004) Channel surfing and spatial retreats: defenses against wireless denial of service. In: Proceedings of the 3rd ACM Workshop on Wireless Security, pp 80–89.

[17] Jain SK, Garg K (2009) A hybrid model of defense techniques against base station jamming attack in wireless sensor networks. In: Proceedings of the 2009 First International Conference on Computational Intelligence, Communication Systems and Networks, pp 102–107.

[18] Thamilarasu G, Sridhar R (2009) Game theoretic modeling of jamming attacks in ad hoc networks. In: Proceedings of 18th Internatonal Conference on Computer Communications and Networks, pp 1–6.

[19] Yoon SU, Murawski R, Ekici E, Park S, Mir Z (2010) Adaptive channel hopping for interference robust wireless sensor networks. In: 2010 IEEE International Conference on Communications, pp 1–5.