Mobile Ad-Hoc Network Attacks on IDS: A Review

Hemlata Kaurav[1], Krishna Kumar Joshi[2]
[1, 2] Department of Computer Science Engineering
[1, 2] Maharana Pratap College of technology, India

Abstract- *Ad-hoc networks have lots of difficulties than conventional networks. It has challenges like foundation less and self-organizing networks. They don't have any settled base. In MANETs there will be no incorporated power to manage the network. Nodes need to depend on different nodes to keep the network connected. As the ad-hoc network is dynamic and each transmission in these networks get to be powerless against numerous number of attacks and security turns into a major issue.*

Keywords- MANET; IDS; Packet dropping attack.

I. INTRODUCTION

A Mobile Ad hoc Network (MANET) is an accumulation of mobile node associated through wireless links. In MANET all nodes are associated with the nodes close in correspondence range. So if a node needs to impart to another node it sends the data to the destination node through the neighbour node. Presently the neighbour node will go about as router prefers wired network. In wired network security protocols will be actualized in router node. Yet, actualizing security in MANET is a testing errand. Since here node itself will be going about as a router node. So distinguishing neighbour node as an honest to legitimate node or malicious node is a troublesome thing in MANET. Correspondence in the network relies on the trust on one another likewise correspondence can work appropriately if every node co-operates for data transmission. As MANET has no fixed infrastructure, they have more security threats when contrasted with the base based wireless networks. Every correspondence layer has heaps of attacks in MANET because of it dynamic nature, absence of unified monitoring, and restricted resources like bandwidth and battery power [1].

A. Security Goals

The accompanying are five major security objectives which require keeping from attacks [2]:

a) Authentication:

Authentication guarantees that the correspondence or transmission of data is done just by the approved nodes.[3] Without authentication any malicious node can profess to be a trusted node in the network and can antagonistically influence the data transfer between the nodes.

b) Availability:

Availability ensures the services ought to be accessible even in the vicinity of the attacks. Frameworks ought to have the capacity to deal with various attacks for example, denial of services, energy starvation attacks, and node misbehavior.

c) Confidentiality:

Confidentiality ensures that data ought to be available just to the planned party. No other node with the exception of sender and receiver node can read the data. This is actualized through data encryption methods.

d) Integrity:

Integrity ensures transmitted data is not being adjusted by some other malicious node.

e) Non-Repudiation:

Non-repudiation ensures that ought neither a sender nor a beneficiary to not deny a transmitted message.

B. Security Challenges

a) Dynamic topology:

In MANETS node might join or leave progressively. As node moves as often as possible setting up trust among nodes is extremely difficult [1].

b) Battery Constraints:

Mobile nodes will be running with battery. On the off chance that node power used pointlessly then node might come to sit out of gear state.[4]

c) Lack of Central Authority:

In MANET there will be no incorporated power like base network. So implementing security without unified power is a testing assignment.

d) Insecure Environment:

Nodes might move arbitrarily in MANET. So malicious node might attack and take the data.

II. INTRUSION DETECTION SYSTEM

Intrusion detection is the procedure of monitoring the occasions happening in a computer system or network and investigating them for indications of conceivable occurrences, which are infringement or fast approaching dangers of infringement of computer security policies, adequate use policies, or standard security practices [5]. IDS can be named: Network construct IDS which keeps running on a gateway of a network obtained audit data from traffic that courses through it, and afterward are examined the data gathered and Host based IDS which obtains this data through trust rating system's log documents that keep running on the node. Contingent upon the detection strategies utilized, IDS can be grouped into three primary classes:

a) Signature-based (Misuse discovery model):

It thinks about known danger marks to watched occasions for identifying intrusion. This is an extremely powerful model for recognizing known dangers yet is predominantly inadequate at identifying obscure dangers and numerous variations on known dangers. Signature-based detection can't track and comprehend the condition of complex communications, so it can't distinguish most attacks that involve numerous events.

b) Anomaly-based detection:

It looks at meanings of what movement is considered as should be expected against watched occasions to recognize huge deviations (atypical conduct). This is finished by monitoring the qualities of run of the mill movement over a timeframe through profiles looked after. The IDPS then analyzes the attributes of current action to limits identified with the profile. Peculiarity based detection techniques are of high use at identifying beforehand obscure dangers yet might create numerous false positives as a slight deviation in user activity might bring about an alarm.

c) Specification-based detection:

It characterizes an arrangement of requirements that clarifies the right operation of a program or protocol. It checks the execution of the system regarding characterized requirements. This system gives a capacity of recognizing already obscure attacks with low false positive rate.

III. MANET ATTACKS

a) Active Attacks

Performed by attackers for reproducing, modifying and deletion of traded data. They attempt to change the conduct of the protocol [6]. These attacks are intended to corrupt or avoid message stream among the nodes. Such attacks all in all can be called as DOS attacks that either corrupt or totally obstruct the correspondence between the nodes. Another sort of attack includes insertion of incidental packets in the network to bring about blockage. Obsolete routing data might be replayed back to the nodes in the network. Active attacks can be identified now and then and this reason makes active attack less utilized by an attacker.

b) Passive Attacks

This sort of attack includes unapproved listening of the routing packets. Attacker might listen in on all the routing updates. For this situation an attacker does not disturb the operation of a routing protocol rather it just listens to it to find the important data about the routing. Such attacks are hard to be detected. From the routing packets an attacker might comprehend around a node which is essential in the network and route to that node is being asked for all the time by each other node. So an attacker tries to debilitate this node to cut the network down. Incorporates Covert channels, Traffic investigation, analysis, shifting to trade off keys.

IV. PACKET DROPPING ATTACK

In MANET, a packet dropping attack is a sort of denial of service in which a node in the network will drop the packets as opposed to sending them, which is appeared in the fig 1. The packet dropping attack [7], [8], [9] is difficult to identify and anticipate on the grounds that it happens when the node gets to be bargained because of various diverse causes. The packet dropping attack in MANETs can be characterized into a few classifications regarding the system embraced by the malicious node to dispatch the attack.

a) The malicious node can deliberately drop all the sent packets experiencing it (black hole).
b) It can specifically drop the packets began from or bound to specific nodes that it disdains.

c) An uncommon instance of black hole attack named gray hole attack is presented. In this attack, the malicious node holds a bit of packets (one packet out of N got packets or one packet in a specific time window), while the rest is ordinarily transferred.

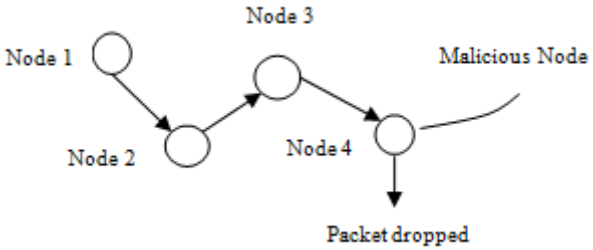

Fig A:- Packet Dropping Attack

The compromised node will show the message [9], [10] that it has the briefest way towards a destination to start packet dropping attack. Consequently, all packet transmissions will be coordinated through the compromised node, and the node can drop the packets. On the off chance that the malicious node end eavors to drop every one of the packets, the attack can be recognized through regular systems networking tools. Besides, when different routers notice that the traded off switch is dropping all packets, they will for the most part start to expel that router from their sending table. Henceforth, there is no packet transmission through the traded off node. Be that as it may, it is frequently harder to recognize the detect the packet dropping attack.

Malicious Packet Dropping

Generally, the initial phase in dispatching a packet dropping attack is for a malicious node to get included amid course development. This is better done by misusing the vulnerabilities of the fundamental surely understood routing protocols utilized MANETs which are composed basing on the presumption of reliability between nodes in a network. Once in the course, the malicious node can do anything including maliciously dropping packets. This Packet dropping at a malicious intermediate node can prompt suspension of correspondence or era of wrong data between the source and destination which is an undesirable circumstance.

a) Packet Dropping in AODV

The route revelation process between source (S) and destination (D) under AODV routing protocol is as delineated in Figure 2.The source shows a RREQ (Route Request) message with remarkable identifier to all its one bounce neighbors. Every collector rebroadcasts this message to its one bounce neighbors until it achieves the destination. The destination on accepting the message redesigns the grouping number of the source and sends a RREP (Route Reply) message back to its neighbor which transferred the RREQ. Then again, a halfway hub that has a course to the destination with destination grouping number equivalent to the one in RREQ can send back a RREP parcel to the source node without handing-off to the destination. For a node to dispatch parcel dropping attack, it must be included in no less than one routing ways in the network. This is delineated in Figure 2; C is a malicious node proposing to drop packets from S to D. To find a way from S to D, S first shows RREQ packet to its neighbors. Each neighboring node keeps on rebroadcasting this message as clarified before until it achieves D.

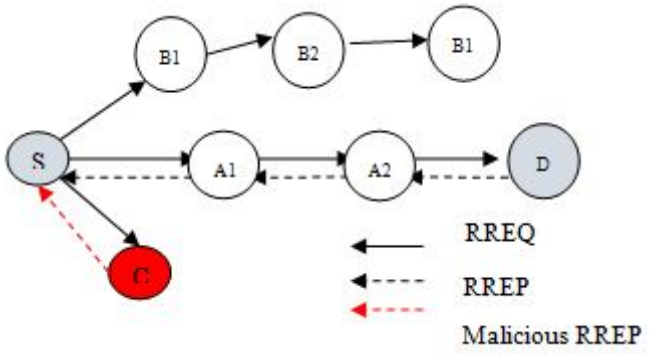

Fig B:- Packet Dropping Attack in AODV

The malicious node C defies this tenet and deceives S claiming it has the most limited way to D and sends a RREP packet to S. Accordingly, S accept that the briefest course to D is through C and begins to send data packets to D through C which are thusly dropped.

The following attacks are given in the literature:

a) Flooding Attack

In this attack when utilized against an on-interest specially appointed network routing protocol, a malicious node creates a large number of fake route requests (RREQ) tended to a destination that does not exist in the network. Following these course demands will never get an answer, they will surge the whole network and stuff the connections. This outcomes in the fatigue of network resources, similar to bandwidth consumption and in addition utilization of a node's resources, as computational and battery power. Thus this attack is otherwise called lack of sleep deprivation or resource utilization attack. This attack break down the execution of the network by upsetting the routing operation. It eventually leads to denial of service.

b) Black hole Attack

In a black hole attack, in the wake of listening to the route request packet in the network the attacker node cases to have an amazingly short course to the asked for destination. The attacker does as such by sending a created RREP to the source node. In this RREP, the destination succession number is set to be equivalent to or more noteworthy than the one contained in RREQ. This gives the source node the false impression that the malicious node has the freshest course to the destination. Subsequently the source node picks the course going through the attacker to send the data packets. Presently since the vast majority of the network traffic goes through the malicious node, it can either drop the packets or control the traffic in any capacity it needs.

c) Wormhole attack

An attack which is otherwise called the tunnelling attack, this attack is conceivable regardless of the fact that the attacker has not traded off whatever other legitimate nodes and regardless of the fact that all correspondence gives legitimacy and secrecy. Consequently it is a standout amongst the most extreme and sophisticated attacks in MANETs. In this attack, a couple of malicious nodes are associated through a speed network, otherwise called the passage. Here, when the attacker gets a RREQ, it advances it to its intriguing accomplice through the passage. The malicious node on the opposite side of the passage, subsequent to accepting this RREQ, replays it to its neighboring hubs. This course demand would be the first to achieve the destination node since it has gone through a quicker medium than the connections between legitimate nodes. In this way the intriguing nodes would most presumably be incorporated into the course, which would give them the opportunity to abuse or discard packets.

d) Selective Forwarding Attack

This attack is otherwise called the gray hole attack. This attack is a refined variant of black hole attack. Not at all like black hole attack, here had has the malicious node dropped just chosen packets and advances different packets, consequently making the location of malicious node troublesome. This attack can be led in different ways. The attacker can either choose a specific source or destination deliver and can decline to forward or drop every one of the packets containing the individual source or destination addresses, or the attacker can arbitrarily choose the packets to be dropped. The previous causes denial of service attack for a particular node. Another type of specific sending attack is to delay packets going through the attacker and consequently making befuddled routing data between the nodes.

e) Selfish Node Attack

In this attack, the node stops using its resources such as bandwidth etc., it stops forwarding or relaying packets. It does so without the network knowing. It does not participate in any of the network operations but uses it for its selfish purposes like saving its own resources like power. This results in highly decreased performance of the network

f) Link Spoofing Attack

In this attack, a malicious node presents false information of having a link with non-neighbors. In OLSR, for example, the attacker can convince the source to include it in its MPR set by presenting false information of having a link to its two-hop neighbors. After the malicious node is chosen to be its MPR, it gets the authority to alter the traffic as desired. It can as a result drop the packets or withhold them in order to degrade the performance of the network immensely.

g) Sybil attack

Here the single attacker node behaves as if it were a group of a number of nodes. It appears to other nodes as a number of different nodes but it is actually a single malicious node. By doing so, it can prevent other nodes from using those addresses. A Sybil attack can be performed in various forms. In Sybil attack, a Sybil node can obtain the identity in two ways either by stealing other node's identity i.e. impersonation or by fabricating false identities. The Sybil node can communicate both directly and indirectly with the legitimate nodes. Also the attacker can have his Sybil identities all participate in the network at once i.e. simultaneously or they can participate in fractions i.e. non-simultaneously. As a result in routing, the seemingly disjoint paths could in fact go through a single malicious node presenting several Sybil identities. These identities can manipulate the traffic by disrupting routing operation.

h) Blackmail Attack

In this attack a legitimate node is misrepresented as a malicious node by the attacker node. Here the malicious node makes an entry of a legitimate node in its blacklist table giving false appearance of being malicious to the legitimate node. This attack occurs against protocols that uses attack detection mechanisms like watchdog and path rater. The malicious node exploits the vulnerabilities of these mechanisms to blackmail a legitimate node. The attacker node thus provokes other legitimate nodes to put this target legitimate node as an attacker in their blacklist table. This results in a good node being considered as a bad node by the network.

i) Location Disclosure Attack

In location disclosure attack, the attacker with the help of traffic analysis techniques or simpler probing and monitoring approaches can get access to highly confidential and important information such as location of nodes, structure of the entire network etc. Here the traffic is analyzed in order to know the traffic patterns and track changes, also the identities of the communicating nodes is collected, after which further attack is planned and launched. This attack is aimed to hamper with the privacy aspect of the network and is lethal for security sensitive scenarios.

j) Detour Attack

Also known as the gratuitous detour attack, this attack is specific to source routing protocols. This attack detours traffic through congested or energy-depleted routes by modifying the route request metrics in such a way that it appears more costly than the route that the attacker aims to detour traffic to. The traffic can be detoured in many ways such as increasing the hop count or delaying rebroadcasting route requests. Also the malicious node during route discovery phase adds a number of virtual nodes to the route. As a result the traffic is deflected to other routes which might appear shorter and less costly. These routes might have other malicious nodes which might launch other attacks. Due to this detour, the energy of the malicious node is saved highly since it doesn't have to forward packet to the destination itself.

ATTACK	ATTACK TYPES	EFFECT ON DATA COMMUNICATION	DETECTION MECHANISMS
Blackhole attack	Non co-operative	Degrade packet delivery ratio	Watchdog
Warmhole attack	Co-operative(needs atleast two attackers)	Degrade packet delivery ratio	ACK-based schemes
Jellyfish attack	Co-operative and Non-co-operative	Degrade end-to- end-delay and packet delivery ratio	Reputation-based schemes
Rushing and flooding attack	Non-co-operative	Increase routing overhead and network contention and congestion	Incentive based schemes
Sybil attack	Non-co-operative	Degrade packet delivery ratio and provide false network topology option.	Lightweight Sybil attack detection
Node-misbehavior attack	Co-operative and Non-co-operative	Provide false network topology information and increase jitter	CONFIDENT
Gray hole attack	Non-co-operative	Degrade packet delivery ratio	Ex-Watchdog

V. RELATED WORK

Here discussing about the various existing approaches for detecting this attack Packet Dropping Attack Detection Techniques Various malicious packet dropping detection systems have been proposed in literature. In this segment we talk about some of them;

a) Watch Dog Technique

The watch dog strategy has been the most surely understand node bad conduct detection in ad hoc networks. In this strategy, each node goes about as a watchdog agent monitoring packet transmissions to neighboring nodes [11]. The watchdog agents spare a duplicate of packets in their watchdog monitoring supports before their transmission to the following node. This serves to monitor packet hand-off from a neighboring node to the following node.

b) Side Channel Monitoring (SCM)

In SCM a sub-set of neighbors for every node in a course in the middle of source and destination are chosen to watch and screen their message sending practices [12]. Alarm

channel (Primary channel and Side channel) is created to educate the source about the getting into misbehaving node; The Primary channel (PC) is framed by nodes in the course and Side channel (SC) is shaped by sub-set of monitoring neighbors.

c) Monitoring Agent Technique

[13], proposed the monitoring agent strategy. The system depends on neighboring so as to catch packets sent nodes inside of a transmission range. Every one of the nodes in a network gather data about their one bounce neighbors inside of a specific timeframe. The gathered data incorporate; the aggregate number of packets transmitted from a particular node (WLi), the normal number of transmitted packets from all its one jump neighbors (AWL), the packet drop rate of a specific one bounce neighbor (DRi), and the normal packet dropping rate by all its one jump neighbors (ADR) which are utilized for recognizing a malicious node.

d) PathRater

PathRater is controlled by each node in the network [14] [15]. A node keeps up evaluations for each other node it knows in the network basing on the information of misbehaving nodes and connection reliability data with a specific end goal to pick the most suitable way. A way metric is ascertained by averaging the appraisals for nodes in the way. In the event that there is more than one way to the destination, the way with the most astounding metric is picked. A pathrater node appoints an impartial rating of 0.5 to nodes known not.It typically allots itself a rating of 1. The appraisals are overhauled in interims of 200ms. The appraisals for nodes in active path are expanded by 0.01 and the greatest rating a node can achieve is 0.8. A node's evaluating is diminished by 0.05 when a connection break is recognized and the node gets to be inaccessible. A negative way metric quality shows vicinity of misbehaving nodes in the way. Because of issues or false allegations, a node might be set apart as a getting out of misbehaving node. It is by and large better not to forever stamp it as misbehaving node. Accordingly, the checked misbehaving nodes' evaluating ought to be expanded gradually or set back to 0.0 after quite a while period.

e) TwoAck

In this procedure, packets sent by a node are relied upon to be gotten by nodes which are two bounces away in the path [16]. Nodes in a way are relied upon to send affirmation packets called TWOACK packets two jumps in reverse. On the off chance that a node neglects to get TWOACK packet in the wake of sending or sending packets, the following node's connection is thought to be making trouble and will be disposed of in the following steering. Keeping in mind the end goal to lessen the overhead because of these affirmation messages, a plan called particular TWOACK (S-TWOACK) which specifically recognizes packets was proposed in [17]. In this plan, an affirmation is sent subsequent to accepting certain number of data packets.

In existing technique LeovigildoSánchez-Casado [18] et al expected to distinguish malicious packet dropping practices in MANETS. For that, components from MAC and network layers are considered. Additionally, the cross layer methodology depends on an analytical model that speaks to the sending process in an ad hoc network. author work on two layer one is network layer and second is mac layer mac layer are used for directional connectivity in which first source send RTS and after that if CTC is receive communication take place. Network layer use for secure routing.

VI. CONCLUSION

Packet-dropping attack has dependably been a noteworthy risk to the security in MANET. In this paper we have introduced an overview of the best in class on securing MANETs against packet dropping attack. A large portion of the current methodologies are utilized to identify just the bad conduct interfaces as opposed to the malicious nodes. Besides, they neglect to identify halfway dropping of packets in MANET. The detection of packet droppers in MANETs is a test despite the fact that numerous methodologies have been proposed against packet dropping attack. Some methodologies that depend on cryptography and key management are too expensive.

REFERENCES

[1] Hao yang, Haiyunluo, Fan ye, Songwulu, and Lixiazhang,"Security in Mobile Adhoc Networks:Challenges and Solutions", IEEE WirelessCommunications, Feb 2004

[2] C.-K Toh, Ad Hoc Mobile Wireless Networks:Protocols and Systems, Prentice Hall, New Jersey, pp:34-37, 2007.

[3] J.P.Hubaux, L.Buttyan, S.Capkun, "The Quest ForSecurity In Mobile Ad Hoc Networks," Proceedingsof the ACM Symposium on Mobile Ad HocNetworking and Computing (MobiHOC), October,2001.

[4] I.Chlamtac, M.Conti, and J.Liu, "Mobile Ad HocNetworking: Imperatives and Challenges," Ad HocNetworks, vol. 1, no. 1, pp. 13-64, 2003.

[5] Noman Mohammed, HadiOtrok, Lingyu Wang, MouradDebbabi and Prabir Bhattacharya "Mechanism Design-Based Secure Leader Election Model for Intrusion Detection in MANET", IEEE Transactions on Dependable and Secure Computing, vol. 99, no. 1, 2008

[6] C. Siva Ram Murthy, and B.S. Manoj, Ad HocWireless Networks: Architectures and Protocols,Prentice Hall communications engineering andemerging technologies series Upper Saddle River,New Jersey, 2004.

[7] S. Djahel, F.N. Abdesselam, Zonghua Zhang, Mitigating Packet Dropping Problem in Mobile Ad-hoc Networks : Proposals andChallenges, IEEE Communications Surveys & Tutorials, Vol.13, No.4, Fourth Quarter 2011.

[8] E. Hernandez, M.D. Serrat, Improving Selfish Node Detection in MANETs Using a Collaborative Watchdog, IEEE CommunicationsLetters, Vol.16, No.5, May 2012.

[9] N. Kang, E. Shakshuki, and T. Sheltami, "Detecting misbehaving nodes in MANETs," in Proc. 12th Int. Conf. iiWAS, Paris, France,Nov. 8–10, 2010, pp. 216–222.

[10] N. Kang, E. Shakshuki, and T. Sheltami, "Detecting forged acknowledgements in MANETs," in Proc. IEEE 25th Int. Conf. AINA,Biopolis, Singapore, Mar. 22–25, 2011, pp. 488–494.

[11] S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad hocNetworks", Proc. 6th Annual Intl. Conf. on Mobile Computing and networking (MobiCom'00),Boston, Massachusetts, August 2000, pp. 255-265.

[12] X. Li, R. Lu, X. Liang, and X. Shen, "Side Channel Monitoring: Packet Drop Attack Detection inWireless Ad hoc Networks", publication in the IEEE ICC proceedings, 2011.

[13] J. Ko, J. Seo, E. Kim and T. Shon, "Monitoring Agent for Detecting Malicious Packet Drops forWireless Sensor Networks in the Microgrid and Grid-enabled Vehicles", International Journal ofAdvanced Robotic Systems, 19 Apr 2012.

[14] P. Peethambaran and J. S. Jayasudha, "Survey Of Manet Misbehaviour Detection Approaches",International Journal of Network Security & Its Applications (IJNSA), Vol.6, No.3, May 2014.

[15] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad HocNetworks", Available from: http://www.cs.cmu.edu. Accessed on: 28th August 2014.

[16] K. Balakrishnan, D. Jing and P.K. Varshney, "TWOACK: Preventing Selfishness in Mobile Ad HocNetworks", Wireless Communications and Networking Conference, IEEE, 2005.

[17] K. Balakrishnan, J. Deng, and P.K.Varshney," TWOACK: Preventing selfishness in Mobile Ad HocNetworks," Proc. IEEE Wireless Comm. and Networking Conf. (WCNC'05), Mar.2005.

[18] Leovigildo Sánchez-Casado, Gabriel Maciá-Fernández, Pedro García Teodoro, Roberto Magán-Carrión ,"A model of data forwarding in MANETs for light weight detection of malicious packet dropping". Elsevier, 2015.