Journal of Theoretical and Applied Information Technology
15th August 2011. Vol. 30 No.1

ISSN: **1992-8645** www.jatit.org E-ISSN: **1817-3195**

SURVEY ON SURVIVAL APPROACHES IN WIRELESS NETWORK AGAINST JAMMING ATTACK

FARAZ AHSAN [1], ALI ZAHIR [1], SAJJAD MOHSIN [1], KHALID HUSSAIN [2]
[1] COMSATS Institute of Information Technology, Islamabad, Pakistan
[2] University Technology Malaysia, Skudai, Johor. Malaysia.
{(fahsan, alizahir, smohsin)@comsats.edu.pk, hkhalid2@live.utm.my}

ABSTRACT

Wireless networks are more depicted to intentional or unintentional threats than their wired based equivalent networks. Major reason being the wireless medium which can be listened and interfered by non-participants, in an on-going valid communication. In the absence of a collision detection mechanism and relying mainly on cooperation of each other for packet routing, the standard defined for wireless network is unable to identify any malicious activity, by default [1]. Among attacks the ones which create isolation of the nodes on the network are considered more severe. If they last long enough, can result in denial-of-service and hence network collapses completely. The simplest form of such attacks is jamming attack which can block any current legitimate communication. It is easy to launch as no especial hardware is required and the area in range can be jammed for any legal communication. Jamming is a specialized Denial of Service attack in which purpose is not to overflow buffers, instead to choke the physical communication channel, hence handling jammer is much harder than other attacks. Unlike other attacks, especially routing attacks, no network parameter and topology etc need to be known in advance before launching jamming attack. However, if the network parameters are known and the attack is intelligently placed, a jammer can last longer on the network resulting in more survival time and thus increased damage. This paper surveys on different types of jamming attack and the mitigation techniques generally used. Besides this, we investigate about the approaches proposed that are considered efficient to survive in a jammed region, actively. Finally, we conclude by highlighting the potential areas which can be targeted to optimize in minimizing the effects of a jamming attack, as future directions.

Keywords: *WLAN, Jamming Attack, Wireless Network, Survival Approaches, DOS*

1. INTRODUCTION

Due to ease of installation and usage, unlicensed band, cheap hardware, mobility, portability and expandability, wireless network has become the most popular technology among current communities. New network of businesses are quickly deploying by saving cost and time of having wired offices and workstations, resulting in a real business success tool. Different types of wireless systems ranging from WLAN to mesh and sensors network are available as per the requirement. However, one critical issue of security exists in wireless networks; especially some attacks are medium dependent and do not exist in the earlier counterpart [2]. The wireless medium introduces many threats which cannot be easily addressed by the traditional protection methods. One significant set of such attacks is denial-of-service (DoS) which is concerned with satisfying user or system domain buffers. But in wireless realm, attackers may attain ability to prevent legitimate nodes from communication by capturing the medium. It is because wireless networks are constructed via open medium which creates a trouble-free path for intruders to introduce such attacks [3]. In wireless network defenses like cryptography, pass-phrase sharing etc., can be overrun by a simple DoS attack that can shutter the whole network.

Jamming is a special category of DoS attacks which is used in wireless networks, where an attacker disrespects the medium access control (MAC) protocol [1] and transmits on the shared channel; either continuously or periodically to target all or some communication, respectively [4-6]. Figure 1 shows a jamming scenario in wireless network, where the red area marks the jammed region. Since, jamming cannot be handled other than preventing it, either using logical or physical retreat. Such schemes are generally employed at the MAC layer and so is our emphasis in this study, but other approaches are not being ignored. Additionally, we

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

focus on the network nodes having only single antenna. We initially enlist the variations that the jammers are capable of in next section. The third section comprises of the basic parameters and metrics that are helpful in detection of a jamming attack. Unlike other security attacks, jamming attacks are handled by avoiding the malicious entity via escape; either physically or logically. Such retreats are discussed in the following section. Thereafter, we discuss the mitigation techniques that are used and have been proposed in near past, followed by a critical review of the said studies. Finally, we conclude and highlight future directions.

2. JAMMING CHARACTERISTICS AND EFFICIENCY CRITERIA

Firstly one should know what jammer is. According to [7] jammer is defined as an individual who is intentionally obstructing the methods of legal wireless communication. Such an individual is treated as an active attacker depending upon its intentions and actions. From the jammer's perspective, it can accomplish its aim from seizing the sender such that it is unable to transmit or, as a second option which is found better, hinder the receiver so that it cannot understand the message completely or partially. For the sake of concept, suppose that in communication of the two nodes where jammer, residing nearby, can prevent the sender from initiating a data communication by constantly emitting low powered signals on the channel; allowing the sender to presume that the medium is occupied. Alternatively, if for some reason the data is transmitted successfully, jammer can target the receiver's end via inclusion of noise in the transmitted packet. Thus, jammer can target a whole area in its range or a particular transmission.

Before going into the details of tackling and mitigating a jamming attack, it is vital to overview some factors and measures on the basis of which jamming attack is categorized and identified. Ideally [8], jammer ought to have elongated energy to continuously hinder the communication. Additionally, it should adopt the methodology not to get detected. A third criterion is that it should disrupt the communication to possible extent i.e. level of DOS attack depends on interests of jamming scenarios. That is, an adversary with restricted energy will not be much effective, because the primary concern will be to lengthen its existence on the network, rather than efficiently disrupt the communication. [9] specifies the factors that are extensively utilized for measuring jamming effectiveness:

- Energy competence
- Likelihood of Exposure
- Domain of DoS
- Potential alongside physical layer techniques

In order to measure the degree to which a jammer assures these factors, [7] analyzed and discussed two methods that are of great importance:

Packet Send Ratio (PSR): Packet send ratio depends on the number of packets, which are successfully sent out, to the amount of packets that were intended to be sent out. Due to broadcast nature of wireless medium there is always chance of interference, we can not provide surety of non interference [10]. If 'm' is the number of packets sent out and 'n' being the quantity of packets which were intended to be transmitted, then PSR can be defined mathematically as:

$$PSR = \frac{m}{n} = \frac{Packetsent}{Packetsintendtobesent}$$

PSR can be easily measured by wireless device that keeps track of amount of packets it wanted initially to send in correspondence to the actual packets successfully transmitted.

Packet Delivery Ratio (PDR): PDR is defined as numbers of packets that are received by recipient compared to of packets that have been sent out by source [10]. If 'q' is number of packets received and 'm' being packets transmitted then PDR can be defined mathematically as:

$$PDR = \frac{q}{m} = \frac{Packetsreceived}{Packetssent}$$

Even after packets are sent out by A, B can not receive message completely due to presence of X. PSR can be easily calculated by the amount of packets that successfully passed CRC at B with respect to overall packets received.

3. JAMMING ATTACK MODELS

From the physical layer perspective, the jamming attack can be classified as follows [11]:

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

3.1. Noise Jamming:

The channel bandwidth used by the targeted system is jammed with noise energy. This raises the level of background noise at the receiver and makes it difficult to detect frames correctly. In other words, the SNR (Signal-to-Noise Ratio) at the receiver end is decreased.

3.2. Bit Jamming:

Jamming at the same frequency and modulation scheme as the targeted system seriously decreases the network performance as the devices try to detect a known pattern in the bit stream allowing them to synchronize. Since this modulated signal may not be filtered out like white noise, it decreases the SNR at the receiver and occupies the channel heavily.

3.3. Frame Jamming:

Jamming thorough frames according to the targeted system is hard to detect, because the jamming signal is masked as regular frames. Its impact goes beyond minimizing the signal-to-noise ratio. Due to unfairness of jammer, the channel may be occupied over long periods of time. Depending on the system, this might be achieved with very low energy consumption by periodically announcing long duration frames which forces the participating nodes to remain in silent mode for this amount of time.

Furthermore, from viewpoint of jammers the use of additional information at the MAC layer can increase their effectiveness. For a channel aware jammer, a single jamming pace is usually applied for every likely status of channel like busy, idle, etc. In a continuous-time model, signals are produced based on Poisson distribution having diverse ratio for varying status. Additionally, intelligent jammers may have varying states depending upon the targeted communication. e.g. reactive jammer seeks a non-colliding transmission and immediately targets it with a particular possibility of collision.

3.4. Types of Jammers

A jamming strategy describes the way an attacker disturbs the medium. Besides the time-based strategies, where the jamming signal is active only in specific time intervals, there are more advanced jamming schemes possible which make use of knowledge about the physical and link layer specifications of the targeted system. Based on the selected strategy, the effective jamming is then performed by emitting an appropriate radio frequency signal. This could be noise or modulated signals. The device that generates a noise and creates intrusion for network is referred as a jammer [12, 13]. [12] explains different types of jammer. Most common ones are known as proactive and smart jammers as discussed below:

3.4.1. Proactive Jammers

The jammer emits a signal irrespective of the regular network traffic [3]. Figure 2 shows the effect of proactive jammers on the network during packet transmission.

a) Constant Jamming:
It continuously emits a signal on the medium meaning that there are no silent time intervals in its transmission. Hence, forcing legitimate nodes in the range to always back-off, i.e. starve.

b) Periodical / Random Jamming:
In contrast to the constant jammer, a periodical jammer suspends its transmission during a specified time in regular intervals. A modified version is the random jammer, which uses a random duration, a random interval or both.

3.4.2. Smart Jammers

If the jammer uses a certain a priori knowledge of the used communication system in order to optimize its attacks, then it is treated as a smart jammer. As attacks of this type highly depend on the used communication system, there are an infinite number of possible strategies, major ones being [3]:

a) **Reactive Jamming:**
Reactive jamming requires the sensing of the channel. As the transmission is detected, jammer starts its intrusion. A more advanced form of reactive jamming includes the analysis of the detected regular data stream. The jamming is then applied systematically to frames from or to specific nodes or to frames of a certain type.

b) **Deceptive Jamming**:
Deceptive jamming denotes attacks where false messages are sent to the channel with the objective of disturbing the organization of the network. In case of WLAN, this could be spoofed management or control frames for example. This way, also higher layer vulnerabilities may be easily exploited in order to launch denial of service attack.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

c) **Brilliant Jamming:**
Brilliant jammers attempt to change specific bit patterns of the frames. However, this requires a very high timing precision and significant a priori knowledge of the target signal structure.

d) **Frequency Swept Jammer:**
It provides continuous transmission which varies over a range of frequencies at a specified rate. The sweep through the frequencies is modeled by sampling the encompassing sweep bandwidth into a specified number of frequency intervals and continuously cycling through these intervals, issuing an equal length transmission at each step.

3.4.3. Mobile Jamming

Another form of jamming is the mobile jamming attack that not only threatens the MAC or physical layer, but also breaks the routing in an adhoc network. As the name represents mobile jammer has mobility and sneaks in the critical path based on the information it collects overtime by eavesdropping the amount of traffic load and the direction of the dataflow. Besides, the mobile jammer can decide when to jam an area based on the value called jamming threshold. Mobile jammers are more successful in environments where nodes have no or less mobility and a single channel is used for communication, e.g. wireless mesh networks and WSN. To overcome mobile jamming multiple dataflows are introduced in a network so that even if one dataflow and its critical path get compromised network traffic does not face a bottleneck [14]. From the jammer's perspective, it eavesdrops for a continuous communication first and learns the delivery direction and the traffic load. If the traffic load does not reach the jamming threshold, this mobile jammer then moves to the upper link following the dataflow and eavesdrops again. Jammer will not be detected by network during this monitor phase. If the traffic load reaches the jamming threshold, the mobile jammer begins to jam the network. Mobile jammer normally arrives at the critical path at this time, as the critical path disruption plays an important role on the network.

Furthermore, from viewpoint of jammers the use of additional information at the MAC layer can increase their effectiveness. For a channel aware jammer, they have basically single jamming rate for each possible state of the channel (e.g., busy, idle). Additionally, intelligent jammers may have varying states depending upon the targeted communication.

4. TECHNIQUES OF DETECTING JAMMING ATTACKS

For the detection of jamming attacks, several practical implementations are possible. One approach is to perform the detection on the active nodes during their own transmissions. Since these nodes have a different view on the data flow depending on whether they act in the role of the transmitter or receiver, they define two separate algorithms for both cases, i.e. transmitter-based and receiver-based detection, depending upon where among both the parties the detection algorithm is initiated. The *dedicated- technique* is useful in scenarios where the power consumption and device complexity of most of the participating nodes should be low. The detection is then performed by only one or a few nodes having enough resources available. Finally, the development of a *cooperative-technique* is motivated by the expected increase of detection performance compared to the standalone detection mechanisms, since a broader view of the network is available. In the following, each of the four detection strategies is discussed [15]. Additionally, another detection strategy of jamming discussed by [16] is RF finger printing being useful for the wireless networks. If the fingerprint of the wireless network is not identified or considered as a threat then the security of the network can be increased by testing the legitimate user to ensure its authentication.

4.1. Transmitter-Based Detection:

In a wireless ad hoc network, the communication takes place among different nodes by sending and receiving data frames. So every node can transmit and receive the data at the same time. Different detection approaches of jamming exists, consider an ad hoc network with node *A* sending to node *B*. To apply the decision algorithm [15] which is described in the previous section, the transmitter has to determine the four metrics, as follows

- PDR (Packet Devilry Ratio)
- RSSI (Received Signal Strength Indication)
- PHY rate (Physical Rate)
- Noise

4.2. Receiver-Based Detection:

The main difference between receiver-based and transmitter-based detection lies in the computation of the PDR. Although in transmitter based

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

detection, the transmitter knows the exact number of data frames sent including all retransmissions; this being a priori not known at the receiver since several frames might get lost during transmission. Therefore, it is necessary that the data frames contain additional information which enables the receiver to determine the total number of sent frames. This can be achieved by adding a sequence number to every single data frame, as in the WLAN standard [15].

4.3. Dedicated Detection:

In case of dedicated detection [15], the RSSI and PHY rate are read from the acknowledgement frames arriving from the receiver, i.e. node *B*. As always, the noise level is taken from arbitrary frames arriving at the monitor. Based on the gathered statistics over several ACK frames, the monitor then applies the decision algorithm. Finally, the node dedicated to the jamming detection announces his decision to the other participating nodes in a broadcast frame. This broadcasting is then repeated whenever the decision changes in future.

4.4. Cooperative Detection:

This detection scheme is the combination of all the previous three strategies. In this case the technique is to share all the information at all nodes among each other and to make a decision based on this broader view. This means that every participating node in the ad hoc network gathers its own information, independently using any of the above techniques and shares with its neighbors.

4.5. Detection through RF Fingerprinting:

RF finger printing is used as the way of increasing the wireless network security. As the transmitter of the radio activates, the transmission of the RF signals demonstrates the temporary behavior with reference to the instantaneous frequency and amplitude. The time duration of the transient performance can be changed due to the type of the model and type of the transmitter. The difference between the same types can be observable which can be caused due to the aging and the manufacturing tolerance of the devices. The unique turn-on transient signal behavior is called the RF finger-print of a radio and can be used to identify the transmitter [17].

5. PREVENTION TECHNIQUES FOR JAMMING ATTACKS

In this section we survey the methods of mitigating a jamming attack that include use of spread spectrum at the physical level, followed by MAC layer approaches to evade and retreat a jammed channel; either physically or logically moving away from the jammer. Finally, the techniques of resumption of network nodes to reestablish a network are discussed.

5.1. Spread Spectrum

Spread spectrum has two basic motivations [18]:

- **Provide resistance against jammer**
- **Hide communication**

In a wireless environment, most commonly used anti-jamming technique at physical layer is spread spectrum based communication. However it does not fully secure communication against jamming attack. Major drawback being that invader does not have to be conscious of whole spectrum alteration progression in order to interrupt communication. For instance, in the case of voice communication, small part of conversation between human users, if corrupted will have a minor effect on the quality of communication.

5.2. Evasion Techniques

5.2.1. Channel Hopping

When jammed, communicating nodes hop on to a new channel independently and try to get synchronized with other participants. However, when any node is unable to communicate for a certain period of time it starts listening on other channels in order to sense whether its neighboring nodes have hopped on due to jamming or not [19-24]. We will further investigate about the typical techniques adopted for temporal retreat in the later section.

Nevertheless, another technique worth mentioning in this regard that provides urgent and robust response to the jamming attack is known as MULEPRO [25]. It stands for MULti channel Ex-filtration Protocol. It is designed to quickly Ex-filtrate the sensed data from jammed region to the area which was currently not under jammer. This technique is suitable for many types of network applications like perimeter and infrastructure defense system, homeland security systems, battlefield sensing systems etc.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

5.2.2. Spatial Retreat

Spatial retreat is a mechanism to physically evade the jammed area. The rationale behind this strategy is that when an area is jammed in the wireless network, based on the detection algorithm all nodes try to estimate the jammed region and flee physically in the direction of safer place. Based on their estimation about the jammed region, nodes independently opt for shortest path to avoid being jammed and move accordingly. Figure 4 shows the spatial retreat approach for two party communication scenario [9]. The area illustrated via slashed stripes is jamming range. As wireless networks are vulnerable to such intrusion which interrupts node communication, therefore to survive against such interference basically two approaches are used in this technique:

i. Jammed Area Mapping (JAM)

This mechanism employs scattered approach to draw the jammed area so communications with that part of the network node can be avoided during specification of routes [26]. Once, out of the jammed region legitimate nodes try to relocate others and hence, may change their direction and speed according to the predefined algorithm [27].

ii. Node Escape

This technique is for the physical escape of the node from the jamming location. In view of the fact that mostly devices of a wireless network are mobile, like cell phones or WLAN enabled laptops, this technique is more likely to be adopted. Main theme being to move away from the jammed area and periodically sense the medium if it has become interference free. This procedure is repeated till node reaches to an interference free location [7].

5.2.3. Retreat Restoration

A very important phase of handling jamming in an adhoc network is to restore a network to non-defensive mode when the attacker goes out of range. This phase is highly important because in adhoc networks our prime focus is to conserve energy utilization so as to prolong lifetime of nodes. In a proactive defense mode energy consumption is increased by manifolds. Hence making it all the more vital to bring down network nodes to a normal level of energy consumption essential for basic functionality in terms of performance. Retreat restoration can take place in either the manner; by coordinated or uncoordinated communication. The communication is based on a pre planned hop pattern between senders and receivers. Such pattern is already decided among the network nodes prior to starting communication and as soon as nodes intend to get in synch with any particular node they switch channel or frequencies according to the pre-defined pattern to find the receiver node [28]. Such pre-defined hop coordination can be a formula for finding the right control and data channel.

5.2.4. Hybrid Approaches

These approaches are the ones which have defined new protocols based upon multiple of existing approaches to present an even effective anti-jamming mechanism. Some approaches involve preemptive channel hopping or frequency hopping [29,30] instead of reactive ones in order to prevent getting into a state where jamming disrupts normal communication. Other implementations include synchronous and asynchronous spectral multiplexing where the concept of intermediary nodes has been introduced to communicate at multiple channels. When a node changes its channel because of jamming one of its neighbors takes upon itself to communicate with the node on its new channel and rest of the network on the old channel [31]. Another strategy which targets prediction of nodes which are about to be jammed and hence should be removed from routing in a wireless network. This strategy uses LEACH as its base routing protocol and uses JAM for predictive determination of jamming holes [32].

DEEJAM [33] protocol is an amalgamation of frame masking, channel hopping, packet fragmentation and redundant encoding in order to avoid all four types of jamming classes and succeeds in reducing pulse jam attack impact to 11%. However the extra computational overhead in these approaches is unresolved. This magnifies in situations where there simply is no jammer in the vicinity. Swarm intelligence is yet another strategy finding its popularity in field of wireless routing and other issues related to WLAN. One such swarm based methodology is simulation of ants behavior in path translation to a food source. This method is very effective and energy efficient as is based on a natural process of pheromone laying and determining optimum routes [34]. However implementation details of this process are pretty complex, as volatility of this process and intelligent learning is a little difficult to model.

5.2.5. Cognitive Radio

[35] In his study describe some attack mitigation schemes like robust Sensory Input, Mitigation in

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Individual Radios, and Mitigation in Networks. In robust sensory input, the improved input sensor helps significantly to reduce the credulity of cognitive radios. For example, if radios could carefully characterize the difference between interference and noise, they could distinguish between natural and man-made RF events. Such sensors could also feed specialized policy engine subroutines that specifically look for hostile signals that may be attempting to corrupt a radio's beliefs. [36] describes the typical cognition cycle of *Observe! Orient! Plan! Decide! Act*. If the radio maintains learning, whenever this loop results in a new operating state for the radio, another stage called Learn is injected into the cognition cycle that allows the radio to add to its memory information about how the radio transitioned to this new operating state information that can be used by Plan and Decide in future cognition cycles. Improving sensor input can significantly help reduce the gullibility of cognitive radios.

Discussion on Proposed Algorithms

So far we overviewed the general techniques that exist in mitigating the jamming attack, either detection or retreat. In this section we investigate deeply on other ideas that can be applied to handle a jamming attack, both on control and data plane. Table-1 presents a logical division of all the techniques and proposed algorithms that have been highlighted earlier. In this section we will discuss them in detail on the basis of the category the study lies in. The listed studies are of recent years, some emphasize only on a single approach whereas others have focused on combination of strategies (like detection and retreat, etc.). Additionally, some have categorized the jamming attack on basis of control and data packets. Lastly, based on varying jamming attacks by a single intelligent jammer, protocols suites that avoid such jammer are also present.

Even though, the focus of this study is on the MAC layer approaches that have so far been proposed to tackle a jamming attack, however we will start with the physical layer approaches first. Physical layer metrics help in deciding anti jamming strategies and suggest changing physical level details of communicating traffic. The said change may be in form of implementation of spread spectrum (FHSS or DSSS) or in form of accommodating extra information in basic packet headers. Under this category are also studies which suggest modification of communication packet size (packet fragmentation) and hiding of packet header markers (frame masking) as suggested in [33]. [14] focuses on the frequency hopping spread spectrum (FHSS) and direct sequence spread spectrum (DSSS), considered to be highly resilient in jammed environment at the physical layer. The major contribution of this work is the analysis of a variety of counter measures opposing jammers which facilitate the network to endure and employ correctly in a seized situation. Authors have recommended the utilization of a particular FHSS method in 5 GHz band having 55 channels. Using a secret key shared between the source and the sink nodes, a channel sequence may be generated. Each channel uses DSSS modulation with 16 bit Pseudo Noise (PN) code, which derives from the same secret word used for FHSS channel generation. [29] proposed a new mechanism to mitigate jamming attacks via random channel selection protocol, especially developed to facilitate communication among nodes in the presence of jammers. To make this possible the pair-wise key pre-distribution protocol is used which is based on bi-variate polynomial in order to build a secure random frequency hopping schedule between two nodes. The major limitation being in above techniques either the typical issues that exist in cryptography for key exchange methods or the involvement of higher layers against intelligent jamming.

[3] Explains the detection of jamming attacks in WLANs on the control packets i.e. RTS and CTS jamming and a CUSUM based detection method is proposed, that is capable of locating a jammer precisely at the cost of small storage and computation. A transformation-point is detected due to contiguous fake packets on the medium, when such points are noticed in the traffic patterns received; alarms are triggered to intimate all. [34] Proposes an Intrusion Detection System (IDS) that satisfies requirements and conditions of WSNs. Preventive mechanisms are generally required to defend against such intrusions. Though, certain intrusions exist where no well-known avoidance methodology can be applied and hence, becomes essential to utilize some means of intrusion detection. This way, not only the network is avoided from any harm caused by the intruder, but also helps in developing prevention system by analyzing the attacking techniques.

[8] proposes channel hopping and physical shift away from the jammed area and demonstrated it using Mica2 networks. However, the focal point being the methodologies to determine the instance about jammer being active. (afterwards in [16]),

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

instead of proposing an avoidance scheme, overall. Besides, authors did not address the overhead involved in channel hopping or inspecting about existence of jammer. [30] considers a situation about a complex jammer that congests an environment with fake packets using single channel communication. Probability based signals are emitted by the jammer so that maximum loss with respect to communication links occur over the network. Additionally, the jammer is smart enough to seize itself when a monitoring node transmits a notification message out of the jammed region, and knows it has been detected. Monitoring node identifies the jammer with the help, of an optimal detection test, of packet clashes that took place over a period of time. Once triggered by the monitoring node, the network calculates the likelihood of channel access, to minimize frequent jamming identification and notification messages. [7] mainly explains the physical evasion needs the nodes being mobile and thus not energy efficient in environments like sensor networks. The theme in this approach lies that when nodes being mobile face distortion on a particular location continuously, ought to merely fly out in search of a secure region. It is usually an attractive technique for wireless networks as devices are generally mobile, like cell phones or WLAN enabled laptops. However, the main concern of adopting this technique is to come up with the tactic through which devices need to fly away, while being in synchronization with other members of the network.

Another technique which provides urgent and robust response to the jamming attack is known as MULEPRO [25]. It stands for MULti channel Ex-filtration Protocol and is designed to quickly Ex-filtrate the sensed data from jammed region to the outer area. Major strength of this technique lies in distributed nature, where all nodes based on a single seed value can calculate the time slot and channel where data communication will take place. [28] In his study explains Asynchronous Multi-channel Coordination Protocol (AMCP), a MAC protocol that works in a distributed fashion, which enhances cumulative network throughput, also tackles with elementary synchronization issues that lead to isolation. AMCP realistically develops and verifies via case scenarios, an estimated lesser range on the throughput of any flow in a random setup. On the other hand, it considerably conveys enhanced throughput with respect to each flow as compared to WLAN and multichannel propositions. However, complexity for these techniques enhances with the increase of nodes.

Temporal retreat is a mechanism to logically avoid the jamming area by changing the channel order a node communicates on. This mechanism gives an impression to the attacker that the node is not available on the same channel anymore and hence the retreat without any physical movement. [37] proposes an Uncoordinated Frequency Hopping (UFH) technique which is independent and individually applied by all nodes. The problem of jamming resistant key establishment can be solved by some anti jamming techniques like FHSS or DSSS that favors devices for communicating the key establishment; condition to that a secret spreading key/ code has been carved up, in advance. Even though, this condition being quite minimum, but generates a cyclic reliance among key arrangement and spread spectrum based communication; and is yet to be addressed.

[38] highlights complexity of equality in uncoordinated deployments, emphasizing mainly on channel assignment view point in a wireless environment. The proposed answer lies on the idea of temporal retreats. It is distributed in nature, involves no prior harmonization between APs owned by various hotspots, is simpler to employ and finally compatible with in-hand standards. Specifically speaking, proposed idea is called MAXchop, that works effectively with non-overlapped wireless channels. Although, is found efficient in exploiting partially-overlapped channels, in particular. Additionally they assess how the said approach (of channel assignment) balances itself with earlier anticipated carrier sensing schemes to provide additional performance enhancements using widespread simulations.

Since, jamming is considered a severe threat for wireless networks, as normal measures fail to secure and counter it. [39] explains the two defense strategies of jamming mitigation with respect to single and multiple antenna apparatus. These are proactive and reactive channel hopping. Proactive channel hopping algorithms have been of prime concern so far as compared to reactive techniques. From single-radio point of view, theoretical models have been developed to investigate the blocking probability for combinations of defense and attack strategies. In multiple antenna devices, jamming problem was applied min-max game theory and using simulation illustrate that the result of the game is dependent on the payoff function.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Additionally, authors demonstrate that reactive techniques offer improved jamming resilience as compared to proactive ones, but are the same in terms of energy efficiency.

Mobility lists down papers which have presented solutions for catering to mobility as a property of communicating nodes in a network as well as of the attacking jammer. It also lists down approaches to diminish affects of a mobile jammer, evading which is much more complex and energy consuming than other forms of attacking jammers. Distinct feature of such approaches is the "Restoration phase", where network nodes assume their original communication positions as they were prior to getting under the influence of a mobile jammer. [40] discusses a novel and powerful jamming attack called mobile jamming attack. Besides, he proposes a multi-dataflow topologies scheme that can effectively defend the mobile jamming attack. The simulation results of this study demonstrate that the mobile jamming attack is more devastating than traditional jamming attacks and the proposed defense scheme can effectively alleviate the damage. [41] presents three defense techniques: reactive, proactive, and hybrid. MMAC marks work, which present use of multiple channels as an inherent communication property in an adhoc network. This category is more focused towards proactive use of channel for overcoming affects of a jammer in surroundings.

Finally, jamming is not being taken as an adversary always; instead it can be used in a constructive manner among network nodes, as in [45]. Using jamming on unwanted traffic helps save other nodes from trying to process them as legitimate information and hence conserve energy.

Conclusion and Future Directions

Jamming attack is different from its other counter parts, as it cannot be mitigated like the others. The severity increases many folds in a wireless environment due to lack of detection and prevention mechanism in 802.11 standards [1]. In this paper, we surveyed the ways through which an attacker can disrupt the medium. It has been analyzed that in addition to the time-based strategies, in which the jamming signal is active only for a specified interval of time, there are efficient jamming schemes possible which make use of knowledge about the physical and link layer specifications of the targeted system. Hence, an intelligent jammer can survive longer on the network.

Jamming attacks are avoided by escaping from the jammed area. In case of mobility as in WLAN, legitimate jammed nodes need to be equipped with jamming detection technique, via which they can physically escape from the jammed region and later try to relocate other nodes by periodically moving and sensing beacon messages from others. Nodes flee out of the jammed region by estimating the jammer's signal strength on the basis of jammer detection mechanism. So far, the jamming attack detection mechanisms are threshold based and may increase false alarm rate. Additionally, the relocating algorithm to find peer nodes is independently run on each node, via randomly chosen speed and direction. The combination of above stated algorithms is quite complex and is found effective in dense environment, only where chances of relocating other nodes is higher.

The use of multi-channel in wireless networks has been in focus for increasing throughput and use of simultaneous communication in the same vicinity. However, the additional channels are also a solution against single band jammers where legitimate nodes hop to another channel either on the basis of earlier coordination or randomly chosen channel where they can later try to resume communication with others. Besides, for uncoordinated escape from jammer as in adhoc network, uses of boundary nodes is considered useful for the nodes stuck in jammed region and are unable to move away. When the wireless network gets jammed, each node becomes independent, as it is unable to communicate with others and thus all above techniques are applied by the node autonomously, requiring more power and energy consumption. Furthermore, channel switching has its own overhead involved but is found valuable for stationery nodes having large number of channels, especially against frequency swept jammers.

As discussed earlier, that proactive and reactive algorithms have approximately same energy consumption in case of jammer avoidance, generally. However, the added advantage in using the earlier ones is that no detection mechanism is needed. Therefore, couple of studies has proposed proactive protocol suites in WLAN and WPAN environment. But the challenge is of developing such protocols for MANETS, especially against intelligent jammers with the emphasis on energy efficiency.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

REFERENCES:

[1]. IEEE 802.11, 1999 Edition (ISO/IEC 8802-11:1999). IEEE Standards for Information Technology – Telecommunications and Information Exchange between Systems – Local and Metropolitan Area Network – Specific Requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.

[2]. Salem M., Sarhan A., Abu-Bakr M., "A DOS Attack Intrusion Detection and Inhibition Technique for Wireless Computer Networks", ICGST- CNIR, Volume (7), Issue (I), July 2007.

[3]. Xu W., Trappe W., Zhang Y., Wood T., "The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks", In Proceedings of the Sixth ACM International Symposium on Mobile Ad-hoc Networking and Computing (MobiHoc), Urbana-Champaign, IL, USA, May, 25-28, 2005.

[4]. Ståhlberg M. , "Radio Jamming Attacks Against Two Popular Mobile Networks", Seminar on Network Security. Mobile Security. Helsinki University of Technology, Fall 2000.

[5]. Noubir G., Lin G., "Low-power DoS Attacks in Data Wireless LANs and Countermeasures," in proceedings of the Fourth ACM International Symposium on Mobile Ad Hoc Networking and Computing, Annapolis, MD, USA, June 1-3, 2003.

[6]. Bayraktaroglu E., King C., Liu X., Noubir G., Rajaraman R., Thapa B., "On the Performance of IEEE 802.11 under Jamming," in Proceedings of IEEE 27th Conference on Computer Communications (INFOCOM'08), Phoenix, Arizona, USA, April 13 - 19 2008.

[7]. Xu W., Trappe W., Zhang Y., "Defending Wireless Sensor Networks from Radio Interference through Channel Adaptation," ACM Transactions on Sensor Networks (TOSN), Volume 4, Issue 4, August 2008.

[8]. Xu W., Wood T., Trappe W., Zhang Y., "Channel Surfing and Spatial Retreats: Defenses Against Wireless Denial of Service, " in Proceedings of the 2004 ACM workshop on Wireless security (WiSe), pg. 80 - 89, 2004.

[9]. Acharya M., Thuente D., "Intelligent Jamming Attacks, Counterattacks and (Counter)2 Attacks in 802.11b Wireless Networks", in Proceedings of the OPNETWORK Conference, Washington DC, USA, August 2005.

[10]. Zhang Z., Wu J., Deng J., Qiu M., "Jamming ACK Attack to Wireless Networks and a Mitigation Approach," in Proc. of IEEE Global Telecommunications Conference - Wireless Networking Symposium (GLOBECOM '08), New Orleans, LA, USA, November 30-December 4, 2008, vol. ECP.950, pp. 1-5.

[11]. Bayraktaroglu E., King C., Liu X., Noubir G., Rajaraman R., Thapa B., "On the Performance of IEEE 802.11 under Jamming," in Proceedings of IEEE 27th Conference on Computer Communications (INFOCOM'08), Phoenix, Arizona, USA, April 13 - 19 2008.

[12]. Wu S.L., Lin C.Y., Tseng Y.C., Lin C.Y., Sheu J.P., "A Multi-Channel MAC protocol with Power Control for Multi-Hop Mobile Ad Hoc Networks," The Computer J., vol. 45, no. 1, 2002. pp.: 101-110.

[13]. Hung W.C., Law K.L.E., Garcia A.L., "A Dynamic Multi-Channel MAC for Ad Hoc LAN," in Proceedings of 21st Biennial Symposium on Communications, Kingston, Ontario, June 2002. pp. 31-35.

[14]. Mpitziopoulos A., Gavalas D., Pantziou G., "Defending Wireless Sensor Networks from Jamming Attacks", in proceedings of The 18th Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC'07), Athens,. Greece, 3–7 September, 2007.

[15]. Chen K.C. "Cognitive Radio Networks", Ramjee Prasad Publisher John Wiley and Sons, 2009

[16]. Chen Y., Xu W., Trappe W., Zhang Y.Y., "Securing Emerging Wireless Systems": Lower-Layer Approaches, 1st Edition. 2009.

[17]. Ureten O. and N. Serinken, "Wireless Security Through RF Fingerprinting," Canadian Journal of Electrical and Computer Engineering, vol. 32, no. 1, pp. 27 – 33, Winter 2007

[18]. Peterson R. L., Ziemer R. E., Borth D. E., "Introduction to Spread-Spectrum Communications" Prentice Hall, 1st Edition, 1995.

[19]. Navda V., Bohra A., Ganguly S., Rubenstein D., "Using Channel Hopping to Increase 802.11 Resilience to Jamming Attacks", in proceedings of 26th IEEE International Conference on Computer Communications, Joint Conference of the IEEE Computer and Communications Societies, Anchorage, Alaska, USA, 6-12 May 2007.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[20]. Khattab S., Mosse D., Melhem R., "Modeling of the Channel-Hopping Anti-Jamming Defense in Multi-Radio Wireless Networks", in proceedings of MobiQuitous 2008, Dublin, Ireland, July 21 - 25, 2008

[21]. Nahrstedt K., Campbell R.H., Vaidya N.H., "Identifying Insider-based Jammers in Multi-channel Wireless Networks", in proceedings of GLOBECOM'10. Miami, Florida, USA, 6-10 December, pp.1-6

[22]. Nguyen H., Pongthawornkamol T., Nahrstedt K., "Alibi: A Framework for Identifying Insider-based Jamming Attacks in Multi-channel Wireless Networks", in proceedings of 16th ACM Conference on Computer and Communications Security (CCS), Hyatt Regency Chicago, IL, USA, November 9-13, 2009.

[23]. Lee E.K., Oh S.Y., Gerla M., "Randomized Channel Hopping Scheme for Anti-Jamming Communication", In proceedings of Wireless Days Conference, Venice, Italy, October. 2010.

[24]. Othman J.B., Hamieh A., "Defending Method Against Jamming Attack in Wireless Ad Hoc Networks", The 5th IEEE International Workshop on Performance and Management of Wireless and Mobile Networks (P2MNET 2009), Zürich, Switzerland; 20-23 October 2009.

[25]. Alnifie G., Simon R., "A Multi-channel Defense Against Jamming Attacks in Wireless Sensor Networks" In Proc. of the third ACM International Workshop on QoS and Security for Wireless and Mobile Networks (Q2SWinet 2007). Chania, Crete Island, Greece, October 22, 2007. pp: 95–104.

[26]. Wood A. D., Stankovic J. A., Son S. H., "JAM: A Jammed-Area Mapping Service for Sensor Networks," in Proceedings of 24th IEEE Real-Time Systems Symposium (RTSS), 3-5 December, 2003. pp: 286 - 297

[27]. Ma K., Zhang Y., Trappe W., "Mobile Network Management and Robust Spatial Retreats via Network Dynamics," in Proceedings of the 1st International Workshop on Resource Provisioning and Management in Sensor Networks (RPMSN05), Ohio, USA, November 7th, 2005.

[28]. J.Shi, T.Salonidis, and E.W.Knightly, "Starvation Mitigation Through MultiChannel Coordination in CSMA Multihop Wireless Networks" Proc. ACM MobiHoc, 2006.

[29]. Mahadevan K., Hong S., Dullum J., "Anti-Jamming: A Study". 2005

[30]. Li M., Koutsopoulos I., Poovendran R., "Optimal Jamming Attacks and Network Defense" In IEEE International Conference on Computer Communications (INFOCOM), Anchorage, Alaska, USA, 6-12 May, 2007.

[31]. Reese K.W. Salem A., "A Survey on Jamming Avoidance in Adhoc Sensory Networks" Journal of Computing Sciences in Colleges, Volume 24 Issue 3, January 2009

[32]. Soreanu P., Volkovich Z., Barzily Z., "Energy-Efficient Predictive Jamming Holes Detection Protocol for Wireless Sensor Networks" in Proceedings of the 2008 Second International Conference on Sensor Technologies and Applications (SENSORCOMM '08), Cap Esterel, France, August 25-31, 2008

[33]. A.D. Wood, J.A. Stankovic, and G. Zhou, "DEEJAM: Defeating Energy-Efficient Jamming in IEEE 802.15. 4-based Wireless Networks", in proceedings of 4th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks, (SECON '07), San Diego, CA, USA, 18-21 June 2007. pp: 60-69

[34]. R.Muraleedharan and L.A. Osadciw, "Jamming attack detection and countermeasures in wireless sensor network using And System" SPIE Defence and Security, Orlando, 2006

[35]. Clancy T.C., Goergen N., "Security in Cognitive Radio Networks: Threats and Mitigation," in Proceedings of International Conference on Cognitive Radio Oriented Wireless Networks and Communication. (CrownCom'08), Singapore, 15-17 May 2008.

[36]. Mitola J., "Cognitive Radio: An Integrated Agent Architecture for Software Defined Radio." Ph.D. Dissertation, KTH, 2000.

[37]. Strasser M. "Jamming-resistant Key Establishment using Uncoordinated Frequency Hopping" , in Proceedings of the 2008 IEEE Symposium on Security and Privacy, Oakland, California, USA , May 18-21, 2008

[38]. Mishra A., Shrivastava V., Agarwal D., Banerjee S., Ganguly S., "Distributed Channel Management in Uncoordinated Wireless Environments" in proceedings o The Twelfth Annual International Conference on Mobile Computing and Networking (MobiCom'06), Los Angeles, CA, USA, 24-29 September, 2006

[39]. Khattab S., Mosse D., Melhem R., "Jamming Mitigation in Multi-radio Wireless Networks: Reactive or Proactive?", in

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Proceedings of the 4th international conference on Security and privacy in communication netowrks (SecureComm '08), Istanbul, Turkey, September 22-26, 2008.

[40]. Hung-Min S., Shih-Pu H., Chien-Ming C., "Mobile Jamming Attack and its Countermeasure in Wireless Sensor Networks" in proceedings of 21st International Conference on Advanced Information Networking and Applications (AINA 2007), Niagara Falls, CanadaMay 21-23, 2007.

[41]. Khattab S., Moss´e D., Melhem R., "Honeybees: Combining Replication and Evasion for Mitigating Base-station Jamming in Sensor Networks", 2006.

[42]. Paula R. da Silva, Marcelo H.T. Martins, and Bruno P.S. Rocha, "Decentralized Intrusion Detection in Wireless Sensor Networks", in Proceedings of the 1st ACM international workshop on Quality of service & security in wireless and mobile networks (Q2SWinet '05), Montreal, Canada, October 10 - 13, 2005

[43]. Lin S., Wueng M., "Concurrent Multi-Channel Transmission (CMCT) MAC Protocol in Wireless Mobile Ad Hoc Networks" in proceedings of The 9th International Conference on Advanced Communication Technology (ICACT'07), Gangwon-Do, S.Korea, 12 Feb - 14 Feb 2007, pp: 445 - 449

[44]. Chen W., Chen D., Sun G., Zhang Y., "Defending Against Jamming Attacks in Wireless Local Area Networks" Autonomic and Trusted Computing, Autonomic and Trusted Computing, Lecture Notes in Computer Science, 2007, Volume 4610/2007, pp: 519-528, DOI: 10.1007/978-3-540-73547-2_53.

[45]. Martinovic, P. Pichota, J.B.Schmitt, "Jamming for good: a fresh approach to authentic communication in WSNs", in Proceeding of the second ACM conference on Wireless network security (WiSec'09), Zurich, Switzerland, March 16-18, 2009.

AUTHOR PROFILES:

Mr. Faraz Ahsan received his master in Computer Science degree from FAST, National University Karachi, Pakistan. Later, after spending a few years in industry, he is currently pursuing his PhD studies as a HEC scholar at COMSATS Institute of Information Technology, Islamabad. He conducts his research in the area of computer networks and distributed systems.

Ali Zahir received the Bachelor of Science in Telecommunication Engineering degree from National University FAST Islamabad, Pakistan in 2008. He is Research Associate in Department of Computer Science, COMSATS Institute of Information Technology, Islamabad, Pakistan and also pursuing his masters in Electrical Engineering from FAST Islamabad. His research interests includes Wireless Networks, Adhoc Sensor Networks, Data Networks, High Performance Computing, Parallel Computing, Clustering

Sajjad Mohsin received the M.Sc. Computer Science degree from Quaid-i-Azam University, Islamabad, Pakistan, in 1987, the M.E. degree in Computer Science and Systems Engineering from the Muroran Institute of Technology, Japan, in 2002, and the Ph.D. degree from the Muroran Institute of Technology, Japan, in 2005. He has 15 journal and conference publications. He is member editorial board of two international journals. He is Associate Professor in Department of Computer Science, COMSATS Institute of Information Technology, Islamabad, Pakistan. His research interests include Neural Networks, Genetic Algorithms, Fuzzy Logic, Soft Computing, Evolutionary Computing, Pattern Recognition, Vector Quantization.

Journal of Theoretical and Applied Information Technology
15th August 2011. Vol. 30 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

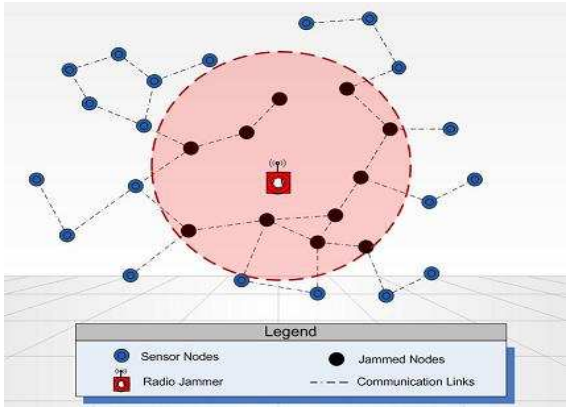

Figure 1: Jammed Scenario in a wireless environment.

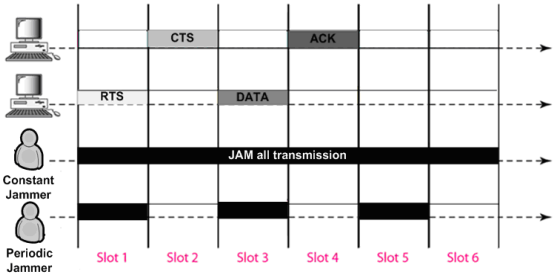

Figure 2: Effect of Proactive Jammers in Wireless network

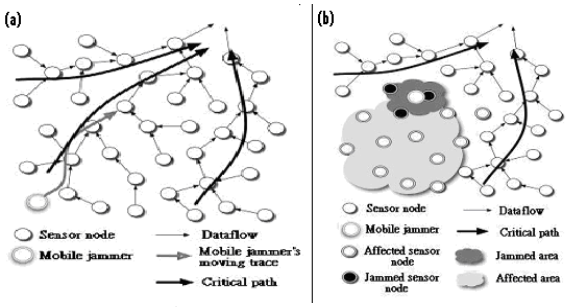

Figure 2: (a) Dataflow and Critical path in our network. (b) Mobile Jammer in an Adhoc environment Error! Reference source not found.

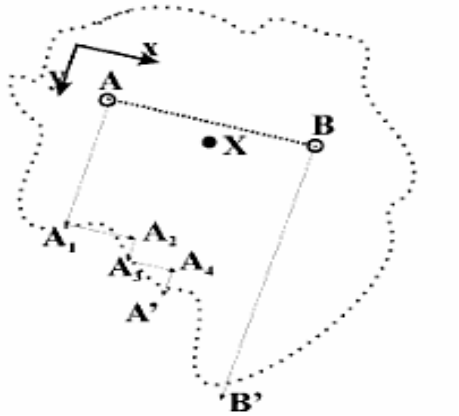

Figure 4: Spatial Retreat strategy for a two party communication scenario [9]

Table 1: Logical Division

Ref. No.	Author	Name of Technique (if any)	Detection	Spatial Retreat	Temporal Retreat	MMAC	Multi-Radio	Energy Efficiency
[7]	W.Xu		X	X	X			
[8]	W.Xu		X	X		X		X
[25]	G. Alnifie	MULEPRO			X	X		
[28]	J. Shi	AMCP	X		X	X		
[30]	M. Li		X		X	X		X
[33]	A.D.Wood	DeeJam	X		X			
[34]	R. Muraleedharan	Ant System	X					X
[35]	T.C. Clancy		X		X		X	
[37]	M. Strasser	UFH	X		X			
[38]	A. Mishra	MaxChop			X			
[39]	S. Khattab				X	X	X	X
[42]	A.Paula R.	DIDS	X					X
[43]	C.S.Lin	CMCT			X	X		
[44]	W.Chen		X					
[45]	Martinovic		X			X		X