ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 3, March 2018

A Taxonomic Survey on Heterogeneous Jamming Attacks and its Counter measures in Wireless Ad-hoc Network

Madhvi[1], Nisha Pandey[2]

M.Tech Student, Department of Computer Engineering, Shri Ram College of Engineering and Management, Palwal, Haryana, India[1]

Assistant Professor, Department of Computer Engineering, Shri Ram College of Engineering and Management, Palwal, Haryana, India[2]

ABSTRACT: Mobile ad hoc network (MANET) is the set of heterogeneous mobile nodes that are dynamically organized, self-configured and infrastructure less devices. Due to open nature of wireless nature, mobile nodes are very vulnerable. One of the main security threat in MANET is jamming attack. Jamming is a type of Denial of Service (DoS) attack in which advisory intentionally send radio signals between mobile nodes to disturb message communication. In this paper, we have discussed various jamming techniques and types of jammers. This survey overviews the major work done in the field of anti-jamming countermeasures with their pros and cons. This survey also provides several research directions for improvement in jamming attack.

KEYWORDS: Jamming attack, jammer, antenna, FHSS, DSSS, directional transmission, MANET.

I. INTRODUCTION

Now- a-days, wireless network [13, 15] turns out to be extremely prevalent for fast viable transmission, they can be based on different ways i.e. wifi network, GSM network, Bluetooth, LTE, etc. Wireless Ad- hoc network is a decentralized sort of wireless network that does not rely on pre-existing skeleton. It is a collection of versatile nodes that can be effectively self- compose with arbitrary and changeable topology to construct the network. Ad-hoc network are persistently escalating towards heterogeneous assaults and accomplishing worldwide figuring. The standard attribute of wireless medium is to share and converge with ware essence of wireless advances and an inexorably complex client- base, grants wifi network to be smoothly observed and relay on. Here, nodes assume both the part of transmitter and switch. Every portable node bargains specifically with each other while those nodes that are not specifically associated with wifi, convey by sending their traffic through relay nodes. In turn, the ad hoc network is resilience, low-priced and robustness and therefore well appropriate for military exercises, crisis activities, catastrophe recuperation, large scale community networks, and small networks [1, 4]. As soon as network picked up prominence, the security of viable communication turned into an issue of research work. Mobile adhoc Network (MANET) is itself a self-governing, zestful and multi-hop network. It does not entail any fixed foundation and can be established dynamically. Due to its dynamic and multi hop nature it is highly susceptible to various types of attacks due to which MANETbecomes more endangered to different attacks such as DDOS, Black hole, Wormhole Replay, Flooding [12], Jamming, [1, 9] etc. that out- turn the pernicious effect of high level security. Thence, security is becoming gruelling day by day. Any hostile client can easily observed communication between two devices and eject false message to block or jam the regular communication.

Jamming attack arises due to continual sending of radio signals which obstruct the authorized communication between sender and beneficiary. Figure 1 demonstrates that jammer detect the communication set up onto the wireless channel.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 3, March 2018

It initiates to send radio signals which infuses dummy packets and recipient gets dummy packets rather than original packet send from transmitter. Attacker focuses on the packets of high significance

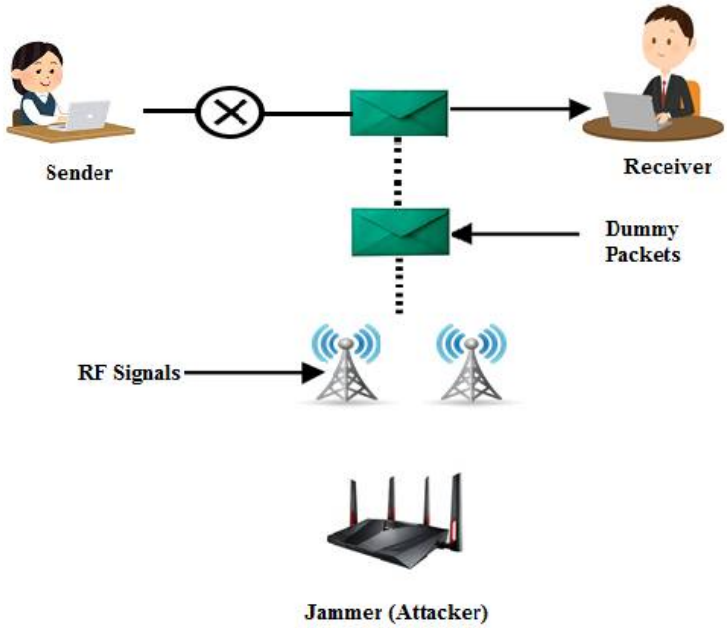

Fig.1: Pictorial view of jamming attack

II. RELATED WORK

Yanbo Dong et.al. [5] - Here, authors surveyed about control system regarding jamming attack with respect to three aspects i.e. attack, defence and arms race between them. They also reviewed various prevailing methods to deal with security issues by introducing gaming theory. They concluded that attacker's desire the jamming attack to be systematic having restraint energy and halted from being perceived by IDS. But defender's motive was achieving higher perceive accuracy by improving IDS to lessen the jamming attack's risk. In their future work, they suggested to merge game theory and machine learning algorithm to overcome security risk.

Sunakshi Jaitly et.al. [6] - In this paper, author surveyed about various security vulnerabilities and countermeasures against jamming attacks in wireless sensor network. They also provided extensive details about jamming techniques and different categories of attacker like proactive, reactive and functional specific jammer technologies with their pros and cons. They also discussed several limitations and challenges of wireless sensor network. Various countermeasures against jamming were also explained like using spread spectrum technologies, polarization of antenna and advantages of using directional antenna. They also concluded that a new defence mechanism was developed for the most sophisticated attacks, if these technologies were used appropriately.

Li Yuan et.al. [7] - In this paper, authors introduced a strategy to maximize the secure transmission rate against eavesdropping and jamming attacks. They modelled the power allocation problem as a stackelberg game where sensor was leader and jammer was follower. They also proposed stochastic algorithm with feedback (SAF) for an optimal value of proposed defence. For simulation they set bandwidth W to 0.2, noise level n to 1 and gain coefficient a as 5. Also they compared the proposed eavesdropping defence using 3 different scenarios namely Random Power Allocation (RPA), Power Allocation without regard to Smart Jammer (PAWSJ) and Power Allocation with Mistake (PAM). Simulation results shown that SAF achieved higher sensor's profit by assistance of control feedback as compared to RPA, PAWSJ and PAM since they have no feedback.

Kaito Kikuchi et.al. [8] - In this paper, authors developed a new consensus framework to deal with attacks where jamming is turned on or off very frequently. In the proposed approach, multi- agents attempt to communicate with neighbour at random time instants that are unknown by attacker. They took two different strategies of the attacker i.e. a

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 3, March 2018

deterministic attack strategy and a more malicious communication aware strategy. Authors concluded that stochastic communication protocol achieved consensus in finite time in both strategies but communication aware strategy was smarter as it allows the attacker to preserve the energy to be used later. In the future work, they suggested to incorporate probabilistic analysis of the consensus time as well as the analysis of communication aware strategy in the situation where the agents are not really synchronized and they endeavour communication at various circumstances.

Rupayan Das et.al. [9] - Here, the authors introduced an algorithm for comparing the effects of different network and physical layer attacks like wormhole, black hole, jamming, byzantine attacks in MANET and wireless sensor network. They used AODV routing protocol. For simulation, they took OPNET 14.5 simulator using some parameters like simulation area of 200m*100m, simulation time of 30 min and simulation speed of 256 bits/sec. Authors have taken following matrices i.e. throughput, load, delay and packet dropped for the analysis of different attacks. Simulation results shown that black hole attack experienced maximum delay since it has higher number of packet dropped as compared to other attacks while load was dependably lower in intruder free network and higher in intruder affected network and at last throughput for all network under any attack was always lesser as compared to network without attack.

Ali Aldarraji et.al. [10] - Here, authors proposed an enhanced countermeasure technique for jamming attacks by utilizing polarized beam forming with a planar array. The proposed technique was designed using the Linearly Constrained Minimum Variance (LCMV) criterion. For performance evaluation, signal to interference ratio was set to be -20dB and evaluated in terms of Bit Error Ratio (BER) to assess its information integrity and anti-jamming characteristics throughout various antenna array sizes. Authors integrated both polarization and space information to suppress undesired interference. After the results, authors concluded that proposed beam former fundamentally enhances the data framework execution when the jammer and desired signal are located intently in space domain. Also, the bigger the array estimate, the less data mistake occurred.

Harish Sharma et.al. [11] - In this paper, authors introduced a model for the detection of Denial of Service (DoS) in VANET with the use of Malicious and Irrelevant packet Detection Algorithm (MIPDA). Here, they also discussed various aspects of attacks in VANET. The proposed algorithm was based on continual position changing requirements of vehicle and attached with each and every RSU. They took frequency (f) and velocity (v) as parameters to analyse malicious and irrelevant packets. After the result, authors concluded that proposed algorithm ensures about generation of malicious and irrelevant packets, enhanced the security in VANET, avoid delay with correct packet generation as well as to analyse the strength of packet generation. In their future work, they recommend to use same approach for detection of multiple malicious, invalid and irrelevant request sent and received from multiple vehicles at a time.

Priyanka Sharma et.al. [12] - In this paper, authors proposed an enhanced security scheme in mobile ad hoc network to mitigate and block the effect of jamming attack. They proposed an algorithm for jamming control using AOMDV with prevention mechanism in which the PDR value of each node was calculated. They used NS-2 simulator and for simulation various parameters were used i.e. simulation area of 800m*600m, number of nodes 50, simulation time of 50 sec and AOMDV routing protocol. Simulation result shown that routing overhead minimizes while PDR was about 95% in presence of jamming attack. They also concluded that proposed approach provides zero infected data delivery in network and proper bandwidth hence performance was enhanced in presence of attacker. In their future work, they suggested to use some other routing protocol.

Ali Hamie et.al. [13] - Here, authors proposed a mechanism POWJAM- A power reaction against jamming attack to eliminate the jamming attack in wireless ad hoc network. They used POWJAM which was based on sending routing information, received routing information and data transmission power calculation. For simulation authors took NS-2 simulator. Simulation parameters used by them were traffic model CBR, routing protocol DSDV and packet size of 1024 bytes. They took throughput and packet delivery ratio as simulation scenarios having varying number of nodes and varying number of connections. After the results, authors concluded that PDR and throughput in POWJAN under jamming was less than network without jamming having varying number of nodes while PDR and throughput in normal network increase rapidly than in a network uses POWJAM under jamming with increase in number of connections. In their future work, they suggested to implement POWJAM in real environment.

Saira Beg et.al. [14] - In this paper, authors proposed an idea to engage a jammer on the jammed channel in MANET. In the proposed technique, the nodes flee away to avoid jamming, but resume on newer channel by alternatively visiting and sending legal packets on network in a coordinated manner. For performance evaluation, authors have taken OPNET simulator with 10 wireless stations having single transceiver only, traffic load of 10 packets/sec and jammed

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 3, March 2018

time of 10-40 sec. After the simulation, authors derived that more than 95% of communication was resumed by this scheme and nearly 85% of overall communication was successful during jam period depending upon traffic load and number of nodes.

Jalel Ben-Othman et.al. [15] -Here, authors proposed a new model to cope with jamming attack in ad hoc network. They also proposed the recovery protocol for receiver using cyclic redundancy code. Authors have used replicating packet redundancy technique to retrieve the jammed packet using some parameters like simulation area of 1500m* 1500m, transmission rate of 2Mbps and transmission range of 250m. For simulation they took NS-2 simulator. After the result, authors derived that throughput starts degrading under jamming attacks while packet delivery ratio remains higher, thus proposed approach maintain very high probability to cope with jamming attack. In their future work, they suggested to find an effective detection mechanism to detect the presence of jamming attacks.

In this broad study of jammer detection methods as shown in Table 1, only one matrices for detection of jammer has not been sufficient, so more than two different parameters were used in all the methods.

Table 1: Comparison of Jamming Detection methods

	Method Used	Technique	Complexity
[7]	Sensor's profit $U_m(P,J)$ and Jammer's profit $J_m(P,J)$	SAF	High
[10]	Polarized beam forming with planar array using LCMV	BER	High
[11]	Overhead, Correct packet generation	MIPDA	Moderate
[12]	Routing overhead, PDR	Security Scheme using AOMDV routing protocol	Moderate
[13]	Throughput, PDR	POWJAM	Moderate
[15]	Throughput, PDR	Replicating packet redundancy	High

III. JAMMING ATTACK

Jamming is examined one of the most common DOS attack, as well as severe security issue in wireless communication. Jamming attack is a unit someone is unfaltering attempting to restrain parallel to the physical transmission and also reception of wireless communication [18]. Practically speaking, Jamming attacks are executed by transmitting meddling RF signals on wireless channel without following an appropriate Media Access Control (MAC) and thus empowering the jammer to obstruct the data transmission over the network and possibly impacts the achievement of tactical operation.

Also, Jammer tries to hinder the communication by producing signals utilizing the same communication frequency, which expands the BER (Bit Error Ratio) at the recipient [13]. It can disturb the communication if the beneficiary is within the jammer's range. These attacks are illustrated in figure 2.

This attack is simple and effective. It just needs to get the communication band of present network through observing latently and after that attack can be quickly propelled. These attacks can attack the server to debilitate the restricted assets of CPU and memory of control system straight forwardly, it can likewise attack the communication channel specifically to cause jamming.

A. TYPES OF JAMMING [1, 15, 16] –

- *PHYSICAL JAMMING*-Physical jamming over wireless network is facile however it originate different types of DOS attack, which chiefly jam the channel or network by persistently sending jamming signals or radio frequency signals or by forwarding irregular packets. It retain entire control over the wireless medium. This formulate squander of time as each node go into holding up stage and need to hold up till the time jammer deactivate itself and channel turn inactive to imparts.
- *VIRTUAL JAMMING*-The utilization of Virtual sensing detecting system done at MAC (Media Access Control) layer. Virtual jamming plays an important role in diagnosing the existence of jammer in the network. There are various merits of MAC layer as compare to physical jamming for example, equivalent nodes; less power utilization. In MAC layer, the impact of jamming start off by assaulting on RTS/CTS frames or DATA/ACK frames.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 3, March 2018

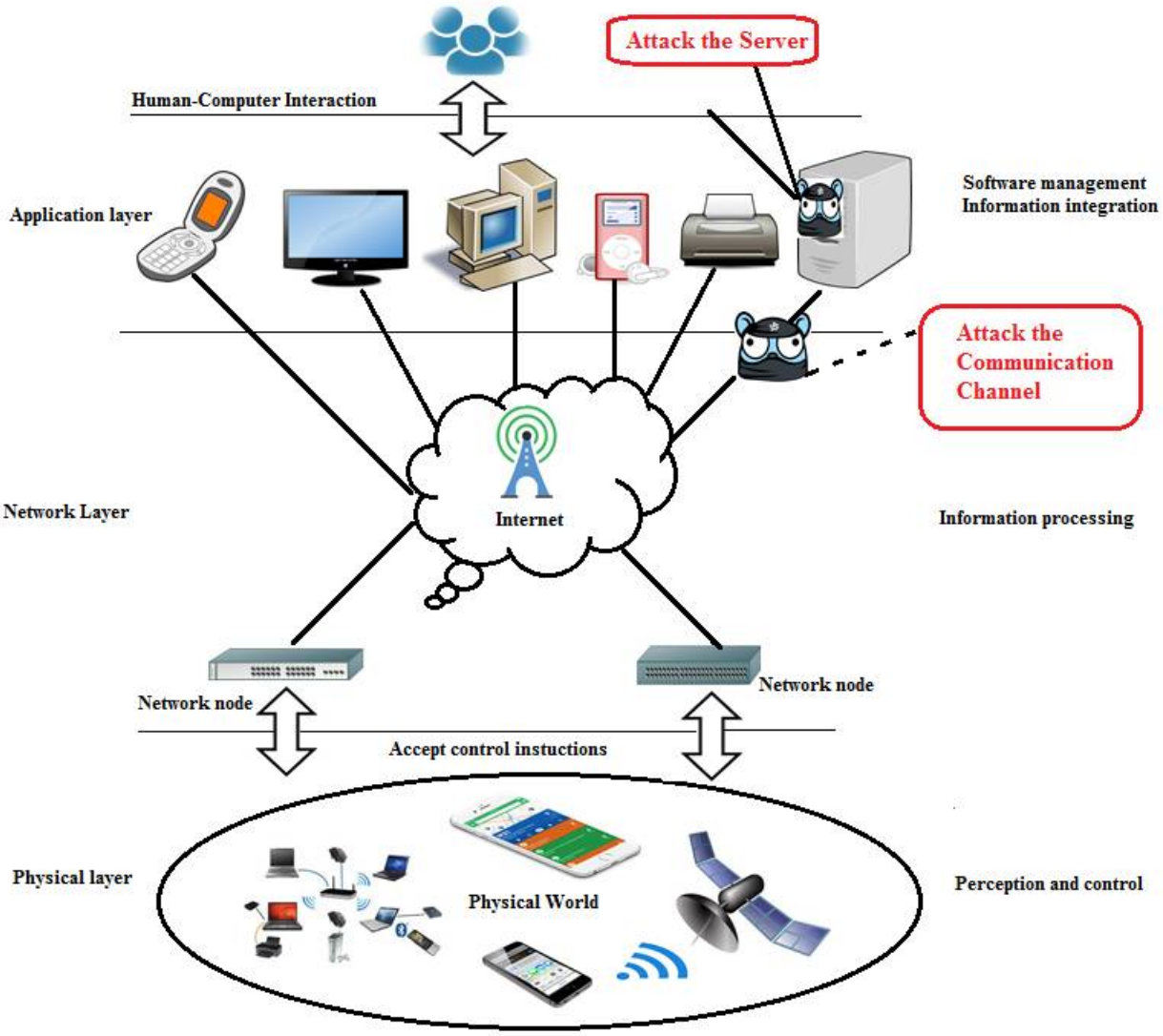

Fig.2 : DoS jamming attack

B. TYPES OF JAMMERS [2, 18, 19] –

The word jammer can be alluded as a tool or a configuration whose aptness can be abused by a rival to accomplish the duty of damaging the wireless network. Jammers are the gadgets which transmits the same frequency as that of wireless network in order to create inference [6]. They may target at physical layer transmission, MAC layer access, network layer and transport layer interaction or their combination.

There are a wide range of attack techniques that a jammer can use with a specific end goal to distort wireless communication. In the perspective of a few classification standards, current jamming attacks can be partitioned into various classes. Here, we embrace the general classification theory, i.e. a jammer can either be rudimentary or savvy upon its jamming models in time, frequency, protocol and other domains.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 3, March 2018

1) *Jamming attack in Time Domain* - With respect to time domain there are four categories of jammers according to different jamming theories i.e. constant jammer, deceptive jammer, random jammer and reactive jammer. Their typical features are described below-

- *Constant Jammer*- The constant jammer persistently transmits radio signals that are absolutely arbitrary. They don't follow any basic MAC protocol and are simply arbitrary bits.
- *Deceptive Jammer*- Rather than conveying arbitrary bits, the deceptive jammer continually infuses regular packets into the channels without any pause between ensuing packet transmission. Therefore, an authorized communication will be misled into accepting there is an authorized packet and will be deceived to stay in receive state.
- *Random Jammer*- Instead of persistently conveying a radio signal, a random jammer fluctuate between sleeping and jamming. In particular, after jamming for t_j units of time, it turns off its radio and enters sleepy zone. It will continue jamming after sleeping for t_s time. T_j and T_s can be either irregular or fixed values.
- *Reactive Jammer*- These are the most vitality effective jammers. They wait for any sort of transmission in wireless network and at whatever point a transmission happens, they begin discharging their own radio frequencies and attempt to create impedance in the network.

Note that constant jammer, deceptive jammer and random jammer can be dealt with active jammer since they effectively produce wireless signals. Conversely, the reactive jammer initiates the jamming attacks when channel is busy/occupied.
The different kinds of jammers are surveyed based on their advantages and disadvantages in the table beneath-

Table 2: Types of Jammers

Jammers		Advantages	Disadvantages
Proactive	Reactive jammer	• Disrupts packet of any size • Difficult detection	• Difficult to design • Energy inefficient • Works on single channel
	Deceptive jammer	• Difficult to detect • Continuously emit jamming signal • Hide jammer's identity	• Energy inefficient
	Constant jammer	• Continuously emit RF signal • Easy to implement	• Easily detected • Energy inefficient • Works on single channel
Random jammer		• Saves energy	• Less effective than other proactive jammers • Incapable of jamming during sleep mode
Function specific jammers		• Less energy consumption • Implemented for multiple channels • Better throughput	• Application specific • Complex programming is required

2) *Jamming Attack in Frequency Domain* - In the viewpoint of frequency domain, jamming attacks can be launched at one or multiple channels which are described below-

- *Spot Jammer* - It coordinates all its transmitting power on a solitary frequency that the target uses with same regulation and enough energy to abrogate the native signal.
- *Follow-on-Jammer* - It hops over every accessible channel frequently (thousand times each second) and jams each channel for a brief timeframe.
- *Channel hopping Jammer* - It can proactively hops among distinctive channels or jams numerous channels at the same time.
- *Pulsed noise Jammer* - It can converse channels and jam on diverse number of channels at various timeframes.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 3, March 2018

- *Barrage Jammer* - It endeavors to expand the commotion level across part or whole working frequencies (channels). As per execution technique, barrage jammer can be additionally separated into a few sub-classes.

3) *Jamming Attack in Protocol Domain* - From the point of view of network protocol, other than transmission at physical layer, jamming attack can focus at the MAC and network layer protocol. For instance, there exist an extensive number of attack techniques target at generally embraced 802.11 MAC protocol. In addition, for network layer packet trade, there are various jamming attacks.
Physical layer Jammer - These jamming attacks focus at signal transmission at physical layer. The previously mentioned attacks in time or frequency domain can be credited to this category from the point of view of protocol layer.
MAC Layer Jammer - Discrete wireless network acquire various MAC protocols. Each MAC protocol controls the entrance of some specific wireless medium and faces its own security dangers.

A couple of typical MAC Layer jammers incorporate –
DIFS Waiting Jammer - Jammer associated with this class hold up until the point when they sense channel idle for a DCF Inter Frame Space (DIFC) time interim. After this period, the saboteur jams the channel. This defiles the communication that takes place after the DIFS idle time. The jammer will degenerate either the DATA packet or RTS packet if the RTS/CTS exchange is utilized.
RTS/CTS Jammer - The malignant node detects the channel and wait for Short Inter Frame Space (SIFS) time interim and sends a short jamming pulse which will bring about tainting the CTS packet. This methodology may bring about zero throughput, since no information will be effectively transmitted.
Wireless Ad-hoc Jammer - These jammer endeavour to keep the WLAN from working in ad-hoc manner.
Implicit Jammer - Implicit jamming attacks are those that in expansion to impairing the usefulness of expected target, cause DOS state at different nodes of the system excessively. This attack misuse the rate adaptation algorithm utilized in wireless network where AP takes into account the frail node by diminishing its rate. Because of this procedure, the AP invest more energy conveying with the frail node than different nodes. Consequently, at the point when the implicit attacker jams a node which is conveying with access points, the rate adjustment impact will expand the AP's emphasis on the jammed/stuck node while making different customers endure.
Selfish Jammer - A selfish jammer seeks to possess all or some portion of accessible radio assets, denying other nodes from retrieving to those and fundamentally lowering the execution of multi hop wireless network.
Channel Selection Jammer -A jammer attempt to forestall other nodes from choosing some specific wireless channel through ceaseless transmission on this channel.
Network Layer Jammer – At the network layer, which is responsible for routing packet among multi hop wireless network nodes numerous jamming attack can be commence towards the routing exchange, neighbour disclosure, channel task and so on. For instance, a jammer can degenerate the routing advertisement packet in wireless medium to wreck the route setup process.

A couple of typical network layer jammer incorporate-
Routing Information Jammer - These jammers can occur in any wireless network that necessities to exchange the routing data among the wireless nodes. A jammer can emphasize on harming the routing data or simply hampering their transmission. This will make it difficult for every node to have a consolidate view on the topology of entire system.
IP Related Jammer - These jammers focus at the address statistics of the wireless nodes and harm the network through IP related assaults for example, IP spoofing, IP infusing and so forth.
Flow Jammer - Flow Jamming attacks include various jammers all through the network which jam the packet to lessen traffic flow. These attacks are propelled by utilizing data from network layer. This sort of jamming attack is useful for the asset compelled aggressor. In the event that there is incorporated control, at that point the base energy to jam a packet is enumerated and jammer demonstrate appropriately. In a non-centralized jammer model, every jammer shares data with neighbour jammer to augment productivity.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 3, March 2018

Transport and Application layer Jammer - The advances of Transport or Application layer protocols can likewise be deployed to launch different jamming attacks. For exemplar, a jammer can degenerate the acknowledgment (ACK) message in wireless medium to harm the initiation or winding up process of Transmission Control Protocol (TCP) session to extremely corrupt the throughput of an end-to-end flow. As a matter of fact, a jammer can harm the system execution without disregarding protocols. For instance, Jellyfish attack is a protocol agreeable attack which points at muddling the performance of transport layer by dropping zero or small fractions of packets. Any attack on physical, link or network or transport layer impacts antagonistically on application layer which is the final layer of communication protocol stack.

A couple of typical transport layer jammer incorporate-
ACK Corruption Jammer - Utilizing a similar approach (as in CTS Corruption jammer), the foe detects the medium for DATA packet. After detecting a DATA packet, it pauses for a SIFS time interim toward the completion of transmission and at that point jams the channel. This will bring about the corruption in MAC layer acknowledgement. The acknowledgement is not gotten by sender and there will be few retransmissions, until the point that sender surrenders furthermore, drops the packet from its MAC layer queue. It is facile to see that this technique may bring about zero throughput.
DATA Corruption Jammer - Almost identical to the past jamming approaches the jammer waits for the CTS packet and afterward checks down a period equivalent to DIFS before jamming the DATA packet.
Jellyfish Jammer - The Jellyfish Jammer can execute the attack by deliberately reversing/reordering the packet it acquire and onwards. TCP has a susceptibility to out of order packet; out of order packet elicit retransmissions and debase network throughput. Dropping a small amount of packets moreover corrupts throughput, like a sinkhole attack. Furthermore, if the nasty node arbitrary delays packets, throughput will be influenced because it makes the TCP clock be invalid, bringing about network congestion.

A couple of typical application layer jammer incorporate-
Sybil Jammer - A jammer executing the Sybil attack will make a substantial number of pseudonymous characters so it can procure a disproportionate vast impact on the network. In other words, the mapping of characters to substances is numerous to one. This will make the trust or reputation system of the management entity fail.
Primary User Emulation Jammer - In cognitive radio network, a primary emulation jammer may alter its air interface with the end goal that it emulates the primary user's signal qualities causing other optional users to dishonestly establish that the frequency is in being used by primary client, thus clear the frequency. This is conceivable since in an unfriendly domain, recognizing the primary user from other can turn out to be a great degree troublesome. The masquerade may execute the attack greedily, so he can utilize the range or maliciously, so the other genuine client will have their communication disturbed, bringing about a refusal of administration attack.
Note that a jammer can start cross layer attacks through consolidating the attack models specified previously. A couple of normal cross layer jammers incorporate –
Selective Jammer - A selective jammer target particular packets of "high" significance. For instance, jamming of TCP ACK's can seriously corrupt the throughput of a TCP association done to clog control component of TCP protocol. It can likewise jam those essential packets in the MAC or network protocol.
Control Channel Jammer - Control channel jammers work is multi-channel network by focusing on the control channel, or on the other hand the channel used to organize arrange action. An arbitrary jammer that aims the control channel could root a serious debasement of system execution, while a consistent jammer focusing on control channel may refuse entrance network utterly. These attacks are normally proficient by bargaining a node in the network. Besides, future control channel areas can be acquired from the bargained nodes.
Lion Jammer - The Lion attack is particular to the cognitive radio network. The attack happens at the physical/link layer while focusing on the transport layer. Basically, the jammer utilizes an essential user emulation attack keeping in mind the end goal to distort the TCP connection. The aggressor can be an outcast or a part of network. The attack influences the TCP by constraining frequency handoffs in clearing the channel because of the observation the essential user is available. At the point when handoff happens, the TCP doesn't know about the switchover. TCP will keep making legitimate connections also, sending packets while not accepting any ACK. Assuming no ACK is returned,

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 3, March 2018

TCP thinks about fragment as lost due to clog. As an outcome, TCP retransmits the fragment while diminishing the blockage window. This results in delays what's more, packet misfortune, lessen throughput.
Figure 3 demonstrates the above mentioned jamming attacks [2]. Moreover, the blend of different jamming models in time, frequency and protocol layer domains makes it illogical to cover all the conceivable jamming attacks models that might exist. Along these lines, we just rundown a couple of common attacks ideal model here-

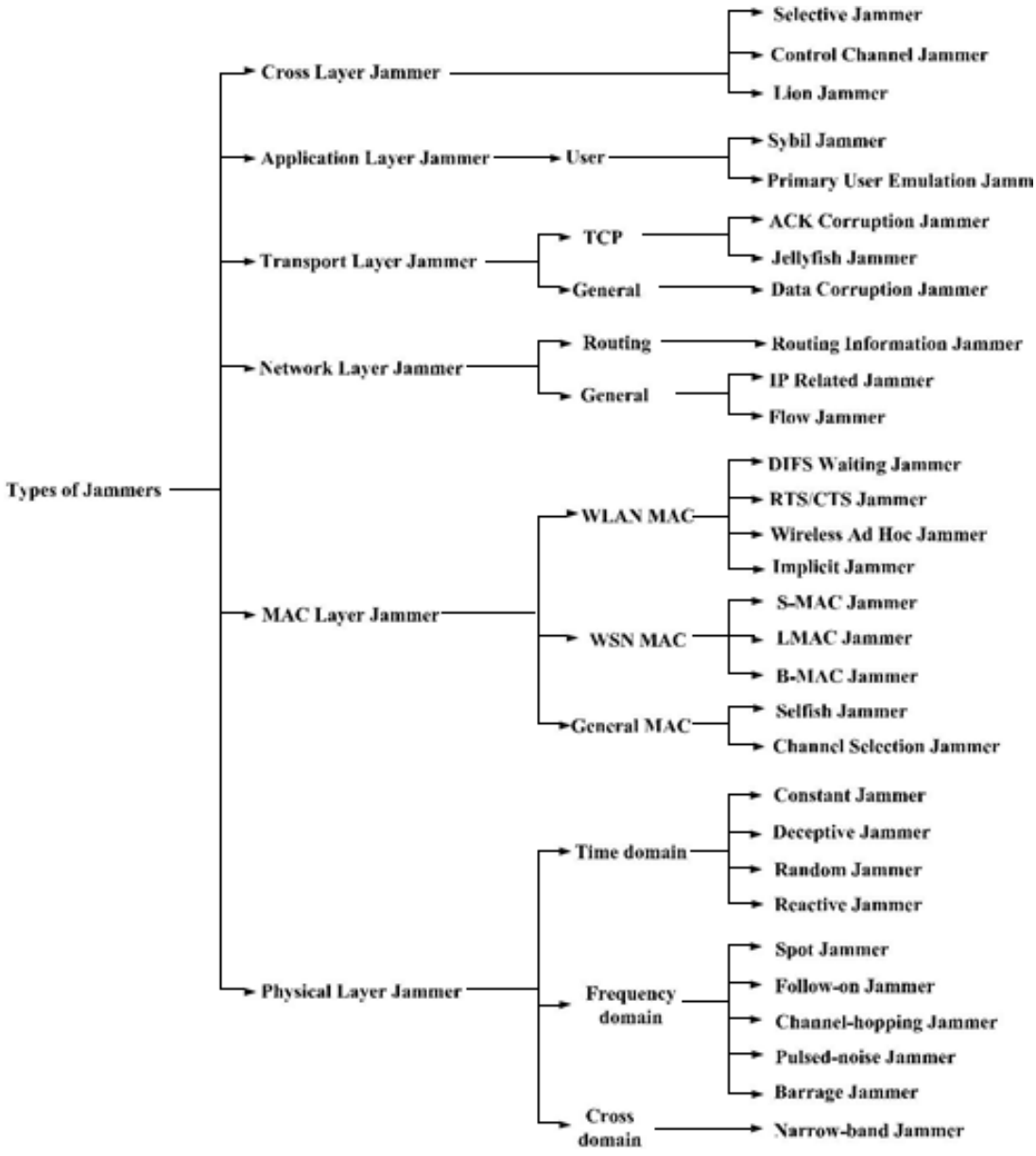

Fig.3: Jamming attacks

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 3, March 2018

IV. COUNTERMEASURES AGAINST JAMMING

Here we introduce a comprehensive audit of different countermeasures that have been proposed in order to overcome jamming attacks[6, 19]. These jamming countermeasures can be outlined as follows in table 3.

- *Appropriate power transmission* - The assailant's proficiency to find an objective is diminished when high power for transmission is utilized. The effectiveness of the jamming signal ought to be higher than that of the native signal so that the jammer can overwhelm the native signal. In the event that the transmitted power is high at that point there will be an accordingly more prominent confrontation towards jamming. Sensor nodes display in WSN have the capacity to modify the transmitter's yield power.
- *Frequency hopping spread spectrum* - In FHSS, radio signals of bearer are frequently exchanged between various frequency channels. Both the transmitter and the beneficiary utilize a pseudorandom arrangement of bearer frequencies to accomplish fast exchanging. The transmitter and also the beneficiary deeds at a mutual algorithm. Focal points of FHSS are that the capture of radio signals from unapproved parties is diminished furthermore, this keeps the prevention of radio transmission. Signal to clamor proportion is enhanced viably. Proficient managing multipath impacts also happens. Coexistence of more than one WSN is conceivable in the single region. The significant disadvantage of FHSS is that it requires considerably more extensive bandwidth for the transmission of information. FHSS has a high jamming protection until the aggressor picks up the learning about pseudorandom attributes. In military utilizations of Spread range, cryptography is utilized to scramble channel arrangement and the secret key is partaken ahead of time by the sender as well as the beneficiary.
- *Direct sequence spread spectrum* - It is a method for spread spectrum regulation which makes a difference in lessening obstruction in the native signal. The information signal furthermore, Pseudo-commotion is accumulate to play out the transmission. The Pseudo-commotion is essentially an arbitrary grouping of 1 and -1 at a considerably more prominent frequency contrasted with unique signal. The yield signal got is like repetitive sound has a more extensive transfer speed signal which replaces the native signal. At the beneficiary end, the clamor is sifted through with a specific end goal to acquire back the native data by ascertaining the result of RF signal and the beforehand utilized modulated bearer. DSSS has all the points of interest introduce in FHSS.
  Furthermore, it is more secured than FSHH on the grounds that it is troublesome to reestablish the transmitted signal of DSSS. It winds up troublesome for the assailant to reestablish the DSSS signal. The DSSS signal is like repetitive sound, making it hard to discover the origin of transmission.
- *Hybrid FHSS/DSSS* - Hybrid FHSS/DSSS proposes a great answer for sticking as it gets the advantage of both FHSS/DSSS. Obstruction is abstained from utilizing recurrence bouncing framework though DSSS employments is more extensive data transmission to diminish obstruction which infers that protection from sticking can be expanded surprisingly by utilizing both the approach together. Properties like Low likelihood of location and low likelihood of block attempt can likewise be accomplished by utilizing this strategy. High quality capture types of gear are required to capture the frequency changes. To recuperate the native signal both the Pseudo-clamor and the Frequency grouping are required. Hybrid FHSS/DSSS has the capacity to battle against the close far impact. In spite of the expansion in multifaceted nature of attune, hybrid techniques are facile but difficult to execute since littler PN codes and lesser number of trusting frequencies can be utilized.
- *Directional transmission* - Presently days, Omni-directional transmission antennas are utilized as a part of the sensor nodes. These antennas are equipped for transmitting and getting waves from each conceivable course at a similar purpose of time which prompts security issues and diminishes the unwavering quality of these antennas while on other hand, the directional antennas transmits and gets in just a particular direction. Henceforth they have more noteworthy resilience to jamming. With the utilization of directional antennas, numerous assaults for example, eavesdropping, jamming and recognizable proof of messages can be evaded. Directional antennas can upgrade the execution of the transmitter and can make the network more impervious to obstruction. Directional transmission has a few issues related with it. It requires a legitimate MAC protocol and directing in various ways turns into a troublesome undertaking. Directional antennas are additionally ordered into two sorts of antennas: Beam forming antennas and Sectored antennas. In sectored antennas, vast

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 3, March 2018

number of stable antennas, looking towards different directions that have the ability of working autonomously are available. In Beam forming, every one of the antennas work at the same time so as to transmit and get waves in different directions.

- *Polarization of antenna* - The polarization of antenna can be characterized as the emplacement of antenna and the transmitted vitality created by them. Polarization is reliant on the structure and the emplacement of antenna. To relay with the diverse antennas, it is obligatory to have same polarization between them. For instance, if an antenna is having a vertical polarization, it won't have the capacity to impart with antenna having right round polarization. An observable pathway ought to be kept up to set up a communication and this property can help nodes in jamming condition, if a node recognizes any obstruction in nature, it can change its polarization and spare the system from jamming. The greatest challenge in this strategy is that each node in the system must illuminate alternate nodes about the changing polarization before any real change in its polarization with the goal that the communication won't be intruded. To defeat this issue, nodes ought to be customized ahead of time to manage this issue.

Table 3: Countermeasures against Jamming attack

COUNTERMEASURES	SALIENT FEATURES
FREQUENCY HOPPING SPREAD SPECTRUM	• Uses speed spectrum method for transmitting signals • Advantageous for WSN • Jamming can be controlled • Provides a better SNR ratio
DIRECT SEQUENCE SPREAD SPECTRUM	• Data is multiplies with pseudo- random digital signal which is a sequence of 1 and -1 • Replaces original signal with wide bandwidth signal • Difficult for attacker to obtain original signal • Difficult to find the transmitting source
HYBRID FHSS/DSSS	• Helps to solve near-far problems • High resistance to jamming • Shares the features of both FHSS/DSSS • Low probability of detection and low probability of interception
ULTRA WIDE BAND TECHNOLOGY	• Hard to intercept • Longer battery lifetime • Difficult to join • Solves multipath effect problem • Wide frequency band for transmission
POLARIZATION OF ANTENNA	• Dependent on structure of antenna • Effective solution for jamming environment • Polarization reduces interference among nodes • Nodes with similar polarization can communicate
DIRECTIONAL TRANSMISSION	• Reliable and secured • Transmits signals in a specific direction • Defensive mechanism against jamming attacks • Categorized into beam forming antennas and sectored antennas

- *Ultra wide band technology* - Ultra wide band is an innovation utilized for transmitting information by spreading the radio vitality in a huge frequency band utilizing a low control spectral density which helps in restricting the impedance from the conventional radio sources, a high throughput can be achieved from the high transfer speed utilized as a part of UWB. This attune innovation transmits shorter pulses over a frequency band of wide range. In this, the sensor systems are sent in savvy way and devours low power. This innovation makes the coral of signal extremely troublesome and furthermore makes it impervious to multipath impacts. UWB additionally proposes long battery lifetime for the nodes and proper confinement. It is likewise an open research issue and still being worked on.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 3, March 2018

V. CONCLUSION

A Mobile Ad hoc Network (MANET) is a gathering of mobile hosts that relies upon wireless network interfaces having like open network boundary, dynamic topology and wireless communication. Hence security becomes profoundly susceptible. Jamming attacks are a subset of denial of service (DoS) attacks in which noxious nodes obstruct authorized communication by causing deliberate impedance in network. In this extensive study on jamming and anti-jamming techniques in wireless networks, we have contributed by classifying and condensing various methodologies and discussing open research issues in the field. Different jammers attack wireless networks in distinct ways so that their attack impacts are significantly different. The target of this survey is to provide the readers with basic understanding and quick reference to various sorts of jammers and its countermeasures based on their application, if used.

REFERENCES

1. Tada, N., Patalia, T., and Rupani, P., "A New Approach to Mitigate Jamming Attack in Wireless Adhoc Network Using ARC Technique", Springer International Conference on Future Internet Technologies and Trends, pp.192-204, 2018.
2. Wei, X., Wang, Q., Wang, T., and Fan, J., "Jammer Localization in Multi-Hop Wireless Network: A Comprehensive Survey", IEEE Communications Surveys & Tutorials, Vol. 19, Issue No. 2, pp.765-799, 2017.
3. Bhojani, R., and Joshi, R., "An Integrated Approach for Jammer Detection using Software Defined Radio", Science Direct International Conference on Communication, Computing and Virtualization, Vol. 79, pp.809-816, 2016.
4. Rahman, F.H.M.A.R and Au,T.W., "Impact of IPsec on MANET", IEEE International Symposium on Computer, Consumer and Control, pp. 408-411, 2016.
5. Dong, Y. and Zhou, P., "Jamming Attacks against Control Systems: A Survey", Springer International Conference on Life System Modeling and Simulation, pp.566-574, 2017.
6. Jaitly, S., Malhotra, H., and Bhushan, B., "Security Vulnerabilities and Countermeasures against Jamming Attacks in Wireless Sensor Networks: A Survey" IEEE International Conference on Computer, Communications and Electronics (Comptelix), pp. 559-564, 2017.
7. Yuan, L., Wang, K., Miyazaki, T., Guo, S., and Wu, M., " Optimal Transmission Strategy for Sensors to Defend against Eavesdropping and Jamming Attacks", IEEE International Conference on Communications, 2017.
8. Kikuchi, K., Cetinkaya, A., Hayakawa, T., and Ishii, H., "Stochastic Communication Protocols for Multi-Agent Consensus Under Jamming Attacks", IEEE 56th Annual Conference on Decision and Control (CDC), pp. 1657-1662, 2017.
9. Das, R., Bal, S., Das, S., Sarkar, M.K., Majumder, D., Chakraborty,A., and Majumder, K., "PERFORMANCE ANALYSIS OF VARIOUS ATTACKS UNDER AODV IN WSN & MANET USING OPNET 14.5", IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference, 2016.
10. Aldarraji, A., Hong, L., and Shetty, S., "Polarized Beamforming for Enhanced Countermeasure of Wireless Jamming attacks ", IEEE 35th Performance Computing and Communications Conference, 2016.
11. Sharma, H., Quyoom, A., Ali R., and Gouttam, D.N., "A Novel Mechanism of Detection of Denial of Service Attack (DoS) in VANET using Malicious and Irrelevant Packet Detection Algorithm (MIPDA)", IEEE International Conference on Computing, Communication and Automation , pp.414-419, 2015.
12. Sharma, P., and Suryawanshi, A., "Enhanced Security Scheme against Jamming attack in Mobile Ad hoc Network", IEEE International Conference on Advances in Engineering & Technology Research, 2014.
13. Hamie, A., "POWJAM: A Power Reaction System against Jamming Attacks in Wireless Ad Hoc Network", IEEE 9th Annual Conference on Wireless On-Demand Network Systems and Services, pp.9-15, 2012.
14. Beg, S., Ahsan, F., and Mohsin, S., "Engaging the Jammer on the Jammed Channel in MANET", IEEE 6th International Conference on Emerging Technologies, pp.410-413, 2010.
15. Othman, J.B., and Hamieh, A., "Defending Method Against Jamming Attack in Wireless Ad Hoc Networks", IEEE 34th Conference on Local Computer Networks, pp- 758-762, 2009.
16. Liu, Z., Liu, H., Xu, W., and Chen, Y., "Exploiting Jamming-Caused Neighbor Changes for Jammer Localization", IEEE Transactions on Parallel and Distributed Systems, Vol. 23, Issue No. 3, pp.547-555, 2011.
17. Chaturvedi, P., and Gupta, K., "Detection and Prevention of various types of Jamming Attacks in Wireless Networks", IRACST International Journal of Computer Networks and Wireless Communications, Vol. 3, Issue No. 2, pp.75-79, 2013.
18. LATHA.S, P., and SABITHA, R., "A Survey of Channel Allocation and Attacks in Multichannel Multi radio Wireless Networks", IEEE Second International Conference on Science Technology Engineering and Management, pp.172-176, 2016.
19. Kanika, G., Alvin, L., and Qing, Y., "Jamming and Anti-jamming Techniques in Wireless Networks: A Survey", International Journal of Ad Hoc and Ubiquitous Computing, Vol. x, Issue No. x, xxxx, pp.1-16, 2014.