JCSE International Journal of Computer Sciences and Engineering Open Access

Survey Paper Volume-6, Issue-1 E-ISSN: 2347-2693

Survey Paper on Various Security Attacks In Mobile Ad Hoc Network

M.Selladevi[1], S. Duraisamy[2]

[1] PG and Research Department of Computer Science,Chikkanna Govt Arts College Tiruppur, Tamil Nadu, India
PG and Research Department of Computer Science,Chikkanna Govt Arts College Tiruppur, Tamil Nadu, India

Corresponding Author: mschella30@gmail.com,

Available online at: www.ijcseonline.org

Received: 22/Dec/2017, Revised: 31/Dec/2017, Accepted: 19/Jan/2018, Published: 31/Jan/2018

Abstract- Mobile Ad-Hoc Network is a self-configured collection of cellular nodes in which there is no need of predefined infrastructure. In this network nodes can arbitrarily alternate their geographic places. MANET is more vulnerable to cyber-attacks than wired networks because of no any central coordination mechanism. Because of their dynamic topology, no infrastructure and no central management system MANETs are liable to various security attacks. In this paper we have proposed a solution to detect and prevent multiple attacks in a network and find a secure way to transfer data from source to destination node. This article briefly discusses about the concept of Mobile Ad Hoc Network (MANET) and its various types of attack and methods to solve the MANET attacks.

Keywords- Ad-hoc network, Infrastructure less network , Dynamic topology, Security attacks

I. INTRODUCTION

A mobile ad hoc network (manet) is a wireless communication network in which nodes that aren't inside direct transmission range establish their communication through the help of other nodes to forward the data. It may function without a constant infrastructure, support consumer mobility and falls under the fashionable scope of multi-hop wireless networking. This sort of networking paradigm originated from the needs in battlefield communications, emergency operations, search, rescue, and disaster relief operations. The network layer has obtained maximum attention when working on mobile ad hoc networks. As an end result, plentiful routing protocols were proposed. Two most vital operations at the network layer are routing and forwarding. Forwarding regulates how packets are taken from one hyperlink and placed on some other. Routing determines which path an information packet has to follow from the supply node to the destination.

II. MOBILE AD-HOC NETWORK (MANET) ROUTING PROTOCOLS

Nodes in ad hoc network also characteristic as routers that discover and maintain routes to different nodes in the network. Thus the primary aim of MANET is to set up an accurate and efficient path between a couple of nodes and to ensure the ideal and timely delivery of packets. A routing protocol is needed each time a packet needs to be transmitted to a destination through number of nodes and numerous routing protocols were proposed for such sort of mobile ad hoc networks. Those protocols discover a route for packet delivery and supply the packet to the perfect destination [3]. Manet routing protocols divided into three trendy classes:

1. Proactive routing protocols

2. Reactive routing protocols

3. Hybrid routing protocol

Pro-active /Table driven routing protocols

These kinds of protocols are referred to as table driven protocols in which, the route to all the nodes is maintained in routing table. Packets are transferred over the predefined route specified in the routing table. In this scheme, the packet forwarding is done faster however the routing overhead is extra because all the routes ought to be defined earlier than shifting the packets. Proactive protocols have decrease latency because all of the routes are maintained at all the times. Example protocols: DSDV, OLSR (Optimized Link State Routing), Destination-Sequenced Distance-Vector (DSDV) protocol.

Reactive/On-demand protocols

These kinds of protocols also are called as on demand routing protocols in which the routes are not predefined for routing a source node calls for the route discovery segment to determine a new route each time a transmission is wanted. This route discovery mechanism is primarily based on flooding algorithm which employs on the approach that a node simply declares the packet to all of its neighbors and intermediate nodes simply forward that packet to their neighbors. This is a repetitive approach until it reaches the destination. Reactive techniques have smaller routing overheads however higher latency. Example protocols: DSR, AODV (Ad hoc On-demand Distance Vector routing).

Hybrid protocols

Hybrid protocols are the mixtures of reactive and proactive protocols and takes advantages of these protocols and as an end result, routes are found quick within the routing zone. Example protocol: ZRP (Zone Routing Protocol).

CLASSIFICATION OF ATTACKS

The classification of attack may be accomplished on the premise of starting place of attack. It could be classified as following

Black hole attack

Black holes refer to locations within the network where incoming or outgoing site visitors is silently discarded (or dropped), without informing the source node that the facts did now not attain its intended recipient. Black holes are certainly invisible and might only be detected by means of tracking the misplaced site visitors. In black hole attack, attackers embed itself into the path from source though destination with the aid of sending a fake RREP containing higher sequence number giving that impact that it has the freshest route closer to destination. Then the source may be captured into constructing a direction through malicious nodes and rejecting all other to be had paths. After doing that, whilst the statistics packets are to be transmitted towards destination, the attacker will sincerely drop they all and as a consequence destination will no longer be able to receive even an absolutely piece of information [1]. Black hole attacks are categorised into categories:

Single Black hole attack

In single Black hole attack only one node acts as malicious node within an area. It is also referred to as Black hole attack with single malicious node.

Collaborative Black hole attack

In Collaborative Black hole attack more than one nodes in a group act as malicious node. It's also known as Black hole attack with multiple malicious nodes.

Wormhole attack

An attacker statistics packets at one place within the network and tunnels them to any other place. Routing can be disrupted whilst routing manage messages is tunnelled. This tunnel among two colluding attackers is called a wormhole. Wormhole attacks are extreme threats to MANET routing protocols.

Byzantine attack

A compromised intermediate node works on my own, or a hard and fast of compromised intermediate nodes works in collusion and carry out attacks which includes creating routing loops, forwarding packets via non-most advantageous paths, or selectively dropping packets, which ends up in disruption or degradation of the routing carrier.

Rushing attack

Two colluded attackers use the tunnel system to shape a wormhole. If a quick transmission course (e.g. a committed channel shared by attackers) exists between the two ends of the wormhole, the tunneled packets can propagate faster than the ones via a normal multi-hop route. This forms rushing attack [4].

SYN flooding attack

Malicious nodes send numerous SYNs and do not longer send the very last acknowledgment to the ACK sent with the aid of the genuine node. It causes Denial of service. This type attack known as SYN flooding attack [9].

III. LITERATURE REVIEW

Gupta et al [5] proposed a brand new technique referred to as RTMAODV (real Time monitoring AODV). It does no longer introduce any overhead. Furthermore, neighbor node detects and prevent black hole attack the usage of actual time monitoring. Source Node sends Route Request (RREQ) is being monitored in promiscuous mode. Detection of malicious node is absolutely accomplished by means of neighbor node of Route Reply (RREP) i.e. suspected node. Two counters as fvalue and rvalue are used for acting a take a look at on malicious node. these are used for counting quantity of forwarded packets and wide variety of obtain packets respectively. fvalue reaches a threshold value and rvalue is 0 then node is considered to be malicious and is discarded from the community through broadcasting INTNOT Packet.

Payal N.Raj et al [6] proposed DPRAODV (Detection, Prevention and Reactive AODV) scheme. On this paper authors proposed method DPRAODV (A dynamic learning system against black hole attack in AODV based MANET) to save you safety of black hole through informing different nodes in the community. In ordinary AODV, the node receives the RREP packet first assessments the value of sequence number in its routing table. If its sequence number is better than the one in routing table, this RREP packet is accepted. In this solution, it has an extra check carried out whether or not the RREP sequence variety is higher than the threshold value. If it is higher than the threshold value, then the node is considered to be malicious node and it provides to the black listing.

Hiremani & Jadhao et al [7] planned to detect and eliminate co-operative black hole attack and grey hole attacks by way of retaining a table known as MEDRI (Modified Extended Data Routing Information) table for each node. The fields of this table are used to detect a malicious node and preserve a records of its preceding malicious to deal with the gray hole behaviour. The MEDRI table includes the records of the preceding malicious nodes. This data is used for the future secure transformation and to find out secure path from source to destination.

Kshirsagar & Patil et al [8] proposed a way that identifies the neighbor of the RREP node author i.e. suspected node. Neighbor node is instructed to listens all the packets send through suspected node. There are two counters values are maintained by neighbor node consisting of fcount and rcount. While a neighbor node forwards any packet to suspected node it will increase the fcount counter by 1. If suspected node forward a packet it will likely be overheard by the neighbor node and rcount is increased by 1. After source node gets RREP it sends packets to route to check the node is malicious node or now not. Neighbor node forwards packets to suspect node till fcount reaches a threshold; thereafter if rcount is 0. RREP author will identify as malicious node and blocked.

Parvinder kaur et al [9] proposed a novel wormhole detection approach. The wormhole link is diagnosed by using calculating the maximum end to end delay among two nodes inside the conversation range. The proposed scheme makes use of threshold values to perceive the wormhole link without the want of any special hardware. On this scheme paths are definitely impartial. Data collection process is one time because we are calculating most distance with appreciate to communication range. This can provide us the maximum value of delay which can arise between the two nodes while forwarding the message to the destination node and while sending message lower back to the source node.

Chaube et al [10] proposed Trust Based Secure On Demand routing protocol referred to as “TSDRP” for making it relaxed to thwart black hole attack. TSDRP protocol is capable of handing over packets to the destinations even in the presence of malicious node while increasing network size.

Zahra hosseini et al [11] endorse Trust-distortion Resistant trust management scheme (TRTMS) which presents nodes with an accurate estimation on other nodes conduct and enables them to address distinctive trust-distortion attack in a multi attack environment. simulation outcomes prove that TRTMS significantly outperforms the existing alternatives within the literature in presence of simultaneous and contradictory one of a kind accept as true trust-distortion attacks.

Arya et al [12] proposed trusted AODV routing algorithm to detect and keep away from the wormhole attack and collaborative black hole attack. During the route discovery of the AODV routing protocol, the trust value is computed for all neighbours. To locate the malicious nodes, each node keeps a trust table. The trust table has two columns. First one is the identifier or name of its complete neighboring node and second is relationship status for the neighbor node. Initially when node joins the networks they are attack considered as an unreliable.

K.Geetha et al [13] proposed a method referred to as GT-IDS-DJ approach is carried out as an intrusion detection system (IDS). The cost spent closer to the safety for a defender and the price spent toward the attack technology through an attacker may be calculated. From this technique, now not most effective the SYN flooding attackers and SYN flooding attacks are recognized however additionally the nodes that intentionally introduce delay to affect the multimedia communication are also detected.

Tan & kim et al [14] proposed extraordinary threshold value for one-of-a-kind environment like small, medium and big. The threshold value is defined in a few percentage of the maximum destination sequence number. On this technique two greater functions are used. Source node use threshold value to test RREP messages from neighboring nodes. Destination node makes use of the defined threshold to confirm the RREQ messages from source node. If the destination sequence number of RREP is greater than threshold value that node is considered as malicious node.

Jian –hua tune et al [15] proposed powerful filtering approach. On this method creator proposed a brand new mechanism to save you RREQ flooding attack. This approach can hit upon the malicious nodes and attacker nodes, which are disturbing the network communication. In this technique there are thresholds RATE_LIMIT and BLACKLIST_LIMIT, which are used to restriction the RREQ message. RATE_LIMIT parameter shows number of RREQ that can be regarded and managed. Here every node monitors the RREQ and keep a count table for RREQ obtained.

Opinder singh et al [16] proposed novel trust management with elliptic curve cryptography (ECC) algorithm to become aware of the attackers. At first, a trust manager is maintained, its capabilities are to categorise the accept as true with into three unique units of trust level primarily based upon the elliptic curve cryptography and schnorr’s signature in the manet. Each consider degree has identified a single attacker. Thus, the proposed method has detected three varieties of attackers such as black hole attack, flooding attack and selective packet dropping attack. Moreover, it has furnished countermeasure for those attackers in the manet in addition to improved performances.

Geetika et al [17] proposed Trust Estimation Technique. A trust estimator is utilized in every node to estimate the consider level of its neighboring nodes. The trust level is a function of various factors like, ratio of number of packets obtained intact from the neighbor to the whole variety of received packets from that node, ratio of the range of packets forwarded efficiently through the neighbor to the entire wide variety of packets despatched to that neighbor average time taken to reply to a course request and so on. This method proposed a distributive method to recognized and prevent the flooding attack.

Sushma kushwaha et al [18] have applied Novel Intrusion Detection device in AODV routing protocol. AODV is a distance vector routing protocol. This approach can appropriately evaluate the signatures of known attacks and has a low fee of packet dropout alarms. The use of novel intrusion detection device send and acquire data, information securely and may block or restriction unknown nodes from attacks.

Sachin d. Ubrhande et al [19] proposed a distributed delegation-based scheme particularly a Secure Path Selection Scheme. The proposed scheme identifies and allows only relied on nodes to become a part of active direction. SPSS scheme to improve safety and performance of manet. The SPSS scheme establishes a secure route from source to destination in presence of attackers.

Marti et al [20] have proposed the Watchdog system to locate malicious nodes in MANET. In watchdog system nodes use promiscuous listening to method, in which, neighbor nodes promiscuously hear sender node transmission. if packet drop discovered, it increases failure counter of sender node. if failure counter exceeds threshold then sender node stated as malicious node.

Table1: Comparison of related works

S.NO	AUTHOR	METHODS	FINDINGS
1	Gupta et al	RTMAODV	Blackhole attacks
2	Payal N.Raj et al	DPRAODV	Blackhole attacks
3	Hiremani & Jadhao et al	MEDRI	Grayhole attack
4	Kshirsagar & Patil et al	RREP Creator	Malicious node
5	Parvinder Kauret al	Novel wormhole detection	Wormhole link
6	Chaube et al	TSDRP	Blackhole attack
7	Zahra Hosseini et al	Trust-distortion Resistant Trust Management Scheme (TRTMS)	Trust-Distortion attacks
8	Arya et al.	trusted AODV	Wormhole and Collaborative blackhole attack
9	K. Geetha et al	GT-IDS-DJ Method	SYN flooding
10	Tan & Kim et al	different threshold value	Malicious node
11	Jian –Hua song et al	Effective Filtering Technique	Flooding attack
12	Opinder Singh et al	novel trust management with elliptic curve cryptography (ECC)	Flooding attack, black hole attack
13	Geetika et al	Trust Estimation Technique	Flooding attack
14	Sushma Kushwaha et al	Novel intrusion detection system in AODV	Malicious node
15	Sachin D. Ubrhande et al	Secure Path Selection Scheme	Trusted node
16	Marti et al	Watchdog System	Malicious node

IV.CONCLUSION

MANET is liable to various security attacks which degrades the security and overall performance. In this paper we have mentioned the techniques and strategies for detection and prevention of malicious node, blackhole, grayhole, wormhole and synflooding attacks in manet. Blackhole attack in manet is a denial of service attack which reduces the network performances. The study here suggests different methods and techniques of various routing protocol which have been proposed and implemented to prevent and discover various types of mobile ad hoc network attacks.

REFERENCES

[1] J.H.Schiller,Mobile communications ,Pearson Education,2003

[2] Nguyen, H.L.; Nguyen, U.T.: A study of different types of attacks on multicast in mobile ad hoc networks. Ad Hoc Netw. 61,32–46(2008)

[3] Panaousis, E.A.; Politis, C.: Securing ad hoc networks in extreme emergency cases. In: Proceedings of the World Wireless Research Forum, Paris (2009).

[4]Anil Lamba1, SohanGarg2, Rajeev Kumar3, A Literature Review of MANET's Routing Protocols Along With Security Issues, 2016 IJSRSET | Volume 2 | Issue 6 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099.

[5] Anurag Gupta, Kamlesh Rana, "Assessment of Various Attacks on AODV in Malicious Environment" 2015 1st International Conference on Next Generation Computing Technologies (NGCT-2015) Dehradun, India, 4-5 September 2015.

[6] Payal N. Raj, Prashant B. Swadas" DPRAODV: A Dyanamic Learning System Against Blackhole Attack in AODV Based Manet." International Journal of Computer Science Issues, Vol. 2, 2009 ISSN (Online): 1694-0784 ISSN (Printed): 1694-0814.

[7] Vani A. Hiremani, Manisha Madhukar Jadhao, "Eliminating Co-operative Black hole and Gray hole Attacks Using Modified EDRI Table in MANET" IEEE ,2013.

[8] Durgesh Kshirsagar, Ashwini Patil, "Black hole Attack Detection and Prevention by Real Time Monitoring" Green Computing, Communication and Conservation of Energy (ICGCE), 2013 International Conference on 12-14 Dec. 2013

[9]Parvinder Kaur1. Dalveer Kaur2. Rajiv Mahajan3.Wormhole Attack Detection Technique in Mobile Ad Hoc Networks,Wireless Personal Communications November 2017, Volume 97, Issue 2, pp 2939–2950.

[10] Nirbhay Chaubey, Akshai Aggarwal, Savita Gandhi, Keyurbhai A Jani, "Performance Analysis of TSDRP and AODV Routing Protocol under Black Hole Attacks in MANETs by Varying Network Size" 2015 Fifth International Conference on Advanced Computing & Communication Technologies.

[11] Zahra Hosseini1. Zeinab Movahedi2.A Trust-Distortion Resistant Trust Management Scheme on Mobile Ad Hoc Networks. Wireless Personal Communications October 2017, Volume 96, Issue 4, pp 5167–5183

[12] Neeraj Arya, Upendra singh, Sushma singh, "Detecting and Avoiding of Worm Hole Attack and Collaborative Black hole attack on MANET using Trusted AODV Routing Algorithm" IEEE International Conference on Computer, Communication and Control (IC4-2015).

[13] K. Geetha1 . N. Sreenath2.Detection of SYN Flooding Attack in Mobile Ad hoc Networks with AODV Protocol, Arabian Journal for Science and Engineering March 2016, Volume 41, Issue 3, pp 1161–1172.

[14] Seryvuth Tan, Keecheon Kim, "Secure Route Discovery for Preventing Black Hole Attacks on AODV-based MANETs" 2013 IEEE International Conference on High Performance Computing and Communications & 2013 IEEE International Conference on Embedded and Ubiquitous Computing.

[15] Jian-Hua Song, Fan Hong and Yu Zhang, "Effective Filtering Scheme against RREQ Flooding Attack in Mobile Ad Hoc Networks", Seventh International Conference on Parallel and Distributed Computing, Applications and Technologies, pages 497-50.

[16] Opinder Singh1, Jatinder Singh. Ravinder Singh, Multi-level trust based intelligence intrusion detection system to detect the malicious nodes using elliptic curve cryptography in MANET, Cluster Computing ,pp 1–13

[17]Geetika Sharma1, Anupam Mittal2, Ruchi Aggarwal3," Attacks on Ad hoc On-Demand Distance Vector Routing in MANET International Research Journal of Engineering and Technology (IRJET) e-ISSN: Volume: 03 Issue: 06 | June-2016.

[18]Sushma Kushwaha1, Prof. Vijay Lokhande2,Security in Wireless Mobile Ad-Hoc Network Nodes Using Novel Intrusion Detection System, DOI 10.4010/2016.777,ISSN 2321 3361 © 2016 IJESC

[19] Sachin D. Ubarhande. Dharmpal D. Doye. Prakash S. Nalwade. A Secure Path Selection Scheme for Mobile Ad Hoc Network. Wireless Personal Communications, Volume 97, Issue 2, pp 2087–2096

[20] Marti, S., Giuli, T. J., Lai, K., & Baker, M. (2000). Mitigating routing misbehavior in mobile ad hoc networks. In ACM Proceedings of the 6th annual international conference on Mobile computing and networking, pp. 255–265.