Jamming and Anti-jamming Techniques in Wireless Networks: A Survey

Abstract: Because of the proliferation of wireless technologies, jamming in wireless networks has become a major research problem due to the ease in blocking communication in wireless networks. Jamming attacks are a 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.

Keywords: Jamming, anti-jamming, wireless networks, classification of jammers, placement of jammers, localizing jammers, detection of jammers, countermeasure for jamming.

1 Introduction

Wireless networking plays an important role in achieving ubiquitous computing where network devices embedded in environments provide continuous connectivity and services, thus improving human's quality of life. However, due to the exposed nature of wireless links, current wireless networks can be easily attacked by jamming technology. Jamming can cause Denial-of-Service (DoS) problem which may result in several other higher-layer security problems, although these are often not adequately addressed (Wood et al, 2007).

Jamming in wireless networks is defined as the disruption of existing wireless communications by decreasing the signal-to-noise ratio at receiver sides through the transmission of interfering wireless signals. Jamming is different from regular network interferences because it describes the deliberate use of wireless signals in an attempt to disrupt communications whereas interference refer to unintentional forms of disruptions. Unintentional interference may be caused by the wireless communications among nodes within the same networks or other devices (e.g. microwave and remote controller). On the other hand, intentional interference is usually conducted by an attacker who intends to interrupt or prevent communications in networks. Jamming can be done at different levels, from hindering transmission to distorting packets in legitimate communications.

To understand how a jammer attacks wireless networks and how to avoid jamming to achieve efficient communication, we investigate three different aspects of wireless network jamming: 1) types of existing jammers, 2) protocols for localizing jammers and 3) jamming detection and countermeasure. First, a network can be jammed in various ways using different types of jammers. To avoid jamming in networks, it is important to know how a jammer works. So we discuss in detail different types of jammers, e.g. proactive, reactive, function-specific and hybrid-smart jammers, and the optimal placements of jammers in order to achieve the best jamming affects. Then, we investigate existing technologies for localizing jammers in networks. Finally, we look into how to deal with the jamming problem. This is the most challenging issue where much research has been conducted. For instance, one simple solution is to apply high transmission power on jammed channels rendering this jamming to be less of a threat. Another countermeasure of jamming is to use directional antennas instead of omnidirectional antennas. However, none of existing detection or countermeasure methods can address all types of jammers without giving false alarms. Therefore, more research is required for detecting and avoiding different types of wireless network jamming.

Although network jamming is usually considered a critical threat, Gollakota and Katabi (2010) proved that jamming can be friendly too. They used jamming as a defense to counteract eavesdropping attacks. Particularly, a node will be jamming oneself on its PHY (physical) layer so that a snooper cannot demodulate a legitimate signal. Then, receivers jam the transmitted signal by flipping certain bits in the packets. Similarly, Gollakota and Katabi (2010) use jamming on wireless channels (instead of PHY) to avoid eavesdropper's attack.

There are three main contributions in this article. First, from the perspective of an attacker, different types of jammers and their optimal placements are discussed. The classification chart can be used to identify the type of a particular jammer. Second, from the security point of view, we analyze existing anti-jamming techniques in detail and classify them into different categories. The summary table can be used to analyze protocols based on different parameters such as network conditions, detection metrics, and countermeasure overhead. Third,

we elaborate on key issues of existing countermeasures of jamming attacks and point out future research challenges in avoiding jamming. Existing surveys either focus on jamming techniques (Pelechrinis et al, 2011) or countermeasures of jammers Mpitziopoulos et al (2009), but our work integrates both topics.

The organization of this paper is as follows: Section 2 describes the definitions of jamming attacks, classifications of jammers, and jammer-placement strategies for effective attacks. In Section 3, we give the details of how to localize jammers in networks. Section 4 describes various protocols for detection and countermeasures for jamming attacks. It provides analyses and discussions on existing schemes. Critical issues in existing protocols and research challenges are described in Section 5. We conclude our work in Section 6.

2 Jamming Techniques

Jamming makes use of intentional radio interferences to harm wireless communications by keeping communicating medium busy, causing a transmitter to back-off whenever it senses busy wireless medium, or corrupted signal received at receivers. Jamming mostly targets attacks at the physical layer but sometimes cross-layer attacks are possible too. In this section, we elaborate on various types of jammers and the placement of jammers to maximize the jammed area.

2.1 Types of jammers

Jammers are malicious wireless nodes planted by an attacker to cause intentional interference in a wireless network. Depending upon the attack strategy, a jammer can either have the same or different capabilities from legitimate nodes in the network which they are attacking. The jamming effect of a jammer depends on its radio transmitter power, location and influence on the network or the targeted node. A jammer may jams a network in various ways to make the jamming as effective as possible. Basically, a jammer can be either elementary or advanced depending upon its functionality. For the elementary jammers, we divided them into two sub-groups: proactive and reactive. The advanced ones are also classified into two sub-types: function-specific and smart-hybrid. The detailed classification of different jammers can be found in Fig. 1.

2.1.1 Proactive jammer

Proactive jammer transmits jamming (interfering) signals whether or not there is data communication in a network. It sends packets or random bits on the channel it is operating on, putting all the others nodes on that channel in non-operating modes. However, it does not switch channels and operates on only one channel until its energy is exhausted. There are three basic types of proactive jammers: constant, deceptive and random. From here on, whenever we use proactive jammers it can mean all these three.

Constant jammer emits continuous, random bits without following the CSMA protocol (Xu et al, 2005). According to the CSMA mechanism, a legitimate node has to sense the status of the wireless medium before transmitting. If the medium is continuously idle for a DCF Interframe Space (DIFS) duration, only then it is supposed to transmit a frame. If the channel is found busy during the DIFS interval, the station should defer its transmission. A constant jammer prevents legitimate nodes from communicating with each other by causing the wireless media to be constantly busy. This type of attack is energy inefficient and easy to detect but is very easy to launch and can damage network communications to the point that no one can communicate at any time.

Deceptive jammer continuously transmits regular packets (Xu et al, 2005) instead of emitting random bits (as in constant jammer). It deceive other nodes to believe that a legitimate transmission is taking place so that they remain in receiving states until the jammer is turned off or dies. Compared to a constant jammer, it is more difficult to detect a deceptive jammer because it transmits legitimate packets instead of random bits. Similar to the constant jammer, deceptive jammer is also energy inefficient due to the continuous transmission but is very easily implemented.

Random jammer intermittently transmits either random bits or regular packets into networks (Xu et al, 2005). Contrary to the above two jammers, it aims at saving energy. It continuously switches between two states: sleep phase and jamming phase. It sleeps for a certain time of period and then becomes active for jamming before returning back to a sleep state. The sleeping and jamming time periods are either fixed or random. There is a tradeoff between jamming effectiveness and energy saving because it cannot jam during its sleeping period. The ratios between sleeping and jamming time can be manipulated to adjust this tradeoff between efficiency and effectiveness.

2.1.2 Reactive Jammer

Reactive jammer starts jamming only when it observes a network activity occurs on a certain channel (Xu et al, 2005). As a result, a reactive jammer targets on compromising the reception of a message. It can disrupt both small and large sized packets. Since it has to constantly monitor the network, reactive jammer is less energy efficient than random jammer. However, it is much more difficult to detect a reactive jammer than a proactive jammer because the packet delivery ratio (PDR) cannot be determined accurately in practice. According to (Pelechrinis et al, 2011), the following are two different ways to implement a reactive jammer.

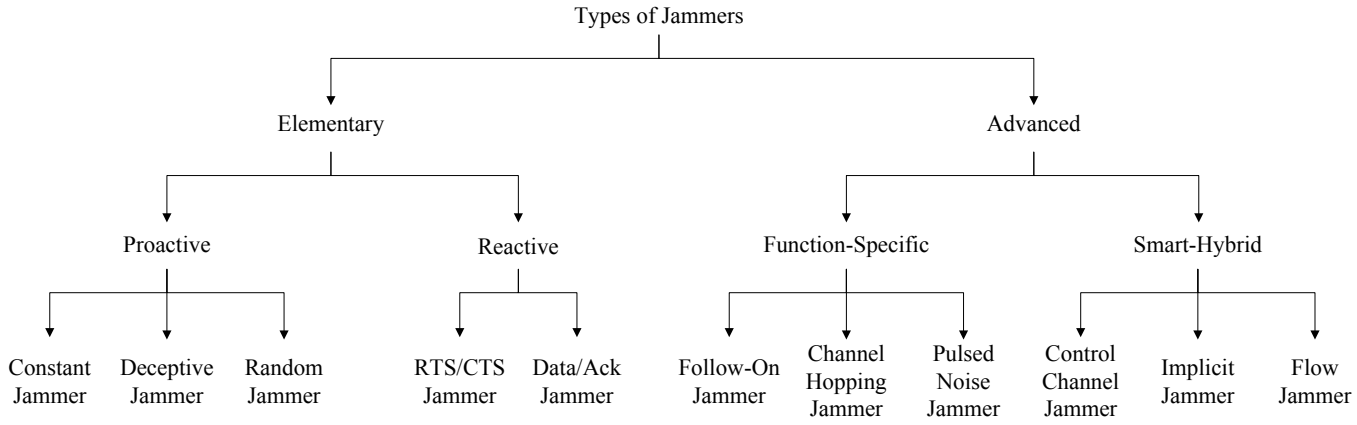

Figure 1 Types of jammers in wireless networks

Reactive RTS/CTS jammer jams the network when it senses a request-to-send (RTS) message is being transmitted from a sender. It starts jamming the channel as soon as the RTS is sent. In this way, the receiver will not send back clear-to-send (CTS) reply because the RTS packet sent from a sender is distorted. Then, the sender will not send data because it believes the receiver is busy with another on-going transmission. Alternatively, the jammer can wait after the RTS to be received and jams when the CTS is sent by the receiver. That will also result in the sender not sending data and the receiver always waiting for the data packet (Pelechrinis et al, 2011).

Reactive Data/ACK jammer jams the network by corrupting the transmissions of data or acknowledgement (ACK) packets. It does not react until a data transmission starts at the transmitter end. This type of jammer can corrupt data packets, or it waits until the data packets reach the receiver and then corrupts the ACK packets (Pelechrinis et al, 2011). The corruptions of both data packets and ACK messages will lead to re-transmissions at the sender end. In the first case, because the data packets are not received correctly at the receiver, they have to be re-transmitted. In the second case, since the sender does not receive the ACKs, it believes something is wrong at the receiver side, e.g. buffer overflow. Therefore, it will retransmit the data packets.

2.1.3 Function-specific Jammers

Function-specific jamming is implemented by having a pre-determined function. In addition to being either proactive or reactive, they can either work on a single channel to conserve energy or jam multiple channels and maximize the jamming throughput irrespective of the energy usage. Even when the jammer is jamming a single channel at a time, they are not fixed to that channel and can change their channels according to their specific functionality.

Follow-on jammer hops over all available channels very frequently (thousand times per second) and jams each channel for a short period of time (Mpitziopoulos et al, 2007). If a transmitter detects the jamming and switches its channel, the follow-on jammer will scan the entire band and search for a new frequency to jam again. Or, it may follow a pseudo-random frequency hopping sequence. This type of jammer conserves power by limiting its attack to a single channel before hopping to another. Due to its high frequency hopping rate, the follow-on jammer is particularly effective against some anti-jamming techniques, e.g. frequency hopping spread spectrum (FHSS) which uses a slow-hopping rate.

Channel-hopping jammer hops between different channels proactively (Alnifie and Simon, 2007, 2010). This type of jammer has direct access to channels by overriding the CSMA algorithm provided by the MAC layer. Moreover, it can jam multiple channels at the same time. During its discovery and vertex-coloring phases, the jammer is quiet and is invisible to its neighbors. Then, it starts performing attacks on different channels at different times according to a predetermined pseudo-random sequence.

Pulsed-noise jammer can switch channels and jam on different bandwidths at different periods of time. Similar to the random jammer, pulsed-noise jammer can also save energy by turning off and on according to the schedule it is programmed for. Unlike the elementary proactive random jammer which attacks only one channel, pulsed-noise jammer can attack multiple channels. Moreover, it can be implemented to simultaneously jam multiple channels. (Muraleedharan and Osadciw, 2006).

2.1.4 Smart-hybrid Jammers

We call them smart because of their power efficient and effective jamming nature. The main aim of these jammers is to magnify their jamming effect in the network they intend to jam. Moreover, they also take

care of themselves by conserving their energy. They place sufficient energy in the right place so as to hinder the communication bandwidth for the entire network or a major part of the network, in very large networks. Each of this type of jammer can be implemented as both proactive and reactive, hence hybrid.

Control channel jammers work in multi-channel networks by targeting the control channel, or the channel used to coordinate network activity (Lazos et al, 2009). A random jammer that targets the control channel could cause a severe degradation of network performance, while a continuous jammer targeting the control channel might deny access to the network altogether. These attacks are usually accomplished by compromising a node in the network. Furthermore, future control channel locations can be obtained from the compromised nodes.

Implicit jamming attacks are those that in addition to disabling the functionality of the intended target, cause denial-of-service state at other nodes of the network too (Broustis et al, 2009). This attack exploits the rate adaptation algorithm used in wireless networks, where the AP (Access Point) caters to the weak node by reducing its rate. Due to this process, the AP spends more time communicating with this weak node than the other nodes. Therefore, when the implicit attacker jams a node which is communicating with the AP, the rate adaptation effect will increase the AP's focus on the jammed node while causing other clients to suffer.

Flow-jamming attacks involve multiple jammers throughout the network which jams packets to reduce traffic flow. As implemented by Tague et al (2008), these attacks are launched by using information from the network layer. This type of jamming attack is good for the resource-constrained attackers. If there is centralized control, then the minimum power to jam a packet is computed and the jammer acts accordingly. In a non-centralized jammer model, each jammer shares information with neighbour jammers to maximize efficiency.

We summarize the features of all the above-mentioned jamming techniques in Table 1. For every type of jammer, we determine whether it is a proactive or reactive, energy efficient or not, and its ability to jam single channel or multiple channels. However, there are some jamming strategies which combine two or more of these techniques (Bellardo and Savage, 2003). For instance, Wilhelm et al (2011) implement a single-tone reactive jamming to generate an optimal jamming strategy by combining the various available forms. Bayraktaroglu et al (2008) use the variations of jammers to analyze the performance of the best jamming strategy in their IEEE 802.11 networks. They experiment with periodic, memoryless jammers based on *Poisson* processes, channel-aware jammers, and omniscient jammers to conclude that channel-aware jammers are the most effective amongst the four types.

In a similar way, Wood et al (2007) use the variations and combination of reactive/random and multi-channel/pulsed-noise jammers to form attacks such as interrupt jamming, scan jamming and pulse jamming. In the interrupt jamming, the jammer stays in sleep states and begins jamming only when it is signaled by the hardware on detection of radio activities. Scan jamming lets the attacker scan each channel first and start jamming if activities are detected. Pulse jamming is the continuously/intermittently jamming on a single channel in which the attacker transmits blindly in short bursts.

2.2 Placement of jammers

In addition to the attacker possessing the above qualities, placement of the jammer plays an important role in effective jamming. Jammers can be placed randomly or can be placed based on a jamming technique which locates the best position to accomplish its objective of jamming with as many nodes as possible. In this section, we will inspect this optimization problem by looking at various placements of jammers.

2.2.1 Optimal jamming attacks

Li et al (2007) show that the probability of jamming can be made high if the attacker is aware of the network-strategy as well as its transmission powers. In addition, the jammer needs to have knowledge about the network channel access probabilities and the number of neighbors to the monitor node (detecting node). All the other nodes in the network just perform the usual IEEE 802.11 simplex communication. The monitor node uses the Sequential Probability Ratio Test for sequential testing between two hypotheses concerning probability of false alarm and probability of missed detection.

The jammers and transmitters/receivers are distributed in a given area using Poisson distribution. The expected values of successful transmission are computed in terms of probabilities. If a particular area is jammed, then the monitor node is expected to send the jamming notification out of the area (using multi-hop transmission); this also suffers from the jamming in the area. Using a probability of distribution and a mathematical proof, the authors proved that the optimal strategy for the attacker tends to be rather mild and long-term.

2.2.2 Jamming under complete uncertainty

Commander et al (2008) use a dynamic approach to compute the location for placing jamming devices by integrating the bounds of the area to be jammed. They assume a square-shaped area encloses the network where the jammers are placed at the intersections of a uniform grid. They formulate the problem as follows. If the jammers have to optimally jam all the nodes of

Table 1 Classification of jammers

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	×	×	×	×	×

the network then where should they be placed? Sub-problems are created and solved in order to achieve an optimal result.

They assume that the attacker has limited network knowledge, i.e., the attacker only knows the bounding area, and that the jammers have omnidirectional antennas. They consider that jamming power decreases inversely to the squared distance from a device. Also, the minimum number of jamming devices to jam the complete network are computed in this scheme, given that at any point there is jamming when the total power received at a particular point is greater than the threshold power required to jam the wireless communication.

2.2.3 Limited-range jamming attacks

Jammers with transmission range half that of legitimate nodes can jam the network because the interference range of wireless devices is twice the transmission range (Huang et al, 2010). Contrary to the above schemes this jamming attack does not require global knowledge. Besides, due to the limited transmission range, these jammers are not easily detected. These jammers are placed at strategic locations. Usually the locations are close to the nodes which have the maximum traffic flow (in/out). The authors have shown the experimental results using normal range, limited range and double range (transmission range) jammers.

The normal range jammers have the same transmission range as legitimate nodes; which makes their interference range twice that of the transmission range. Similarly, the limited-range jammers are formed with half the transmission range and hence, interference range equal to the transmission range of the legitimate nodes. Experiments on these jammers in an OPNET simulator show that the detection of these limited-range jammers is difficult because the transmission power is half that of the legitimate nodes. They concluded that limited-range jammers are difficult to detect because they decrease the metrics that are most commonly used for detection, such as SNR and PDR.

2.2.4 DSS for locating VHF/UHF jammer

Gencer et al (2008) defined a jamming system which should be placed at the optimum location such that it completely demolishes the communication capability of the target system. These kinds of systems are usually used by military applications. More number of candidate points or selected points for deploying jammer system is considered in comparison to the target points and the number of jamming systems available. They assume there is line-of-sight between the jammer and target systems, targets are within the antenna range, and the signal power of the jamming system is higher than the signal power of the target system.

The basic purpose of this decision support system is to find or identify the location at which the radio jammer systems should be placed such that it will jam the maximum area possible. Hence, they use the maximum covering model and solve it using the LINGO-8 package. LINGO is an integrated package that includes a powerful language for expressing optimization models. Given the number of target points, candidate points and jamming systems available, the locations for deploying jammers are obtained.

2.2.5 Nano size jammer

Panyim et al (2009) advocates the use of a large number of tiny, low-power jammers that are difficult to detect as they are not visible to the naked eye, being so smaller in size. The implementation of these jammers is in the form of a network. With the total jamming power being constant, they achieve a phase transition of jamming throughput. Reactive jammers are deployed throughout the network.

Experimental results of this paper show that they provide superior performance to traditional jammers. The number of jammers can be increased, thus reducing their jamming power and holding the total power consumed by the jammers constant. They used the scaling behavior of percolation theory. They proved the difficulty in detecting their jammers because of their low-power, small size and high effectiveness in their network formation.

Table 2 Placement of jammers

Placement strategy	*Network Knowledge*	*Transmission power*	*Number of jammers*	*Detection level*
Optimal jamming attacks	Yes	Controllable	One	Difficult
Jamming under complete uncertainty	Limited	Calculated	Many	Moderate
Limited-range jamming attacks	No	Low	Many	Difficult
DSS for locating VHF/UHF jammer	Yes	High	Many	Easy
Nano Size Jammer	No	Low	Many	Very difficult

In summary, these five jammer placement strategies are analyzed in Table 2 where we investigate if network knowledge is required, the transmission power of jammers, the number of jammers and the difficulty in being detected.

3 Protocols for localizing jammers

Positioning of jammers and manually handling them is one way to deal with jamming attacks. Generally, localization approaches can be divided into two types: range-based and range-free. Since it is not easy to locate a jammer, there is very few work in this area. Current techniques include centroid-based localization approach, virtual-force iterative approach, geometry-covering based localization, light-weight localization, and localization by exploiting neighbors' communication ranges.

3.1 Centroid-based scheme

Centroid-based localization schemes estimate the position of a jammer by averaging the coordinates of the jammed nodes (Liu et al, 2011a). Here, it is assumed that jamming has been detected, the affected nodes are marked as jammed nodes and that these nodes have information about their coordinates. The estimation is totally dependent on the position and number of jammed nodes. It will give very good results for a uniformly distributed network, but seems inappropriate for uneven distribution of nodes in a network.

3.2 Virtual-force iterative approach

To look into unevenly distributed nodes networks, (Liu et al, 2011a) build upon the centroid scheme by using a virtual-force iterative approach, where they estimate the jammer's location iteratively by computing the push and pull virtual forces generating from the boundary nodes of a jammed region and jammed nodes outside the jammed region respectively. Their model is stationary and requires knowledge about their location and those of their neighbors. This work only deals with the location of jammers after jamming has been detected in a network. They consider the region-based as well as the SNR-based models.

3.3 Geometry-covering based localization

Unlike the centroid approach, geometry-covering based localization computes the convex hull instead of the centroid and uses the computed geometry to get the estimated jammer location from the convex hull (Sun and Wang, 2009). Considering that the smallest convex polygon for which each point is given by the convex hull, the authors use this technique to approximate the location of the jammer with high accuracy. After computing the convex hull of the jammed nodes, the smallest circle covering all jammed nodes is calculated, with the center of the circle as the jammer's location.

3.4 Light-weight jammer localization

It is a gradient-based scheme using the theory that as we move closer to the jammer, the PDR becomes low. Pelechrinis et al (2009b) computes the PDR value as a product of the probability of the sender sensing the medium idle, probability that the receiver will receive the packets sent to it and the probability that the sender will receive the acknowledgment. These probabilities are computed using the signal propagation model. This algorithm computes the values independently by sending packets to its neighbors and obtaining the PDR, so it is a good choice for dense as well as sparse environments.

3.5 Exploiting neighbor changes

Liu et al (2011b) conjectures that a jammer may reduce the size of a node's hearing range. It uses the least-squares (LSQ)-based algorithm to localize the jammer. The location is computed according to the changes of a node's hearing range, with the assumption that the initial hearing range of the node is known before the jammer starts its operation. The algorithm forms equations having the unknown jammer coordinates as variables. These equations are equal to the number of nodes whose hearing range changes. They are solved simultaneously. The jammer coordinates are computed from the changes in the hearing range of a group of neighboring nodes.

4 Jamming detection and countermeasure

Since jamming is a very harmful DoS attack, it is important to have effective detection and countermeasure against it. This section discusses some of

these techniques in terms of system model, attack model, and detection metric. In this section, we discuss existing schemes for detection and countermeasure of elementary jamming and advanced jamming.

Table 3 summarizes the different features of all methods covered in this section. We divide them into two groups: detections and countermeasures. For detection techniques, we investigate the working form (individual, distributed, or centralized), detection metric, overhead, cost, and implementation difficulty. For countermeasures, we consider the type of jammer they are against, whether reactive or proactive, working form (individual, distributed, or centralized), overhead, cost, implementation difficulty, and validation methods (theoretical, simulation or experiment bases). Moreover, for each of these methods, we also investigate the network type, condition and whether network knowledge is required.

4.1 Detection and countermeasure of elementary jamming

Elementary jamming consists of proactive as well as reactive jammers. In proactive jamming, the jammer chokes the bandwidth so that a transmitter is unable to transmit. Therefore, carrier-sensing thresholds can be used to detect such type of jammers. When jamming is detected, nodes in the network can map the jammed area and re-route traffic, switch channel, or perform spatial retreat to counteract this jamming act. Reactive jamming conducted at the sender end can be detected by checking received signal strength, signal-to-noise ratio, and packet delivery ratio. These and many other improved metrics have been used for detection and countermeasure of elementary jamming, as discussed in detail below.

4.1.1 JAM: jammed-area mapping protocol

Wood et al (2003) gives a detection and mitigation method which maps out the jammed area in wireless sensor networks and routes packets around the affected region. JAM can map a jammed region in $1-5$ seconds. If a node's utility of channel drops below a certain threshold, e.g. the number of unsuccessful attempts to capture wireless channel is greater than 10, the presence of a jammer is detected. Then, the node's detection system gives a JAMMED or UNJAMMED message which is broadcasted to its neighbor.

When a node (neighboring the jammed node) receives a JAMMED message, it starts the countermeasure in the following ways. It creates a group with a group id and a normalized direction vector pointing to the jammed node. Then, it starts an announce timer for aggregating multiple jammed messages. When the announce timer expires, the node sends its neighbor a BUILD message which contains the group id followed by a membership list. The direction vectors of groups are compared to check for compatibility. If these vectors are compatible, they are coalesced together. When timer for coalesce expires, the mapping node sends its neighbor a BUILD message containing the dominant group id and merged member list. Other mapping nodes will update its coalesce information upon receiving new BUILD messages.

When a jammer is withdrawn from the network, the previously jammed nodes will send UNJAMMED messages to its neighbors. Upon receiving these messages, the mapping nodes notify the group of recovered nodes using a TEARDOWN message which has the opposite membership property of the BUILD message. After the completion of the mapping process, the messages being transmitted in the network follow a different route avoiding the area mapped as jammed. Wood et al (2003) also show that the JAM in sparse networks does not achieve as good convergence as in moderately connected networks.

4.1.2 Ant system

Muraleedharan and Osadciw (2006) propose an evolutionary algorithm for detecting jamming at the PHY layer and redirects messages to an appropriate destination node. It formulates a hypothesis to test whether a DOS attack is genuine or not. By making an agent traverse the network iteratively, the Ant system collects the information for various routes to a destination. This information is then saved in a 'tabu' list and will be used for redirection. The information on energy and distance are used to make decision of whether jamming is detected or not.

They used four types of jammers: single-tone, multiple-tone, pulsed-noise, and ELINT (Electronic Intelligence). The detection of a node is based on its resource's availability such as hops, energy, distance, packet loss, SNR, BER and PDR. After checking for this metrics, they are put into a decision model which states if the detection of jamming is true or not. The outcome may be a *genuine acceptance rate* (acceptance of the fact that a jamming occurs) is high or *false acceptance rate* is high. The system computes the values of transition probabilities iteratively to check if the network is really jammed or not. It calculates a probability for the link between two given nodes. If the probability is within a certain threshold, the route is traversed, otherwise the network is jammed. When jamming takes place on a particular link, the link will not be included in the route and another route is explored.

4.1.3 Hybrid system

Jain and Garg (2009) propose a hybrid anti-jamming system by combining 3 defense techniques: base station (BS) replication, base station evasion and multipath routing between base stations. The replication scheme implies that multiple replicated base stations are present in the network. Evasion scheme refers to the spatial retreat of a base station when jamming is detected.

Multipath routing takes place when there are multiple data routes between a node and a base station.

These countermeasure techniques can be used to deal with jamming at base stations, either individually or collectively. From the simulation results, Jain and Garg (2009) show that the collective implementation gives a better throughput. With the technique of BS replication, if one or more BSs are jammed, the unjammed BSs can serve the network. With the BS evasion, the change of BS locations follows a pre-defined off-line schedule so that no more than one BSs reach the same location at the same time. This is to avoid collision between base stations. The third technique of multipath routing requires multiple paths to exist between every network node and base stations assuming that there is at least one non-jammed path between them.

4.1.4 Channel surfing and spatial retreat

Channel surfing countermeasure provides migration to another channel when a jammer comes within range and blocks communication on a particular channel (Xu et al, 2004). Spatial retreat, on the other hand, moves mobile nodes from the location where they experience jamming to another safe location. Xu et al (2004) investigate three categories of scenarios: two-party communication, infrastructure, and ad hoc networks. The placement of jammers can be either horizontal or vertical. The detection can be conducted at either MAC layer using CSMA or PHY level by measuring ambient noise levels. On the confirmation of a jamming detection, channel changing or spatial retreat procedure is executed (Lazos et al, 2009).

Before switching channels, the next channel is computed by adding one to the previous channel and taking its modulus with the number of orthogonal channels in that band. In other words, given M orthogonal channels, the next channel is $C(n+1) = (C(n)+1)\,\%M$. If it is an infrastructure-based network, the access point checks if all its registered clients are on the same channel after the channel is changed. Otherwise, it broadcasts a channel change command with a private key authentication. In the ad-hoc scenario, dual-radio usage is suggested where one radio is used for monitoring channel changes.

On spatially retreating to a new position, re-configuration of the network is required. If jamming affects communication between two nodes, they need to have a format as to which direction they should move. Therefore, it is necessary for the communicating nodes to know of each other's location coordinates beforehand. When an infrastructure network is under consideration, the moving nodes can establish a connection with the new access points using handoff strategies. Spatial retreat in ad-hoc networks is more complicated and not easily implemented.

4.1.5 Using PDR with consistency checks

Xu et al (2005) propose jamming detection using either location or signal strength consistency check along with packet delivery ratio determination. They conclude that no single measurement can alone determine the presence of jammers efficiently. The presence of constant and deceptive jammers can be distinguished from normal traffic by computing the higher order crossing (HOC). Low PDR leads to the detection of jamming, but it can also be due to several other factors besides jamming. To confirm a low PDR is due to jamming, consistency checks are used.

The reactive signal strength consistency check takes place after the PDR drops below a threshold. High signal strength implies high PDR while low signal strength implies low PDR, but low PDR does not imply low signal strength. If signal strength is high but PDR is low, neighbors' PDRs need to be checked. If at least one neighbor has a high PDR, jamming is not detected. The proactive location consistency check calculates the location irrespective of the PDR value. A node decides its jamming status by observing if its PDR is consistent with its neighbors. If it is observed that all nearby nodes have low PDR values, jamming is detected. If a node does not have nearby neighbors, the value of PDR for this node will be low. For such a node, the effect of jamming is not considered noticeable.

4.1.6 Fuzzy interference system

Misra et al (2010) presents a centralized jamming detection mechanism by computing the jamming index using the signal-to-noise ratio (SNR) and packet dropped per terminal (PDPT) values. This is followed by a confirmatory check, and a 2-means clustering of neighborhood nodes. A base station runs the detection algorithm to obtain the numbers of packets received by a node during a particular time period, packets dropped by the node, and signal strength. The base station then computes the PDPT and SNR from the received data to perceive the presence of a jammer.

The probability of detecting a jammer is decided by a 3-step fuzzy interference system based on the SNR and PDPT values. The fuzzy interference system detects jamming using the following method. If the SNR is low, the jamming probability is high irrespective of the PDPT. For a medium values of SNR, the jamming probability is dependent on the PDPT values. For a high SNR, the jamming probability is a level lower than the PDPT vales. Then, the 2-means clustering algorithm groups neighboring nodes into clusters of jammed and non-jammed nodes.

4.1.7 Game theoretic modeling

Game theoretic model uses a clustering algorithm to identify whether a node belongs to a normal (non-jammed) cluster or anomalous (jammed) cluster based on the retransmit RTS, retransmit DATA, carrier sensing

failure count, and network allocator value (Thamilarasu and Sridhar, 2009). Game theory requires two players: the jammer and the monitor nodes. The purpose of jammers is to maximize the denial of wireless channel access to the legitimate users, while legitimate nodes try to maximize their communication throughput. Monitor nodes use cross layer features for detection of constant jammers by sensing the medium and for detection of reactive jammers by average retransmission rate of RTS/Data packets. Monitor nodes can act continuously or periodically.

In the detection procedure, the normal and anomalous clusters are defined on the basis of the above four features. For each node, the *Euclidean* distance is computed to see if the node has features closer to the normal cluster or the anomalous cluster. If the feature vector is anomalous, jamming attack is detected. To ensure minimum false positives, periodic strategy of monitor is abandoned for continuous constant jamming situations. Constant jammers are detected by continuous detection leading the jammers to select reactive behaviors. This is the trade-off between detection rate and monitoring duration of detection algorithms, or jamming rate and energy conservation of jamming algorithms.

4.1.8 Channel hopping

Channel hopping or switching from one channel to another is the most popular countermeasure to jamming. Proactive channel hopping is the simplest implementation. Different variations of channel hopping are discussed in (Khattab et al, 2008a,b; Wood et al, 2007; Navda et al, 2007; Gummadi et al, 2007; Kerkez et al, 2009; Wang et al, 2011; Yoon et al, 2010). They improve the effectiveness of channel hopping by making it reactive, adaptive and code-controlled.

In proactive channel hopping, the current communicating channel is changed after a certain duration of time. This takes place irrespective of whether or not there is jamming. Due to the impacts of energy spill over the adjacent channels, Pelechrinis et al (2009a) prove that proactive frequency hopping is not very effective. Their experiments on IEEE 802.11a/g and 802.11n, with one jammer and multiple jammers, show that the entire IEEE 802.11a spectrum (with 12 orthogonal channels) can be jammed by 4 jammers. This is because each jammer placed on an orthogonal channel harms the communication of three channels including the two adjacent channels.

Since IEEE 802.11n implements channel bonding to use $40MHz$ channels, it has limited number of orthogonal channels to hop. That makes channel hopping not a good option as a jamming countermeasure in IEEE 802.11n networks. The drawbacks of proactive frequency hopping are the restricted number of orthogonal channels and the smaller frequency separation between channels. Pelechrinis et al (2009a) advocate frequency hopping as an effective technique if and only if the number of orthogonal channels are large.

A slight variation to the simple proactive form is a reactive scheme based on the detection of jamming by channel sensing. A threshold value σ needs to be fixed. If the waiting time for accessing channel exceeds a given threshold value, jamming is assumed and channel is switched to another one selected either randomly or according to a pre-defined strategy. In addition to the pseudo random reactive channel hopping mechanism, straightforward and deceptive schemes are two other strategies proposed by Khattab et al (2008b).

In straightforward channel hopping, the channel to be hopped onto is selected from the set of unused channels. In deceptive scheme, the selection set includes the currently used as well as unused channels. In this case, if an attacker knows the channel hopping history, it can easily track the channel selected for hopping and continue jamming the next channel. Studying the variations leads to the conclusion that the best alternative amongst them is using a pseudo random channel hopping scheme, which selects channels based on a pseudo number generation unknown to jammers (Navda et al, 2007).

Adaptive scheme switches the communication to another channel once every k slots (a slot is defined to be a fixed time interval). After the packet delivery ratio (PDR) is computed for that channel, communication is switched back to the initial channel. When the performance (PDR) of the present channel falls below a threshold, communications are switched to another channel which gives the best PDR value.

Recently, Wang et al (2011) put forward a code-controlled message-driven frequency hopping mechanism. It generates a dynamic hopping pattern each time the channel is changed. Wang et al (2011) use the pseudo noise (PN) sequence coding technique which also partially contributes to detecting jammed channels with the help of spectrum sensing capabilities. The design is proposed for both the transmitter and the receiver. It is an effective hopping technique when nodes have spectrum sensing ability and the jammer are not too complicated.

4.1.9 Reactive Jamming detection using BER

Strasser et al (2010) propose to detect jamming using the bit error rate (BER) for reactive jammers that keep the received signal strength (RSS) low while introducing disruption in a packet. By looking at the RSS of each bit during the reception, it identifies the cause of bit errors for individual packet using predetermined knowledge, error correcting codes (ECC), or wired node chain systems. If the error is due to weak signal, the RSS should be low. If the RSS value is high for a bit error, there are external interference or jamming.

Assuming nodes can assess the expected local interference, the sequential jamming probability test calculates the marginal likelihood of errors due to

unintentional collisions. If this value is less than the log of the ratio of targeted probability for a missed alarm to the targeted probability, then there is jamming and an alarm is raised. If the marginal likelihood is less than the ratio, there is no jamming and the sequence is reset. There is also a possibility that no conclusion is made until there are more conclusive evidences for jamming. In such a case, iterative steps are followed to reach a conclusion. From their experiments, Strasser et al (2010) prove that no false positive occurs, only false negatives which are due to the erroneous calculation of bit errors.

4.1.10 Trigger nodes identification

To tackle reactive jamming, a method for identifying trigger nodes is defined in (Shin et al, 2009). The trigger nodes are those in the network whose broadcasting can trigger reactive jammers into action. Another set of nodes, victim nodes, are defined as those which are attacked by the triggered jammers. Reactive jamming attacks are difficult to detect as they are activated only when transmission of packets takes place in the network, i.e. they are triggered by communication between nodes.

To detect reactive jammers, an integration of three techniques is used: group testing, disk cover, and clique-based clustering. In the first phase, detection of victim nodes is done using a breadth-first search method. At the completion of this phase, a base station has the information of all victim nodes in the network. In the second phase, nodes are divided into groups and tested so that the set of victim nodes being jammed by the same jammer are found. In the third phase, the trigger nodes are identified using a group testing mechanism, called non-adaptive combinatorial testing. Once the trigger nodes are known, a different route is selected for routing packets.

4.2 Detection and countermeasure of advanced jamming

Advanced jammers are either function-specific or smart-hybrid jammers that use a combination of proactive and reactive strategies with smart implementations for conserving energy while they jam a network. In this section, we discuss the various anti-jamming techniques dealing specifically with advanced jammers. For example, in Hermes node countermeasure against follow-on jammers, the control-channel jammer is rendered ineffective when a control channel hopping sequence is applied. In addition, MULEPRO is a multi-channel defense against channel hopping jammer. While the cross-layer approach fights against flow jamming, the FIJI system deactivates implicit jamming.

4.2.1 Hermes node (hybrid DSSS and FHSS)

In defense of jamming attacks by fast-following jammers, direct-sequence spread spectrum (DSSS) and frequency-hopping spread spectrum (FHSS) are used in (Mpitziopoulos et al, 2007) for their respective processing gains. DSSS uses a wider bandwidth for signal transmission while FHSS provides interference avoidance. A hybrid DSSS and FHSS scheme, called Hermes node, is proposed to deal with jamming attacks in sensor networks. The Hermes node performs $1,000,000$ hops per second (FHSS) to avoid the fast-following jammers. DSSS is used to make the attacker sense the data signals as white noise, which prevents the attacker from detecting the communication radio band. Hermes node uses 55 frequency channels for FHSS and $275MHz$ of bandwidth for spread-spectrum in DSSS.

Both the frequency sequence of FHSS and pseudo noise (PN) code of DSSS should be known so that the original signal can be recovered. A secret word is used as a seed for the generations of channel sequence and the PN code. The secret word is usually hard-coded for a particular network so that a new node entering into the network can be identified with the existing nodes. Synchronization between nodes is important for Hermes node to work properly, which is achieved by the sink.

4.2.2 Control channel attack prevention

The control channel in a wireless network coordinates channel usage where multiple channels are used to increase the network capacity. To avoid jamming, Lazos et al (2009) propose several clusters, whereby each maintains its own control channel with a unique hopping sequence. At the higher network level, a jammer can jam the control channel by taking information from a compromised node about the protocol mechanisms and cryptographic quantities. A jammer's capability to successfully determine the future control channel from previously observed information is measured in evasion entropy.

The compromised nodes are identified by computing the Hamming distance between the jammer's hopping sequence and the actual hopping sequence. The identification of the compromised nodes leads to the re-establishment of the control channel using frequency hopping by updating the hopping sequence. The latency of the successful re-establishment of the new control channel is measured as evasion delay. Evasion ratio gives the availability of communication in the presence of jamming.

4.2.3 MULEPRO

Alnifie and Simon (2007, 2010) implements an exfiltration methodology against jamming. They assume that each node independently determines whether it is jammed or not. When a node detects a jamming attack, MULEPRO (MULti-channel Exfiltration PROtocol) is executed and switches the node from normal mode to exfiltration mode. In the normal mode, only the common channel is used for communications. The multi-channel capability comes into play only when the jamming attack takes place. In the exfiltration mode, there are two

phases: 1) when nodes (in the sender set) transmit to receiver set and 2) when nodes (in receiver set) exfiltrate the data in the direction of boundary nodes.

MULEPRO execution determines how data is to be transferred out of the jammed area, either through single-hop if the jammed node can communicate directly with the boundary node, or through multi-hop if there are one or more nodes between the jammed node and the boundary node. Each node sends packets multiple times to ensure that the attacker does not attack all nodes. It uses the assigned channel to receive the exfiltrate data. The node will transmit data packet on the assigned channel for a particular time slot according to the exfiltration matrix formed by the MULEPRO protocol. Throughout the jammed session when the exfiltration mode is executed, the boundary node continues using the common channel.

In addition, MULEPRO will switch between other channels to get data from the jammed nodes and transfer data outside of the jammed area in a single hop case. This takes place when the boundary node has receiver in its matrix while the jammed node has a sender value in its corresponding matrix. In the multi-hop case, each jammed node will be transmitting its data along with its vertex color. The jammed nodes which lie in the outer region have to switch back and forth between the exfiltraing data in the outer direction and listening to data arriving from the inner jammed nodes. The nodes in this case have their time slot divided in 2-mini time slots, one for listening to jammed data and one for sending exfiltrate data to outside. MULEPRO results show that it can act against many kinds of jammers but is quite useful against channel hopping jammer.

4.2.4 Cross-layer jamming detection and mitigation

Jamming detection can be done either at the PHY layer or MAC layer; very rarely is it done on the higher-layers. There are some cases where jamming detection is done using cross-layer approaches. For example, Chiang and Hu (2011) use an asymmetric pattern fast-frequency hopping CDMA to mitigate the effects of jamming in broadcast systems. The protocol is based on PHY layer but uses the upper-layer security mechanisms. A tree-based approach is used to form the asymmetric hopping pattern. Any user can decode the message transmitted by the sender using exactly one hopping pattern. When jamming is detected, the cover is removed and both the children of that root are added to the cover. The detection of jamming is done when the transmitter uses additional test patterns during its transmission.

4.2.5 FIJI: Fighting implicit jamming

Broustis et al (2009) proposes another cross-layer jamming detection against intelligent jammers by implementing part of the system in the driver and part in the network module. An AP running the FIJI system maintains that jammed clients receive the maximum throughput, while non-jammed clients are unaffected. The detection algorithm works by computing the data transmission delay for each of the client connected to the AP. Jamming is perceived when there is an abrupt increase in the downlink traffic due to the increase in the transmission delay time from the client.

On detection confirmation, the data packet tuning procedure reduces not only the size of the data packets sent to the jammed node at lower data rates but also the channel occupancy time for that node. Considering the number of clients to the AP and the number of jammed clients, it calculates the data packet size. To avoid changing the packet size at the network layer, data rate tuning is used. It is implemented in the MAC layer but does not give as fair a solution as the data packet tuning module. However, it helps in increasing the throughput to the non-jammed clients while ignoring the jammed clients.

5 Discussion

In this section, we first analyze the potential issues in existing jamming detection and countermeasure strategies. Then, we point out the open research challenges which require more research work.

5.1 Analysis of existing approaches

There are many solutions to the detection of jamming attacks and anti-jamming countermeasures. Although some approaches present very good techniques with high quality results, others are not perfect. Therefore, we discuss the potential issues with each of them below.

The JAM mapping protocol approach only maps a jammed area; it is not able to quantify the type of attack experienced by a node. Moreover, it does not seem feasible to effectively detect reactive jamming using this scheme. Also, mapping messages (JAMMED/UNJAMMED) increase the overhead of the network. In the Ant system, if jamming is detected in an area much before a tabu list is formed by the agents, then the scheme fails. Also, it takes an additional overhead of time to form the tabu list with the Ant agents. In addition, it incurs memory overhead. They compute the network performance using network parameters and based on those values they decide if some particular nodes/part of the network is jammed or not. The network parameters and metrics considered are good but the computation and decision in jamming detection does not seem convincing.

For the base station replication technique, all the data needs to be copied to all the replicated BSs. Suppose there is a time period defined after which all the replicated BS's data are updated. If a working BS is jammed before the update, then there is data loss for the time period that the BS is jammed. In the evasion techniques, there is an overhead of movement

and network reconfiguration. Multipath routing can only be successful if multiple paths exist for reaching a destination from a particular source and if one out of all the paths is not jammed. Channel surfing at the link layer would require synchronization between two communicating nodes and is an expensive option in terms of time.

Spatial retreat, movement, time and network reconfiguration need to be considered and add to the overhead. In spatial retreat, if a particular communication between two parties is to avoid jamming by moving both the nodes to a new safer location, synchronization between these two nodes should be maintained, which is an additional overhead. In the consistency checks approach, the nodes need to communicate with the neighboring nodes to get the values of RSS and location which are used for comparison. However, in jamming scenarios, these nodes may not be able to communicate with the neighbors to get these values.

Fuzzy Interference mechanism is well-suited for detection of jamming in information warfare environments. In the algorithm "2 means clustering of neighborhood nodes," a densely deployed network would yield better results compared to a sparsely deployed network. Therefore, it is not suitable for networks with fewer neighboring nodes. Channel hopping can be implemented in dense or sparse networks. There is very little overhead required for implementing the hopping technique. Since this scheme uses carrier sense time as the metric, it is not possible to detect reactive jammers in the network.

Reactive jammers are very difficult to identify. BER metric when used in combination with RSS yields an effective scheme for the detection of reactive jammers. Fixing of the threshold values for all the parameters might lead to pitfalls in the method. For example, the threshold value of RSS needs to be fixed after the consideration of the radio and modulation scheme, which might differ from the method of fixing the threshold for the targeted probability for a false alarm. Overhead is high due to increase in header length with ECC usage. The detection of trigger nodes provides a well-drafted mechanism. A strong mathematical explanation backs up the scheme, although this scheme is unable to define the location of the reactive jammers.

5.2 Open research challenges

After analyzing numerous jamming and anti-jamming techniques, we conclude that there is currently no universal anti-jamming technique which deals with all kinds of jammers. Compared to implementing a jammer, it is more difficult to design a detection and countermeasure strategy. In addition, there are increasingly more newer wireless network technologies (e.g. vehicular network, WiMax), making anti-jamming a more challenging issue. In this section, we list a few important research challenges which are still open problems, such as energy efficient jamming detection, detection based on jammer classification, anti-jamming in IEEE 802.11n and wireless mobile networks.

5.2.1 Energy efficient jamming detection

In surveying elementary jamming detection and countermeasures, we realize that a well drafted reactive jamming detection method is not available. A good detection mechanism should be able to distinguish if the packet loss is caused by weak radio link or due to interference signals. Moreover, there are many implementations of low-power jamming techniques such as reactive jammers. However, there is no low-power detection strategy that provides effective detection of low-power jamming.

5.2.2 Detection based on jammer's classification

In classifying jammers, we discover that there are various types of jamming attacks which can be organized in Fig. 1. We believe it is possible to detect a jammer based on its behavior by examining its classification. For instance, the detection algorithm can determine the characteristics of jammers from top down in Fig. 1. The first step is to determine whether the jammer is elementary or advanced. Then, it further classifies the jammer at the second level as being proactive, reactive, function-specific or smart-hybrid. Although a bottom-up approach can also be taken, it seems to be easier to implement a top-down approach.

5.2.3 Anti-jamming in IEEE 802.11n networks

There is very few research work on jamming and anti-jamming techniques in IEEE 802.11n networks. Since the IEEE 802.11n is very different from its predecessor IEEE 802.11a/b/g, the results of applying existing jamming and anti-jamming techniques on IEEE 802.11n network could be very different. For example, XXXX shows that due to the channel bonding effect in IEEE 802.11n, proactive frequency hopping is not a suitable countermeasure for jamming. On the other hand, since the IEEE 802.11n technology uses orthogonal frequency division multiplexing (OFDM), it will be easier to implement an effective reactive countermeasure.

5.2.4 Anti-jamming in wireless mobile networks

Most jamming detection and countermeasure are designed and evaluated in static networks. The anti-jamming problem becomes more challenging in a mobile network environment where jammers may move and cause the malfunction of jammer detection and localization algorithms. So far, spatial retreats seem to be the only strategy implemented on the mobile nodes. Having an effective approach for wireless mobile networks with acceptable overhead is still an open issue. The anti-jamming system for mobile networks should provide fast-detecting and fast-reacting mechanism

which can identify and localize a jammer quickly. Moreover, since the same jammer may move and cause jamming in other areas in the networks, how to prevent jamming based on historical jamming information will be very interesting.

5.2.5 Universal anti-jamming technology

Finally, we want to pose the ultimate question: is it possible to have a single practical anti-jamming solution which can deal with all types of wireless networks (whether it is static or mobile, sensor or Wi-Fi, infrastructure-based or ad-hoc) and detect all kinds of jammers (e.g. constant, deceptive, random, reactive, follow-on, channel hopping, control channel, implicit, flow jammers)? In addition, since we have so many effective jamming techniques, beside preventing eavesdropper's attack, can we use them for any useful purpose?

6 Conclusion

In this extensive study on jamming and anti-jamming techniques in wireless networks, we have contributed by classifying and summarizing various approaches and discussing open research issues in the field. Different jammers attack wireless networks in various ways so that their attack effects are significantly different. For instance, a constant jammer consumes all resources available and continuously jams the network, but it is easily detected. On the other hand, a reactive jammer senses the medium and only attack when a certain condition is satisfied, so it is a good choice for resource-constrained hardware. In summary, if a jammer is a periodic low power one, it is hard to be detected; a powerful jammer will certainly jam most of the networks but will be easily detected.

We also investigate the placement of jammers which is considered to be helpful in making jamming more effective. For example, to achieve a better jamming effect, it is possible to decrease the power of jammers by tactically placing them in the interference ranges of communicating nodes. No matter how smart or effective a jammer is, there is always one or more corresponding anti-jamming techniques. After elaborating on various types of jamming detection and countermeasure schemes, we discover that anti-jamming is such an interesting problem that many methods are tried to solve this issue. For example, artificial intelligence, game theory, mobile-agent, cross-layer, spatial retreat, consistency check, and channel or frequency hopping have all been applied to this field. Some approaches, e.g. JAM, map out the area that is jammed to avoid forwarding packets within that area. Other approaches, e.g. Hermes node, detect jamming and switch channels or move nodes to a new physical location. In summary, after detecting jamming in networks, nodes either choose to switch the jammed channel to a non-jammed one, forward packets outside the jamming areas or simply move to a non-jammed area.

The basic open issues in this field includes: 1) energy efficient detection scheme, 2) jammer classification in detection scheme, and 3) jamming and anti-jamming in mobile networks and IEEE 802.11n networks. Although accurately detecting jammers is the most important job of a anti-jamming system, energy efficiency should be considered for low-powered networks, e.g. sensor networks. While it is possible to detect a jammer, it is currently difficult for a detection mechanism to classify the type of the detected jammer. Moreover, due to nodes' mobility, anti-jamming is extremely difficult in mobile networks and IEEE 802.11n networks.

References

Alnifie G, Simon R (2007) A multi-channel defense against jamming attacks in wireless sensor networks. In: Proceedings of the 3rd ACM Workshop on QoS and Security for Wireless and Mobile Networks, pp 95–104

Alnifie G, Simon R (2010) MULEPRO: a multi-channel response to jamming attacks in wireless sensor networks. Wireless Communications and Mobile Computing 10(5):704–721

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

Bellardo J, Savage S (2003) 802.11 denial-of-service attacks: Real vulnerabilities and practical solutions. In: Proceedings of the 12th Conference on USENIX Security Symposium, pp 15–28

Broustis I, Pelechrinis K, Syrivelis D, Krishnamurthy SV, Tassiulas L (2009) FIJI: Fighting implicit jamming in 802.11 WLANs. Security and Privacy in Communication Networks 19:21–40

Chiang JT, Hu YC (2011) Cross-layer jamming detection and mitigation in wireless broadcast networks. IEEE/ACM Transactions on Networking 19(1):286–298

Commander CW, Pardalos PM, Ryabchenko V, Shylo OV, Uryasev S, Zrazhevsky G (2008) Jamming communication networks under complete uncertainty. Optimization Letters 2(1):53–70

Gencer C, Aydogan EK, Celik C (2008) A decision support system for locating VHF/UHF radio jammer systems on the terrain. Information Systems Frontiers 10(1):111–124

Gollakota S, Katabi D (2010) iJam: Jamming oneself for secure wireless communication. Tech. rep., Massachusetts Institute of Technology

Gummadi R, Wetherall D, Greenstein B, Seshan S (2007) Understanding and mitigating the impact of RF interference on 802.11 networks. In: Proceedings of the 2007 Conference on Applications, technologies, architectures, and protocols for computer communications, pp 385–396

Huang H, Ahmed N, Pulluru S (2010) On limited-range strategic/random jamming attacks in wireless ad hoc networks. In: IEEE 34th Conference on Local Computer Networks, pp 1–8

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

Kerkez B, Watteyne T, Magliocco M, Glaser S, Pister K (2009) Feasibility analysis of controller design for adaptive channel hopping. In: Proceedings of the Fourth International ICST Conference on Performance Evaluation Methodologies and Tools, pp 76:1–76:6

Khattab S, Mosse D, Melhem R (2008a) Jamming mitigation in multi-radio wireless networks: Reactive or proactive? In: Proceedings of the 4th International Conference on Security and privacy in communication netowrks, pp 27:1–27:10

Khattab S, Mosse D, Melhem R (2008b) Modeling of the channel-hopping anti-jamming defense in multi-radio wireless networks. In: Proceedings of the 5th Annual International Conference on Mobile and Ubiquitous Systems: Computing, Networking, and Services, pp 25:1–25:10

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

Li M, Koutsopoulos I, Poovendran R (2007) Optimal jamming attacks and network defense policies in wireless sensor networks. In: IEEE 26th IEEE International Conference on Computer Communications, pp 1307–1315

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

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

Misra S, Singh R, Mohan SVR (2010) Information warfare-worthy jamming attack detection mechanism for wireless sensor networks using a fuzzy inference system. Sensors 10:3444–3479

Mpitziopoulos A, Gavalas D, Pantziou G, Konstantopoulos C (2007) Defending wireless sensor networks from jamming attacks. In: IEEE 18th International Symposium on Personal, Indoor and Mobile Radio Communications, pp 1 –5

Mpitziopoulos A, Gavalas D, Konstantopoulos C, Pantziou G (2009) A survey on jamming attacks and countermeasures in WSNs. IEEE Communications Surveys Tutorials 11(4):42–56

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

Navda V, Bohra A, Ganguly S, Rubenstein D (2007) Using channel hopping to increase 802.11 resilience to jamming attacks. In: IEEE 26th IEEE International Conference on Computer Communications, pp 2526–2530

Panyim K, Hayajneh T, Krishnamurthy P, Tipper D (2009) Jamming dust: A low power distributed jammer network. In: 27th Army Science Conference, pp 922–929

Pelechrinis K, Koufogiannakis C, Krishnamurthy SV (2009a) Gaming the jammer: is frequency hopping effective? In: Proceedings of the 7th International Conference on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks, pp 187–196

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

Pelechrinis K, Iliofotou M, Krishnamurthy S (2011) Denial of service attacks in wireless networks: The case of jammers. IEEE Communications Surveys Tutorials 13(2):245 –257

Shin I, Shen Y, Xuan Y, Thai MT, Znati T (2009) Reactive jamming attacks in multi-radio wireless sensor networks: an efficient mitigating measure by identifying trigger nodes. In: Proceedings of the 2nd ACM International Workshop on Foundations of Wireless Ad Hoc and Sensor Networking and Computing, pp 87–96

Strasser M, Danev B, Čapkun S (2010) Detection of reactive jamming in sensor networks. ACM Transactions on Sensor Networks 7(2):16:1–16:29

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

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

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

Wang H, Zhang L, Li T, Tugnait J (2011) Spectrally efficient jamming mitigation based on code-controlled frequency hopping. IEEE Transactions on Wireless Communications 10(3):728–732

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

Wood A, Stankovic J, Son S (2003) JAM: a jammed-area mapping service for sensor networks. In: 24th IEEE Real-Time Systems Symposium, pp 286–297

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

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

Xu W, Trappe W, Zhang Y, Wood T (2005) The feasibility of launching and detecting jamming attacks in wireless networks. In: Proceedings of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing, pp 46–57

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

Table 3 Classifications of jamming detection and countermeasures

	Network attributes				Detection schemes					Countermeasures					
	Type	*Density*	*Knowledge*	*I/D/C*	*Metric*	*OH*	*Cost*	*DF*	*Jammer*	*R/P*	*I/D/C*	*OH*	*Cost*	*DF*	*T/S/R*
Jam Mapping	WSN	Moderate	Yes	I	CCA	L	L	M	EM	R	D	M - H	M - H	M	S
Ant system	WSN	Moderate	Yes	I	SNR, BER	M	M	M	EM	R	D	H	M	L	S
Hybrid	WSN	Dense	Yes							R	D	H	M	M - H	S
Spatial retreat	WLAN	Moderate	Yes	I	CSMA, Ambient noise	L	L	M	P	R	C	H	H	H	ETS
Channel hopping	WSN/ WLAN		No						P	R/P	I&C	L	L	M - H	S/ETS
Reactive detection	WSN	Dense	Yes	D	BER, RSS	H	H	H	R						ETS
Trigger nodes	WSN	Sparse	Yes	I&D	CCA	H	H	M - H	R	R	D	M	M	M	S
Consistency check	WSN	Dense	Yes	D	CSMA	L	L	M	EM						ETS
Hermes node	WSN		No			M - H	M	H	Follow - on	P	I	M - H	M	H	S
Frequency hopping	Ad hoc		Yes	C/D	Evasion entropy	M	M	M	Control-channel	R	D	L	L	H	T
MULEPRO	WSN		Limited						Channel hopping	R	D	H	M	M - H	S
Game theoretic	Ad hoc		Yes	C	CSMA, RTS				Constant, reactive						T
Fuzzy intelligence	WSN		Yes	C	SNR, PDPT	M	H	H	EM						S
Cross-layer system	Broadcast networks	Moderate	Limited	D	Hopping pattern	M	L	M	Flow jamming						T
FIJI	AP	Sparse	Yes	C	Delay	L	L	M	Implicit	R	C	M	M	H	ETS

I - Individual
D - Distributed
C - Centralized
H - High
M - Medium
L - Low
E - Experiment
T - Theory
S - Simulation
R - Reactive
P - Proactive
OH - Overhead
EM - Elementary
DF - Difficulty