A Taxonomic Survey of Heterogeneous Jamming Attacks and Their Countermeasures in Wireless Ad-hoc Networks

AJAY SONKESRIYA

Lecturer

Electronics And Communication Engineering

Kalaniketan polytechnic College Jabalpur MP

Abstract: The term "mobile ad hoc network" (MANET) refers to a collection of heterogeneous mobile nodes that are dynamically structured, self-configured, and require no infrastructure. Mobile nodes are extremely vulnerable because to the open nature of wireless networks. Jamming attacks are one of the most serious security threats in MANET. Jamming is a form of Denial of Service (DoS) attack in which an advisory sends radio signals between mobile nodes with the purpose of disrupting message communication. Various jamming techniques and types of jammers have been examined in this study. This assessment summarises the important research in the subject of anti-jamming countermeasures, as well as their benefits and drawbacks. This poll also suggests a number of research topics for improving jamming assault.

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

I. INTRODUCTION

Wireless networks [13, 15] are becoming increasingly popular for quick feasible transmission, and they can be based on a variety of technologies, including wifi networks, GSM networks, Bluetooth, LTE, and so on. Wireless Ad hoc network is a type of wireless network that is decentralised and does not rely on a pre-existing skeleton. It is a network constructed from a group of adaptable nodes that may efficiently self-compose with arbitrary and changing topology. Ad-hoc networks are steadily progressing towards diverse attacks and achieving global figuring. The typical characteristic of wireless medium is to share and converge with ware essence of wireless advances and an inexorably complex client-base, allowing wifi network to be watched and relayed on with ease. Nodes act as both a transmitter and a switch in this scenario. Every portable node bargains with each other directly, while nodes that aren't directly connected to wifi communicate by sending traffic through relay nodes. Ad hoc networks, on the other hand, are resilient, low-cost, and robust, making them ideal for military exercises, crisis operations, disaster recovery, large-scale community networks, and small networks [1, 4]. As soon as the network became popular, the security of viable communication became a research topic. The mobile adhoc network (MANET) is a self-governing, lively, and multi-hop network in and of itself. It does not require a solid base and may be set up on the fly.

Because of its dynamic and multi-hop nature, MANET becomes more vulnerable to many sorts of assaults, such as DDOS, Black hole, Wormhole Replay, Flooding [12], Jamming [1, 9], and so on, which counteract the harmful impact of high-level security. As a result, security is getting increasingly difficult. Any hostile client can simply detect communication between two devices and send a fake message to disrupt or jam normal communication.

Jamming attacks occur when radio signals are continuously sent, obstructing authorised communication between the sender and the recipient. Figure 1 shows how a jammer can identify communication set up on a wireless channel.

It starts sending radio signals that infuse dummy packets, which the recipient receives instead of the original packet sent by the transmitter. The attacker concentrates on high-value packets.
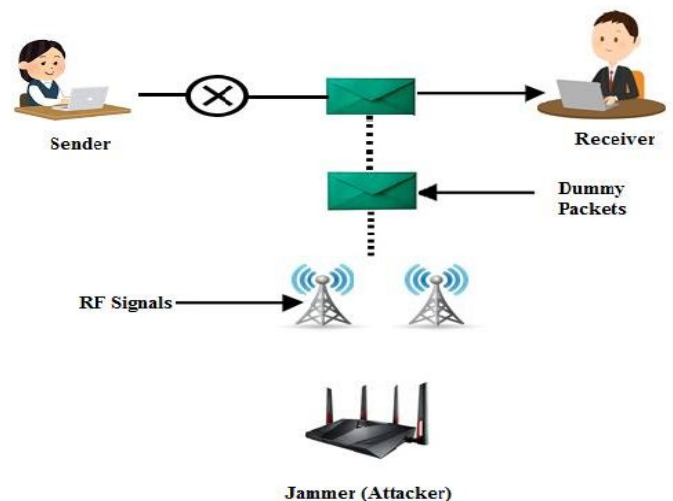

Fig.1:Pictorialview ofjammingattack

II. RELATEDWORK

Yanbo Dong et.al. [5] - Here, authors surveyed about control system regarding jamming attack with respect to threeaspects i.e. attack, defence and arms race between them. They also reviewed various prevailing methods to deal withsecurity issues by introducing gaming theory. They concluded that attacker's desire the jamming attack to be systematichaving

restraint energy and halted from being perceived by IDS. But defender's motive was achieving higher perceiveaccuracy by improving IDS to lessen the jamming attack's risk. In their future work, they suggested to merge gametheoryandmachinelearningalgorithmtoovercomesecurityr isk.

SunakshiJaitly et.al. [6] - In this paper, author surveyed about various security vulnerabilities and countermeasuresagainst jamming attacks inwireless sensor network.They also provided extensive details about jamming techniquesand different categories of attacker like proactive, reactive and functional specific jammer technologies with their prosand cons. They also discussed several limitations and challenges of wireless sensor network. Various countermeasuresagainst jamming were also explained like using spread spectrum technologies, polarization of antennaand advantagesofusingdirectionalantenna.They alsoconcludedthatanewdefencemechanismwasdevelopedforthe mostsophisticatedattacks, ifthesetechnologies wereusedappropriately.

Li Yuan et.al. [7] - In this paper, authors introduced a strategy to maximize the secure transmission rate againsteavesdropping and jamming attacks. They modelled the power allocation problem as a stackelberg game where sensorwas leader and jammer was follower. They also proposed stochastic algorithm with feedback (SAF) for an optimalvalue 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 toRPA,PAWSJandPAMsincetheyhavenofeedback.

Kaito Kikuchi et.al. [8] - In this paper, authors developed a new consensus framework to deal with attacks wherejamming is turned on or off very frequently. In the proposed approach, multi- agents attempt to communicate withneighbourat randomtime instantsthatare unknownbyattacker.Theytooktwodifferentstrategiesofthe attackeri.e.adeterministic attack strategy and a more malicious communication aware strategy. Authors concluded that stochasticcommunication protocol achieved consensus in finite time in both strategies but communication aware strategy wassmarteras itallowsthe attackerto preserve the energy tobe used later.Inthe future work,they suggested toincorporate probabilistic analysis of the consensus time as well as the analysis of communication aware strategy in thesituationwheretheagentsarenotreallysynchronizedandtheyen deavourcommunicationatvarious circumstances.

Rupayan Das et.al. [9] - Here, the authors introduced an algorithm for comparing the effects of different network andphysical 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 likesimulation area of 200m*100m, simulation time of 30 min and simulation speed of 256 bits/sec.Authors have takenfollowing matrices i.e. throughput, load, delay and packet dropped for the analysis of different attacks. Simulationresults shown that black hole attack experienced maximum delay since it has higher number of packet dropped ascompared to other attacks while load was dependably lower in intruder free network and higher in intruder affectednetwork and at last throughput for all network under any attack was always lesser as compared to network withoutattack.

Ali Aldarraji et.al. [10] - Here, authors proposed an enhanced countermeasure technique for jamming attacks byutilizingpolarizedbeamformingwithaplanararray.The proposedtechnique wasdesignedusingtheLinearlyConstrained Minimum Variance (LCMV) criterion. For performance evaluation, signal to interference ratio was set tobe-20dB and evaluated interms of BitErrorRatio (BER) to assess its information integrity and anti-jammingcharacteristics throughout various antenna array sizes. Authors integrated both polarization and space information tosuppressundesiredinterference.Aftertheresults,authorsconclu dedthatproposedbeamformerfundamentallyenhances the data framework execution when the jammer and desired signal are located intently in space domain. Also,thebiggerthearrayestimate, thelessdatamistakeoccurred.

Harish Sharma et.al. [11] - In this paper, authors introduced a model for the detection of Denial of Service (DoS) inVANET with the use of Malicious and Irrelevant packet Detection Algorithm (MIPDA). Here, they also discussedvarious aspects of attacks in VANET. The proposed algorithm was based on continual position changing requirementsof vehicle and attached with each and every RSU. They took frequency (f) and velocity (v) as parameters to analysemalicious and irrelevant packets. After the result, authors concluded that proposed algorithm ensures about generationof malicious and irrelevant packets, enhanced the security in VANET, avoid delay with correct packet generation aswell as to analyse the strength of packet generation. In their future work, they recommend to use same approach fordetectionofmultiplemalicious,invalidandirrelevantrequestse ntandreceivedfrommultiplevehicles atatime.

Priyanka Sharma et.al. [12] - In this paper, authors proposed an enhanced security scheme in mobile ad hoc network tomitigate and block the effect of jamming attack. They proposed an algorithm for jamming control using AOMDV withprevention mechanism in which the PDR value of each node was calculated. They used NS-2 simulator and forsimulationvarious parameters were used i.e. simulation area of 800m*600m, numberof nodes 50, simulationtime of50 sec and AOMDV routing protocol. Simulation result shown that

routing overhead minimizes while PDR was about95% in presence of jamming attack. They also concluded that proposed approachprovides zero infected data deliveryin network and proper bandwidth hence performance was enhanced in presence of attacker. In their future work, theysuggestedtousesomeotherroutingprotocol.

Ali Hamie et.al. [13] - Here, authors proposed a mechanism POWJAM- A power reaction against jamming attack toeliminate the jamming attack in wireless ad hoc network. They used POWJAM which was based on sending routinginformation, received routing information and data transmission power calculation. For simulation authors took NS-2simulator. Simulation parameters used by them were traffic model CBR, routing protocol DSDV and packet size of1024 bytes.They tookthroughput and packet delivery ratio as simulationscenarios having varying numberof nodesand varying number of connections. After the results, authors concluded that PDR and throughput in POWJAN underjamming was less than network without jamming having varying numberof nodes while PDR and throughput innormal networkincrease rapidly thanina networkusesPOWJAMunderjammingwithincrease innumberofconnections.Intheirfuturework,theysuggestedtoimplementPOWJAM inrealenvironment.

SairaBeget.al.[14]-
Inthispaper,authorsproposedanideatoengageajammeronthejammedchannelinMANET.Inthe proposed technique, the nodes flee away to avoidjamming, but resume onnewerchannel by alternativelyvisiting and sending legal packets on network in a coordinated manner. For performance evaluation, authors have takenOPNETsimulatorwith10wirelessstationshavingsingletransceiveronly,trafficloadof10packets/secandjammed time of 10-40 sec. After the simulation, authors derived that more than 95% of communication was resumed by thisscheme and nearly 85% of overall communication was successful during jam period depending upon traffic load andnumberofnodes.

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 replicatingpacket 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. Afterthe result, authors derived that throughput starts degrading under jamming attacks while packet delivery ratio remainshigher, thus proposed approach maintain very high probability to cope with jamming attack.In their future work, theysuggestedtofindaneffectivedetectionmechanismtodetectthe presenceofjammingattacks. InthisbroadstudyofjammerdetectionmethodsasshowninTable1, onlyonematricesfordetectionofjammerhasnotbeensufficient,so morethantwodifferentparameterswereusedinallthemethods.

Table1: ComparisonofJammingDetectionmethods

	MethodUsed	Technique	Complexity
[7]	ensor'sprofitU_m(P,J)andJammer'sprofitJ_m(P,J)	SAF	High
[10]	Polarizedbeamformingwith planararrayusingLCMV	BER	High
[11]	Overhead,Correctpacket generation	MIPDA	Moderate
[12]	Routingoverhead,PDR	Scheme using AOMDVroutingprotocol	Moderate
[13]	Throughput,PDR	POWJAM	Moderate
[15]	Throughput,PDR	Replicatingpacketredundancy	High

III. JAMMINGATTACK

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].

Practicallyspeaking,Jammingattacksareexecutedbytransmitting meddling RF signals on wireless channel without following an appropriate Media Access Control (MAC) and thusempowering the jammer to obstruct the data transmission over the network and possibly impacts the achievement oftacticaloperation.

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 iswithinthejammer'srange. These attacks are illustrated in figure2.

This attack is simple and effective. It just needs to get the communication band of present network through observinglatently and after that attack can be quickly propelled. These attacks can attack the server to debilitate the restrictedassets of CPU and memory of control system straight forwardly, it can likewise attack the communication channelspecificallytocausejamming.

A.   TYPES OFJAMMING[1,15, 16]–

- *PHYSICAL JAMMING*-Physical jamming over wireless network is facile however it originate different typesof DOS attack, which chiefly jam the channel or network by persistently sending jamming signals or radiofrequency signals or by forwarding irregular packets. It retainentire control over the wireless medium. Thisformulate squander of time as each node go into holding up stage and need to hold up till the time jammerdeactivateitselfandchannelturninactivetoimparts.

- *VIRTUALJAMMING*-TheutilizationofVirtualsensing detectingsystemdoneatMAC(MediaAccessControl) 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; lesspowerutilization. In MAC layer, the impact of jamming start off by assaulting onRTS/CTS frames orDATA/ACK frames.
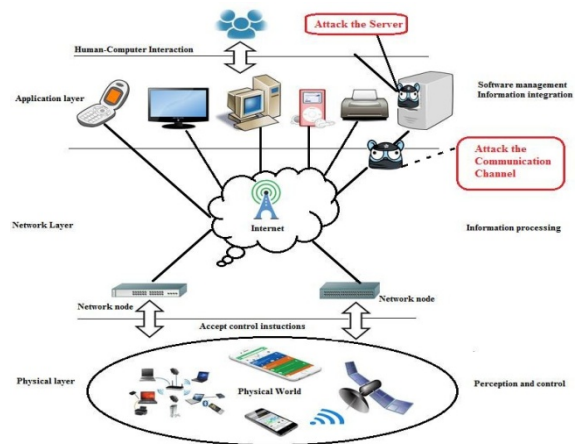

Fig.2:DoSjammingattack

B.   TYPES OFJAMMERS[2, 18, 19]–

Thewordjammercanbealludedasatooloraconfigurationwho seaptnesscanbeabusedbyarivaltoaccomplish the duty of damaging the wireless network. Jammers are the gadgets which transmits the same frequency asthat of wireless network in order to create inference [6]. They may target at physical layer transmission, MAC layeraccess,networklayerandtransportlayerinteractionortheircombination.

There are awide range of attack techniques that ajammercan use with aspecific end goal to distort wirelesscommunication. In the perspective of a few classification standards, current jamming attacks can be partitioned intovariousclasses. Here, we embrace the general classification theory, i.e. a jammer can either be rudimentary or savvyuponitsjammingmodelsintime, frequency,protocolandotherdomains.

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

- *Constant Jammer*- The constant jammer persistently transmits radio signals that are absolutely arbitrary. Theydon'tfollowanybasicMACprotocolandaresimplyarbitrarybits.

- *Deceptive Jammer*- Rather than conveying arbitrary bits, the deceptive jammer continually infuses regularpackets into the channels without any pause between ensuing packet transmission. Therefore, an authorizedcommunication will be misled into accepting there is an authorized packet and will be deceived to stay inreceivestate.

- *Random Jammer*- Insteadof persistently conveyingaradio signal,arandomjammerfluctuatebetweensleeping and

jamming. In particular, after jamming for t_j units of time, it turns off its radio and enters sleepyzone.It willcontinuejammingaftersleepingfor$t_s$time.$T_j$and$T_s$canbe eitherirregularorfixedvalues.

- *Reactive Jammer*- These are the most vitality effective jammers. They wait for any sort of transmission inwireless network and at whateverpoint a transmission happens, they begindischarging theirownradiofrequenciesandattempttocreateimpedancei nthenetwork.

Note thatconstantjammer,deceptivejammerandrandomjammer canbe dealtwithactivejammersincetheyeffectively produce wireless signals. Conversely, the reactive jammer initiates the jamming attacks when channel isbusy/occupied.

Thedifferentkinds ofjammersaresurveyed basedontheiradvantagesanddisadvantagesin thetablebeneath-

Table2:Types of Jammers

Jammers		Advantages	Disadvantages
Proactive	Reactivejammer	Disruptspacket ofanysize Difficultdetection	Difficulttodesign Energyinefficient Worksonsingle channel
	Deceptivejammer	Difficulttodetect Continuously emit jammingsignal Hidejammer'sidentity	Energyinefficient
	Constantjammer	ContinuouslyemitRF signal Easytoimplement	Easilydetected Energyinefficient Worksonsingle channel
Randomjammer		Savesenergy	Less effective than otherproactivejammers Incapableofjammingduringsleepmode
Functionspecificjammers		Lessenergyconsumption Implemented for multiplechannels Betterthroughput	Applicationspecific Complex programming isrequired

JammingAttackinFrequencyDomain-
Intheviewpointoffrequencydomain,jammingattackscanbelaunc hedatoneormultiplechannelswhicharedescribedbelow-

- *SpotJammer*- Itcoordinatesallitstransmittingpoweronasolitaryfrequenc ythatthetargetuseswithsameregulationandenoughenergyt oabrogatethenativesignal.
- *Follow*-*on-Jammer*- Ithopsovereveryaccessiblechannelfrequently(thousandti meseachsecond)andjamseachchannelforabrieftimeframe .
- *ChannelhoppingJammer*- Itcanproactivelyhopsamongdistinctivechannelsorjamsnu merouschannelsatthesametime.
- *Pulsed noiseJammer* - Itcanconversechannelsandjamondiversenumber ofchannelsatvarioustimeframes.

- *Barrage Jammer* - It endeavors to expand the commotion level across part or whole working frequencies(channels).Asperexecution technique,barragejammercanbeadditionallyseparatedintoaf ewsub-classes.

2) *Jamming Attack in Protocol Domain* - From the point of view of network protocol, other than transmission atphysical layer, jamming attack can focus at the MAC and network layer protocol. For instance, there exist anextensive number of attack techniques target at generally embraced 802.11 MAC protocol. In addition, fornetworklayerpackettrade,therearevariousjammingattack s.

Physical layer Jammer - These jamming attacks focus at signal transmission at physical layer. The previouslymentioned attacks in time or frequency domain can be credited to this category from the point of view ofprotocollayer.

MAC Layer Jammer - Discrete wireless network acquire various MAC protocols. Each MAC protocol controlstheentranceofsomespecificwirelessmediumandfac esitsownsecuritydangers.

AcoupleoftypicalMACLayerjammersincorporate–
DIFS Waiting Jammer - Jammer associated with this class hold up until the point when they sense channel idle for aDCF

InterFrame Space (DIFC) time interim.Afterthis period,the saboteurjams the channel.This defiles thecommunication that takes place after the DIFS idle time. The jammer will degenerate either the DATA packet or RTSpacketiftheRTS/CTSexchangeisutilized.

RTS/CTS Jammer - The malignant node detects the channel and wait for Short Inter Frame Space (SIFS) time interimand sends a short jamming pulse which will bring about tainting the CTS packet. This methodology may bring aboutzerothroughput,sincenoinformationwillbeeffectivelytrans mitted.

WirelessAd-hocJammer-Thesejammer endeavourtokeeptheWLAN fromworkingin ad-hocmanner.

Implicit Jammer - Implicit jamming attacks are those that in expansion to impairing the usefulness of expected target,causeDOSstateatdifferentnodesofthesystemexcessively. Thisattackmisusetherateadaptationalgorithmutilizedin wireless network where AP takes into account the frail node by diminishing its rate. Because of this procedure, theAP invest more energy conveying with the frail node than different nodes. Consequently, at the point when the implicitattacker jams a node which is conveying with access points, the rate adjustment impact will expand the AP's emphasisonthejammed/stucknodewhilemakingdifferentcustom ersendure.

Selfish Jammer - A selfish jammer seeks to possess all or some portion of accessible radio assets, denying other nodesfromretrievingtothoseandfundamentallyloweringtheexec utionofmultihopwirelessnetwork.

Channel Selection Jammer -A jammer attempt to forestall other nodes from choosing some specific wireless channelthroughceaselesstransmissiononthischannel.

Network Layer Jammer – At the network layer, which is responsible for routing packet among multi hop wirelessnetwork 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 towrecktheroutesetupprocess.

Acoupleoftypicalnetworklayerjammerincorporate-

Routing Information Jammer - These jammers can occur in any wireless network that necessities to exchange therouting data among the wireless nodes. A jammercanemphasize on harming the routing data or simply hamperingtheirtransmission.This will make it difficult forevery node to have aconsolidate view onthe topology of entiresystem.

IP Related Jammer - These jammers focus at the address statistics of the wireless nodes and harm the network throughIPrelatedassaultsforexample, IPspoofing, IPinfusingandsoforth.

Flow Jammer - Flow Jamming attacks include various jammers all through the network which jam the packet to lessentraffic flow. These attacks are propelled by utilizing data from network layer. This sort of jamming attack is useful forthe asset compelled aggressor. In the event that there is

incorporated control, at that point the base energy to jam apacket is enumerated and jammer demonstrate appropriately. In a non-centralized jammer model, every jammer sharesdatawithneighbourjammertoaugmentproductivity.

Transport and Application layer Jammer - The advances of Transport or Application layer protocols can likewise bedeployed 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 systemexecution without disregarding protocols. For instance, Jellyfish attack is a protocol agreeable attack which points atmuddling the performance of transportlayerby dropping zero orsmallfractions of packets.Any attack onphysical,linkornetworkortransportlayerimpactsantagonistica llyonapplicationlayerwhichisthefinallayerofcommunicationpro tocolstack.

Acoupleoftypicaltransportlayerjammer incorporate-

ACK Corruption Jammer - Utilizing a similar approach (as in CTS Corruption jammer), the foe detects the medium forDATA packet. After detecting a DATA packet, it pauses for a SIFS time interim toward the completion of transmissionandatthatpointjamsthe channel.Thiswillbringaboutthe corruptioninMAC layeracknowledgement.Theacknowledgement is not gotten by sender and there will be few retransmissions, until the point that sender surrendersfurthermore, drops the packet from its MAC layer queue. It is facile to see that this technique may bring about zerothroughput.

DATA Corruption Jammer - Almost identical to the past jamming approaches the jammer waits for the CTS packet andafterwardchecksdownaperiodequivalenttoDIFS beforejammingtheDATApacket.

Jellyfish Jammer - The JellyfishJammer canexecute the attack by deliberately reversing/reordering the packet itacquire and onwards. TCP has a susceptibility to out of order packet; out of order packet elicit retransmissions anddebase 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 clockbeinvalid, bringingaboutnetworkcongestion.

Acoupleoftypicalapplicationlayerjammer incorporate-

Sybil Jammer - A jammer executing the Sybil attack will make a substantial number of pseudonymous characters so itcan procure a disproportionate vast impact on the network. In other words, the mapping of characters to substances isnumerous toone.Thiswillmakethetrustorreputationsystemofthemanageme ntentityfail.

Primary User Emulation Jammer - In cognitive radio network, a primary emulation jammer may alter its air interfacewiththe

end goal that it emulates the primary user's signal qualities causing otheroptional usersto dishonestlyestablish that the frequency is in being used by primary client, thus clear the frequency. This is conceivable since in anunfriendly domain, recognizing the primary userfrom othercan turnout to be a great degree troublesome.Themasquerade may execute the attack greedily, so he can utilize the range or maliciously, so the other genuine client willhavetheircommunicationdisturbed,bringingaboutarefusalof administrationattack.

Note that a jammer can start cross layer attacks through consolidating the attack models specified previously. A coupleofnormalcrosslayerjammersincorporate–

Selective Jammer - A selective jammer target particular packets of "high" significance. For instance, jamming of TCPACK's can seriously corrupt the throughput of a TCP association done to clog control component of TCP protocol. ItcanlikewisejamthoseessentialpacketsintheMACornetworkpro tocol.

ControlChannelJammer - Controlchanneljammers work is multi-channel network by focusing onthe controlchannel, or on the other hand the channel used to organize arrange action. An arbitrary jammer that aims the controlchannel could root a serious debasement of system execution, while a consistent jammer focusing on control channelmay refuse entrance network utterly. These attacks are normally proficient by bargaining a node in the network.Besides,futurecontrolchannelareas canbeacquiredfromthebargainednodes.

Lion Jammer - The Lionattack is particularto the cognitive radio network. The attack happens at the physical/linklayer while focusing on the transport layer. Basically, the jammer utilizes an essential user emulation attack keeping inmind the end goal to distort the TCP connection. The aggressor can be an outcast or a part of network. The attackinfluences the TCP by constraining frequency handoffs in clearing the channel because of the observation the essentialuser is available. At the point when handoff happens, the TCP doesn't know about the switchover. TCP will keepmakinglegitimateconnectionsalso,sendingpacketswhilenot acceptinganyACK.AssumingnoACKisreturned,

TCP thinks about fragment as lost due to clog. As an outcome, TCP retransmits the fragment while diminishing theblockagewindow.Thisresultsindelays what'smore,packetmisfortune,lessenthroughput.

Figure 3 demonstrates the above mentioned jamming attacks [2]. Moreover, the blend of different jamming models intime, frequency and protocol layer domains makes it illogical to cover all the conceivable jamming attacks models thatmightexist.Alongtheselines,wejustrundownacoupleofcom monattacksidealmodelhere-
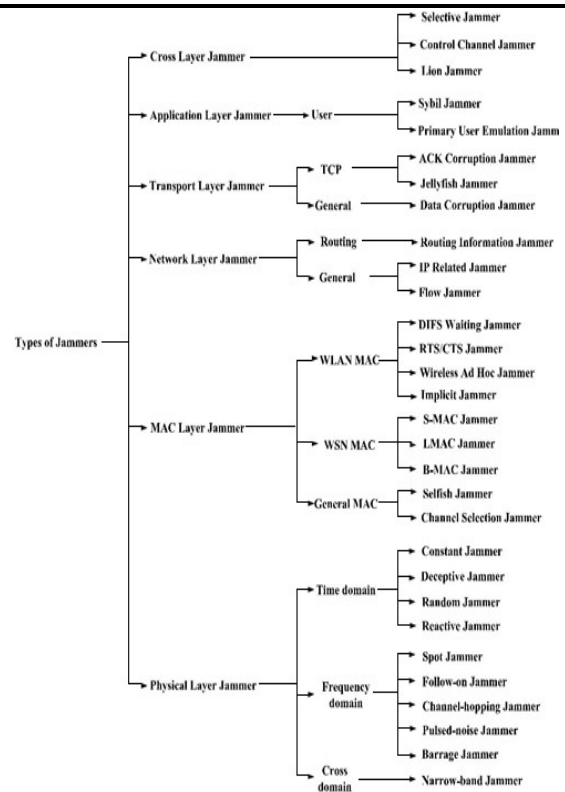

Fig.3:Jammingattacks

IV. COUNTERMEASURESAGAINSTJAMMING

Here we introduce a comprehensive audit of different countermeasures that have been proposed in order to overcomejammingattacks[6,19]. Thesejammingcountermeasures canbeoutlinedasfollowsintable3.

- *Appropriate power transmission* - The assailant's proficiency to find an objective is diminished when highpower for transmission is utilized. The effectiveness of the jamming signal ought to be higher than that of thenative signal so that the jammer can overwhelm the native signal. In the event that the transmitted power ishigh at that point there will be an accordingly more prominent confrontation towards jamming. Sensor nodesdisplayinWSNhavethecapacitytomodifythetransmitt er'syieldpower.

- *Frequency hopping spread spectrum* - In FHSS, radio signals of bearer are frequently exchanged betweenvarious frequency channels. Both the transmitter and the beneficiary utilize a pseudorandom arrangement ofbearer frequencies to accomplish fast exchanging. The transmitter and also the beneficiary deeds at a mutualalgorithm. Focal points of FHSS are that the capture of radio signals from unapproved parties is diminishedfurthermore, 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 thesingle region. The significant disadvantage of FHSS is that it requires considerably more extensive bandwidthfor the transmission of information. FHSS has a high jamming protection until the aggressor picks up thelearning about pseudorandom attributes. In military utilizations of Spread range, cryptography is utilized toscramble channel arrangement and the secret key is partaken ahead of time by the sender as well as thebeneficiary.

- *Direct sequence spread spectrum* - It is a method for spread spectrum regulation which makes a difference inlesseningobstructioninthenativesignal.Theinformationsignalfurthermore,Pseudo-commotionisaccumulate 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 likerepetitive sound has a more extensive transfer speed signal which replaces the native signal. At the beneficiaryend, the clamor is sifted through with a specific end goal to acquire back the native data by ascertaining theresult of RF signal and the beforehand utilized modulated bearer. DSSS has all the points of interest introduceinFHSS.

  Furthermore, it is more secured than FSHH on the grounds that it is troublesome to reestablish the transmittedsignal of DSSS. It winds up troublesome for the assailant to reestablish the DSSS signal. The DSSS signal islikerepetitivesound,makingithardtodiscovertheoriginoftransmission.

- *Hybrid FHSS/DSSS* - Hybrid FHSS/DSSS proposes a great answer for sticking as it gets the advantage of bothFHSS/DSSS.ObstructionisabstainedfromutilizingrecurrencebouncingframeworkthoughDSSSemployments is more extensive data transmission to diminish obstruction which infers that protection fromstickingcanbeexpandedsurprisinglybyutilizingboththe approachtogether.PropertieslikeLowlikelihoodof location and low likelihood of block attempt can likewise be accomplished by utilizing this strategy. Highquality capture types of gear are required to capture the frequency changes. To recuperate the native signalboth the Pseudo-clamor and the Frequency grouping are required. Hybrid FHSS/DSSS has the capacity tobattle against the close far impact. In spite of the expansion in multifaceted nature of

attune, hybrid techniquesare facile but difficult to execute since littler PN codes and lesser number of trusting frequencies can beutilized.

Directional transmission - Presently days, Omni-directional transmission antennas are utilized as a part of thesensor nodes. These antennas are equipped for transmitting and getting waves from each conceivable course ata similar purpose of time which prompts security issues and diminishes the unwavering quality of theseantennas while onotherhand,the directional antennas transmits andgets injusta particulardirection.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 imperviousto obstruction. Directional transmission has a few issues related with it. It requires a legitimate MAC protocoland directing in various ways turns into a troublesome undertaking. Directional antennas are additionallyorderedintotwosortsofantennas:BeamformingantennasandSectoredantennas.Insectoredantennas,vast number of stable antennas, looking towards different directions that have the ability of working autonomouslyare available. In Beam forming, every one of the antennas work at the same time so as to transmit and getwaves indifferentdirections.

Polarization of antenna - The polarization of antenna can be characterized as the emplacement of antenna andthe transmitted vitality created by them.Polarization is reliant on the structure and the emplacement ofantenna. To relay with the diverse antennas, it is obligatory to have same polarization between them. Forinstance, if an antenna is having a vertical polarization, it won't have the capacity to impart with antennahaving right round polarization.Anobservable pathway ought to be kept up to set up a communication andthis property can help nodes injamming condition, if a node recognizes any obstructionin nature, it canchange its polarization and spare the system from jamming. The greatest challenge in this strategy is that eachnode in the system must illuminate alternate nodes about the changing polarization before any real change inits polarization with the goal that the communication won't be intruded. To defeat this issue, nodes ought to becustomizedaheadoftimetomanagethisissue.

Table3: CountermeasuresagainstJammingattack

COUNTERMEASURES	SALIENTFEATURES
FREQUENCYHOPPINGSPREADSPECTRUM	Usesspeedspectrummethodfortransmittingsignals AdvantageousforWSN Jammingcanbecontrolled Providesa betterSNRratio

DIRECTSEQUENCESPREADSPECTRUM	Data is multiplies with pseudo- random digital signal whichisasequence of1and-1 Replacesoriginalsignalwithwidebandwidthsignal Difficultforattackertoobtainoriginalsignal Difficulttofindthetransmittingsource
HYBRIDFHSS/DSSS	Helpstosolvenear-far problems Highresistancetojamming SharesthefeaturesofbothFHSS/DSSS Low probabilityofdetectionandlowprobabilityofinterception
ULTRAWIDEBANDTECHNOLOGY	Hardtointercept Longerbatterylifetime Difficulttojoin Solvesmultipatheffectproblem Widefrequencybandfortransmission
POLARIZATIONOFANTENNA	Dependentonstructureofantenna Effectivesolutionforjammingenvironment Polarizationreducesinterferenceamongnodes Nodeswithsimilarpolarizationcancommunicate
DIRECTIONALTRANSMISSION	Reliableandsecured Transmitssignalsinaspecificdirection Defensivemechanismagainstjammingattacks Categorizedintobeamformingantennasandsectoredantennas

- *Ultra wide band technology* - Ultra wide band is an innovation utilized fortransmitting informationbyspreading the radio vitality in a huge frequency band utilizing a low control spectral density which helps inrestricting the impedance from the conventional radio sources, a highthroughput canbe achievedfrom thehigh transfer speed utilized as a part of UWB. This attune innovation transmits shorter pulses over a frequencyband of wide range. In this, the sensor systems are sent in savvy way and devours low power. This innovationmakes 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 openresearchissueandstillbeingworkedon.

V. CONCLUSION

A Mobile Ad hoc Network (MANET) is a gathering of mobile hosts that relies upon wireless network interfaces havinglike open network boundary, dynamic topology and wireless communication. Hence security becomes profoundlysusceptible. Jamming attacks are a subset of denial of service (DoS) attacks in which noxious nodes obstruct authorizedcommunication by causing deliberate impedance in network. In this extensive study on jamming and anti-jammingtechniquesinwirelessnetworks,we have contributedby classifyingandcondensingvariousmethodologiesanddiscussing open research issues in the field. Different jammers attack wireless networks in distinct ways so that theirattack impacts are significantly different. The target of this survey is to provide the readers withbasic understandingandquickreferencetovarious sortsofjammersanditscountermeasures basedontheirapplication,ifused.

REFERENCES

1. Tada,N.,Patalia,T.,andRupani,P.,"ANewApproachtoMitigateJammingAttackinWirelessAdhocNetworkUsingARCTechnique",SpringerInternationalConference onFuture InternetTechnologiesandTrends,pp.192-204,2018.
2. Wei,X.,Wang,Q.,Wang,T.,andFan,J.,"JammerLocalizationinMulti-HopWirelessNetwork:AComprehensiveSurvey",IEEECommunicationsSurveys&Tutorials,Vol.19,IssueNo.2,pp.765-799,2017.
3. Bhojani,R.,andJoshi,R.,"AnIntegratedApproachforJammerDetectionusingSoftwareDefinedRadio",ScienceDirectInternationalConferenceon Communication,ComputingandVirtualization,Vol.79,pp.809-816,2016.
4. Rahman,F.H.M.A.RandAu,T.W.,"ImpactofIPseconMANET",IEEEInternationalSymposiumonComputer,ConsumerandControl,pp.408-411,2016.
5. Dong,Y.andZhou,P.,"JammingAttacksagainstControlSystems:ASurvey",SpringerInternationalConferenceonLifeSystemModelingandSimulation,pp.566-574,2017.
6. Jaitly,S.,Malhotra,H.,andBhushan,B.,"SecurityVulnerabilitiesandCountermeasuresagainstJammingAttacksinWirelessSensorNetworks:ASurvey"IEEEInternationalConferenceonComputer,CommunicationsandElectronics(Comptelix), pp.559-564,2017.
7. Yuan,L.,Wang,K.,Miyazaki,T.,Guo,S.,andWu,M.,"OptimalTransmissionStrategyforSensorstoDefendagainstEavesdroppingandJammingAttacks",IEEE InternationalConference on Communications,2017.
8. Kikuchi,K.,Cetinkaya,A.,Hayakawa,T.,andIshii,H.,"StochasticCommunicationProtocolsforMulti-AgentConsensusUnderJammingAttacks",IEEE56th AnnualConference onDecisionand 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 VARIOUSATTACKS UNDERAODV INWSN&MANETUSINGOPNET14.5", IEEE Annual Ubiquitous Computing, Electronics& MobileCommunicationConference,2016.
10. Aldarraji, A., Hong, L., and Shetty, S., "Polarized Beamforming for Enhanced Countermeasure of Wireless Jamming attacks ", IEEE 35thPerformanceComputingand CommunicationsConference,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 usingMaliciousandIrrelevantPacketDetectionAlgorithm(MIPDA)",IEEEInternationalConferenceonComputing,CommunicationandAutomation,pp. 414-419,2015.

12. Sharma, P., and Suryawanshi, A., "Enhanced Security Scheme against Jamming attack in Mobile Ad hoc Network", IEEE InternationalConferenceonAdvancesinEngineering&Technology Research,2014.

13. Hamie, A., "POWJAM: A Power Reaction System against Jamming Attacks in Wireless Ad Hoc Network", IEEE 9th Annual Conference onWirelessOn-DemandNetwork SystemsandServices,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 onEmergingTechnologies,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 LocalComputerNetworks,pp-758-762,2009.

16. Liu, Z., Liu, H., Xu, W., and Chen, Y., "Exploiting Jamming-Caused Neighbor Changes for Jammer Localization", IEEE Transactions onParalleland DistributedSystems,Vol.23,IssueNo.3,pp.547-555,2011.

17. Chaturvedi, P., and Gupta, K., "Detection and Prevention of various types of Jamming Attacks in Wireless Networks", IRACST InternationalJournalofComputerNetworksand WirelessCommunications,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", IEEESecondInternationalConferenceon ScienceTechnologyEngineeringandManagement, 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 AdHocand UbiquitousComputing,Vol.x, IssueNo.x,xxxx,pp.1-16,2014.