iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** IV **Month of publication:** April 2018

DOI: http://doi.org/10.22214/ijraset.2018.4463

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue IV, April 2018- Available at www.ijraset.com

Attacks in Mobile Adhoc-Networks

Madhur Kumawat[1], Saif Ali[2], Dr. Bharti Sharma[3], Pavan Kumar Pande[4]
[1, 2, 3, 4] *Department of Computer Application, National Institute of Technology, Kurukshetra, India.*

Abstract*: *A MANET (Mobile Ad hoc Network) is a gathering of the mobile nodes which makes a network and communicate over a shared wireless channel without any pre-existing infrastructure and no or minimal central administration. This paper studies security issues in MANET and then discussed the most serious attack in the network layer, is Black Hole Attack. After that efforts that are available for preventing the BLACK HOLE ATTACK.
Keywords*: *Black-Hole Attack, Manet, Network Layer, Routing Protocol, Security Issues.

I. INTRODUCTION

Mobile Ad hoc Network(MANET) is a remote network with self-designing property consisting of the mobile nodes that can speak with one other over the remote mediums. Since the nodes are portable, so the network topology may change quickly and unpredictably after a period of time. For a swish info transmission, nodes ought to send and get info in an ensured manner. On the of probability that nodes lies within the transmission range then these nodes can undoubtedly transmit information, if the nodes are not in each other's range then such networks follow the concept known as multi hop data transmission, where the middle of nodes provides a route from source to goal. Different protocols are meant for routes disclosures from source to goal. With this dynamic topology new and frequent route discoveries are going to be of prime concern. Due to all the above described features of MANET, it has several applications like Disaster management, Battle field communication, personal networks etc. In MANET routing protocols are developed with an assumption to attain a trusted and collaborated environment. As such, various attacks are effortlessly created by the attackers to affect the MANET routing protocols activity. Due to the open medium in MANET of the communication channel it increases the vulnerability of protocols. AODV protocol is the popular routing protocol in Mobile Ad hoc Network (MANET). It gives several benefits as compared to others, such as dynamic, self-starting and multi-hopes routing. In this protocol it provides topology changes, loop-free, and automatically rejects the inactive routes. Unfortunately, his routing protocol is prone to several attacks [11, 12]. Among the network attacks, black hole attack is that the most serious attack in the AODV-based MANET [12]. In this attack the malicious node tells that it has the shortest path to destination as compare to the others. When source node sends the packet to this malicious node it drops all the packets. This work surveys the attacks in the AODV-based MANET, discusses the foremost severe attack among the network, i.e., the blackhole attack, and therefore reviews the efforts of preventing the blackhole attack. This review has been meted out by considering further than five articles and papers printed within the most well-liked databases, like the Google Scholar, internet of Science, IEEE Xplore, Science Direct, Springer Link and ACM Digital Library. 2 keywords, i.e., “blackhole AODV” and “blackhole AODV” were employed in searching the relevant papers and the articles among the databases. etc.

II. MANET ROUTING PROTOCOLS

Lack of the central server that makes it significantly vital to require the routing call and act as router for the swish functioning of network. Protocols facilitate nodes to find the different routes for sending the packets from supply node to the destination node. These routing protocols area unit divided into 3 classes: Proactive, Reactive and the hybrid protocols [1]. Let us in short discuss these protocols here-

A. Proactive Protocols

Proactive protocols is a Table Driven protocols, where each node maintains a particular table for the routes discoveries for each different nodes within the network. For Example- Destination Sequenced Distance Vector (DSDV) [1].

B. Reactive Protocols

Reactive Protocols square are called as on demand routing protocols, because the name counsel the protocols solely discovers routes from supply to the destination once knowledge packet is to be sent. Example- Ad-hoc on demand distance vector (AODV) [1].

C. Hybrid Protocols

Hybrid protocols are those protocols that uses two types of protocols i.e. proactive and the reactive protocol. For Example – Zone Routing Protocols (ZRP) [1].

III. COMPLICATIONS IN SECURITY OF MANET

Complication in MANET is vital worry, because it can affect the performance of networks system. Web-net facilities, intimacy, integrity or trustworthiness of the data can be accomplished by guarantee that security problems have been met. MANET has many features like it is an open medium, changing nature of its topology, absence of central observing functionality, no unmistakable barrier system. MANET is dependable on the nodes that can freely connect and disconnect to any network. There is no specified principle structure that watches constantly on nodes. Here are some weaknesses of MANET that makes it powerless or vulnerable to network attacks, these are talked about beneath [2].

A. Non Protected Perimeter

The MANET system is woundable to many kind of attacks which has no reasonable limitations or perimeters. It has the best opportunity to nodes i.e. to connect or disconnect to any web-network [5].

In network system, nodes can connect consequently if they are in radio range of network. In this scenario Lack of protected boundaries, in MANET the attack is may be floatable or changeable, denial of services, spillage of data, wrong message delivery, or changing the data performance. In this scenario there is no assurance on these attacks like control on its access, which shows about the wound-ability of MANETs threat-ability [2].

B. Self-Configured Network

MANETs does not have central management system. In MANET each node performs as router and works on data packets sending and receiving [2].

MANET performs operation with the predefined structure. The absence of central system in MANET promotes to attacks. Observance of path traffic and attacks on MANET are extremely tough and thanks should be go to non self configured network.

C. Compromise Nodes

In MANET there are many attacks that induce the access in network in order to induce the management. On the node in network system victimize to hold their pernicious movement. In MANET the mobile nodes are square measure unengaged to move, be a part of or disconnect the network in other kind of measurable quarrel of mobile nodes.[2] On the issue of mobile node's we will have many troubles on nodes to stop the various harmful activities because it perform with human action. Quality of Ad-hoc network makes it more efficient to alter its location therefore off times creating it a lot of difficult and hard to trace the malicious activity.

D. Issues on Scalability of Nodes

In older time of network system, the network establishes and connect to any opposite machine with facilitate of wires. The network scalability is outlined which don't change a lot of throughout the employment. In other words we are able to conclude the quantifiably of system network, which is outlined from the starting part of planning to network.

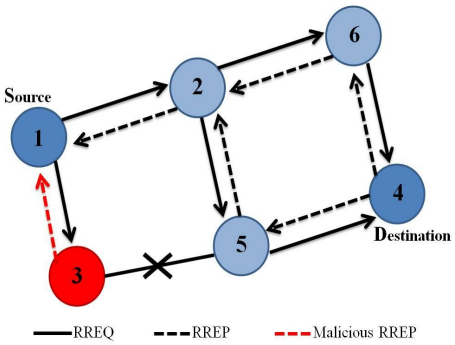
MANETs is opposite in this phenomena because the mobile nodes square measures on the basis of quality, and on MANET dynamical dimensions. The mobile nodes are square free measure for move to inside or outside the circumstantial network that is much adaptable.

IV. NETWORK LAYER ATTACKS

A. Black Hole Attack

It is very popular attack in Mobile ad hoc network (MANET). In this attack a nasty node broadcasts to all of the neighbour nodes so that it has the smallest way to the destination node without any information about its routing table. The Source node will send its data to this particular nasty node. And after getting all the data it drops all of the data and does not forwards to the destination.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue IV, April 2018- Available at www.ijraset.com



B. Wormhole Attack

The wormhole attack is occur due to the formation of a low-latency link that is formed in order that the packets will send from one end to the other faster than normally via a multi-hop route.The wormhole attack is a threat against the routing protocol and is difficult to detect and prevent. In this particular type of attack, an adversary can convince the distant nodes that are only one or two hops away through the wormhole inflicting the confusion within the network routing mechanisms.

C. Grayhole Attack

Grayhole attack is the modified form of black hole attack. In this type of attack malicious node's behavior is exceptionally unpredictable. In the black hole attack the attacker places itself in between the source node and the destination node. The attacker attracts the information packets to it by advertising itself having the shortest route to the destination and then they capture the data packet and drops it. However in grayhole attack the data packets are dropped at random or in some statistical manner. For any instance they may drop the packets from a specific node or in another pattern. A malicious node in this type of attack can behave normal at some particular period of time. So, it is very difficult to predict or to detect this type of attack in Mobile ad hoc network (MANET).

D. Byzantine Attack

The Byzantine Attack are often launched by a single or group of malicious nodes. This type of attack can be launched by creating routing loops, forwarding packets in an exceedingly long route rather than the optimal path or selectively drop packets. Byzantine attack is also responsible for the disruption or degradation of whole network. Attacks wherever the adversary has full control of an authenticated device and can be perform arbitrary behaviour to disrupt the whole system.

E. Sybil Attack

Sybil Attack occurs when an attacker uses a malicious device for creating a large range of entities so as to gain the influence within the network traffic. The ID of these malicious nodes can be the result due to the fake network additions or duplication of the existing legitimate identities. The Sybil attack sometimes targets the fault tolerant schemes including the distributed storage, topology maintenance, and the multi-hop routing.

F. Flooding Attack

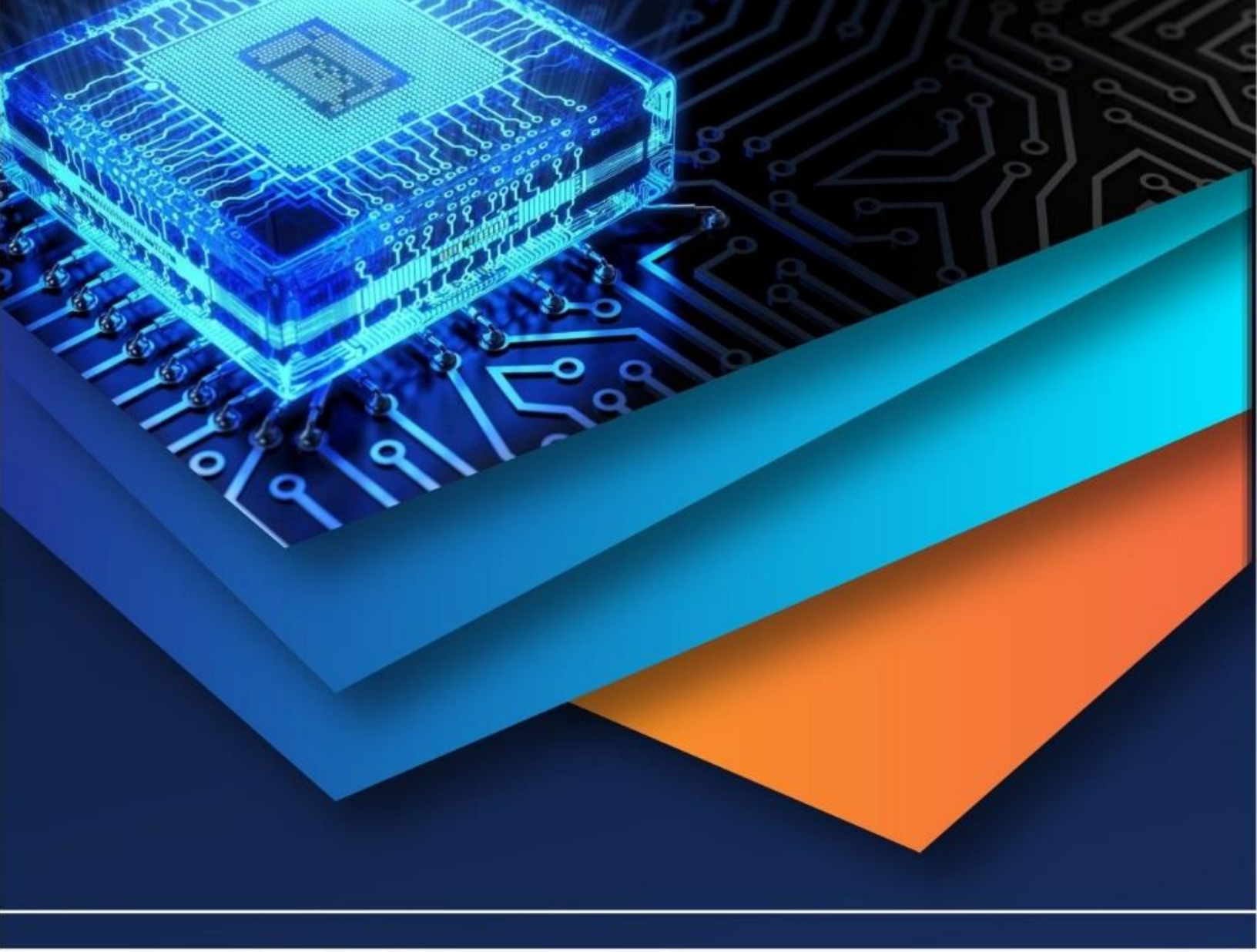
The flooding attack is easy to implement however cause mostly damage. This type of attack can be achieved either by using the RREQ or the Data flooding technique. In the RREQ flooding attacker floods the RREQ within the whole network which takes a lots of network resources. This can be achieved by attacker node by choosing such I.P addresses that do not exist within the network. By doing this, no node is in a position to answer RREP packets to those flooded RREQ. In the data flooding attacker get into the network and set up methods between all the nodes within the network. Once the paths are established the attacker injects a huge amount of useless data packets into the network which is directed to all other nodes in the network. These huge unwanted data packets within the network choke off the network. Any node that serves as the destination node are going to be busy all the time by receiving the useless and unwanted data all the time. The aim of the flooding attack is to exhaust the network resources: bandwidth and to consume a node's resources, such as battery power and computational or for the disruption of the routing operation to cause severe degradation in the network.

V. CONCLUSIONS

Due to pervasive computing it is the need of moving nodes for self-configure these topology [MANET]. However Mobile ad hoc network (MANET) is vulnerable to attack. Here we survey various types of attacks that could be possible on MANET.

REFERENCES

[1] Vishnu Sharma, Akansha Vij, "Security issues in mobile adhoc network: A Survey Paper", "International Conference on Computing, Communication and Automation(ICCCA)", 2016.
[2] Pooja Jaiswal, Dr. Rakesh Kumar, "Prevention of Black hole Attack in Manet", "International Journal of computing networks and wireless communication(IJCNWC)", ISSN:2250-3501 Vol.2.No.5 october 2012.
[3] Fan-Hsun Tseng1, Li-Der Chou1 and Han-Chieh Chal "A survey of black hole attacks in wireless mobile ad hoc networks", Tseng et al. Human-centric Computing and Information Sciences 2011,
[4] Saritha Reddy Venna, RameshBabu Inampudi, "A Survey on Security Attacks in Mobile Ad Hoc Networks", "International Journal of Computer Science and Information Technologies (IJCSIT)", 2016
[5] Sachin Lalar, "International Journal of Multidisciplinary and Current Research", "Security in MANET: Vulnerabilities, Attacks & Solutions", 2014
[6] Priyanka Goyal, Sahil Batra, Ajit Singh, "A Literature Review of Security Attack in Mobile Ad-hoc Networks", "International Journal of Computer Applications" November 2010
[7] Y. Hu, A. Perrig, D. Johnson (March 2003), Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks. Proceedings of The 22nd Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2003).
[8] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, A. Jamalipour. A survey of routing attacks in mobile ad hoc networks. Security in wireless mobile ad hoc and sensor networks, October 2007.
[9] CH.V. Raghavendran, G. Naga Satish, P. Suresh Varma, " Security Challenges and Attacks in Mobile Ad Hoc Networks" **"**I.J. Information Engineering and Electronic Business" 2013.
[10] Dr. Nabeel Zanoon1, Dr. Nashat Albdour2, Dr. Hatem S. A. Hamatta1, and Rasha Moh'd Al-Tarawneh1, "SECURITY CHALLENGES AS A FACTOR AFFECTING THE SECURITY OF MANET: ATTACKS, AND SECURITY SOLUTIONS", International Journal of Network Security & Its Applications (IJNSA), May 2015.
[11] "A REVIEW: TRUST, ATTACKS AND SECURITY CHALLENGES IN MANET", Informatics Engineering, an International Journal (IEIJ), September 2015
[12] Priya Manwani, Deepty Dubey, Hybrid Protocol for Security Peril Black Hole Attack in MANET International Journal of Computer Engineering In Research Trends(IJCERT), March-2016.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY