International Journal of Engineering Research-Online
A Peer Reviewed International Journal
Articles available online http://www.ijoer.in

Vol.3., Issue.6., 2015
(Nov.-Dec.,)

REVIEW ARTICLE

ISSN: 2321-7758

MANET & ITS BLACKHOLE ATTACK: REVIEW

SWATI[1], HARJIT SINGH[2]

[1]Dept. of Communication System, Guru Nanak Dev University-RC, Gurdaspur, Punjab, India
[2]Dept. of ECE, Guru Nanak Dev University-RC, Gurdaspur, Punjab, India

SWATI

ABSTRACT

Mobile Ad Hoc Networks comprises of wireless mobile nodes that synchronize wit other to create a provisional network devoid of its pre-existing infrastructure. It is governing system which consists of wireless mobile hosts devoid of any fixed infrastruc network and integrated access point for instance a base station. Due to absence of defined central authority, Mobile Ad Hoc Networks are quite defenceless to various att its security and therefore security is vital requirement in Mobile Ad Hoc Networks contrary to the wired network. AODV is widespread and most-used Ad-hoc distance routing reactive protocol that is utilized to discover shortest and exact route destination. In this paper, we have make an effort to exemplify an outline of AODV protocol, the probable security attacks which might occur on Mobile Ad Hoc Networks our main focus is on black hole attack in AODV using Mobile Ad Hoc Networks.

Keywords: MANET, ADOV, Security, attacks, Black hole.

INTRODUCTION

Mobile Ad Hoc Networks is a self-constructing network of wireless moveable nodes which construct network which have capability of topology changing dynamically. Every single node in the specific network acts as a kind of router, forwarding the data packages to other additional nodes [1]. Mobile Ad Hoc Network have several impending applications for example relief operations in disaster, military services specifically in battlefield, as well as in business/commercial environments.

Every specific device in a Mobile Ad Hoc Network is permitted to travel individually in any sort of direction, and this will consequently alter its connections to other devices recurrently [2]. Every node must frontward traffic which is unrelated towards its own utilization, and consequently be as a router. Such type of networks might probably function by themselves or it might be associated towards the bigger Internet. The features of MANETs for instance: node mobility, dynamic topology, it also offers huge number of degree of independence along with self-establishing ability which make it entirely dissimilar from other additional network. It is utilized in applications for instance disaster recovery, device network, automated battlefields, virtual classroom, law enforcement, sensor networks, search and rescue, public meeting, emergency relief scenarios, data network, and other additional security sensitive computing environment [3].

The main challenges and characteristics of the Mobile Ad Hoc Networks could be categorized as follows:

1) Co-operation: Mobile Ad Hoc Networks depend on the co-operation of the mobile nodes for packet transmission and routing. In any condition, the destination node and source node are not in the

group with each other as compared to the communication amongst them takes place by the co-operation of other additional nodes.

2) Topology Dynamism: The Mobile Ad Hoc Network nodes are changeable and arbitrary and so as the topology. The nodes might possibly join or leave the specific network at any specific time. And the topology is susceptible to failure of connection; all these would impact the position of trust amongst several nodes and the intricacy of routing.

3) Absence of fixed infrastructure: The lack of a central or else fixed infrastructure is a significant characteristic of Mobile Ad Hoc Networks. As a result of this lack of authority, old-style methods of security and network management are barely pertinent to MANETs.

4) Resource constraints: Mobile Ad Hoc Network are a group of mobile devices that are of limited or low capacity of power, memory, computational capacity, bandwidth etc. by default. In order to attain a secure and consistent communication amongst nodes, these constraints of resource make the task much more enduring.

Routing in mobile ad-hoc network is quite intricate because of its dynamic changing topology and mobility of nodes as matched to old-style wired networks [4]. Limited battery and bandwidth makes routing more challenging in mobile ad-hoc network. Because of these important features of MANET, it is vulnerable to several sorts of attacks such as spoofing of control or data packages, malicious modification of the contents of package, eavesdropping with malicious intent, and DoS attack such as blackhole, wormhole, sinkhole, gray hole attacks etc. [5]. All of them are network layer attacks. Thus, routing security is the key problem for which investigators desire to work for discovering its solution. Here, Routing protocol plays an important character in network security. Adhoc On-demand Distance Vector is protocol for routing utilized as well as intended for mobile ad-hoc network to create route on request/demand. It does not required to sustain routes that are not dynamic/active.

OVERVIEW OF AODV PROTOCOL

It is a reactive type of routing protocol, but then again it is fundamentally a development of DSDV routing protocol i.e. also a type of proactive routing protocol. This routing protocol initiates route discovery process routes only when there is any requirement to discover specific node [3]. It could controls all type of low, moderate, as well as comparatively higher mobile rates, composed with a range of data-traffic loadings. Nevertheless, it does not make any kind of provisions intended for security [6]. In the process of Route Discovery in Adhoc On-demand Distance Vector routing protocol, there are categories of messages such as:

- Route Request (RREQ),
- Route Reply (RREP), and
- Route Error (RERR) messages.

A specific source node transmits a Route request message through route discovery process on every occasion it desires to communicate in the direction of destination node but then again it does not have a new route to communicate. All kind of intermediate nodes which might obtain this Route Request message or either direct a Route Reply in the direction of the source node or forward the route request message to the other additional nodes. Route Reply message is directed/sent only in the circumstance if intermediate nodes have a new route towards the direction of destination node and the flag of "destination only" is not set. If in any condition, the request package has been further advanced by this specific intermediate node earlier, then it is released silently. Once, the actual destination node obtains a Route Request for itself, it directs back a route reply message on the back route towards the source. The requesting node and the nodes which are receiving Route Reply messages on the route to upgrade their routing tables with the some fresh route. A particular route produces a Request Error message either a route breakdowns or it doesn't have a specific route towards the destination towards which the data package is to be sent.

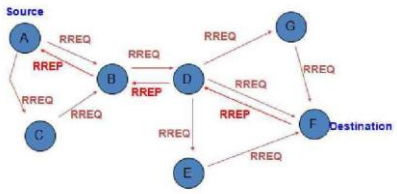

Fig: 1. Example of AODV Routing Protocol

SECURITY THREATS IN AODV

AODV routing protocol has no or less security arrangements, so the malicious nodes can perform many attacks. A node is compromised if a node behaves maliciously. It usually occurs when a genuine node acts malevolently but then again the network could not acknowledge it [8].The forms of malicious activity reliant upon the working of the specific protocols. The attacks could be categorized as active or passive type attacks [7].

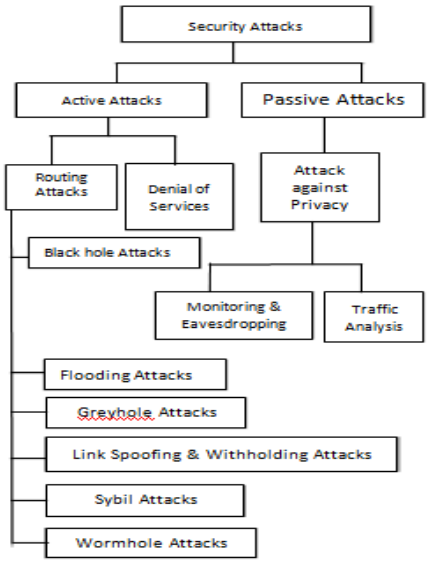

Fig: 2. Types of Attacks

1) Passive attacks: In passive attack, an illegal node uninterruptedly monitors specific network and agreeable to acquire the data [9]. During this attack, communications is not interrupted. And also no direct destruction occurs towards the network. For instances:

- ***Eavesdropping Attacks:*** This is also acknowledged as dis-closure attack. The invader collects data for instance public or private key or even passwords of the network mobile nodes and it also examines transmission messages in the direction of disclosing some beneficial data regarding the network.
- ***Traffic Analysis:*** In this type of attack, the network traffic along with it's messages are scrutinized to discover information. It could possibly be implemented on specifically encrypted messages. In this the attackers utilize methods for instance monitoring time correlation and traffic rate analysis, etc.

2) Active Attacks

Active attacks will reason for unapproved state changes in the specific network like modification of data packages, DoS, and so on. These type of attacks are commonly propelled by nodes or clients with consent to function inside the specific network [9]. These attacks could be categorized into a number of groups as given below:

- ***Dropping Attacks:*** This attack is a sort of DoS attack and it is one of the most challenging one to prevent and perceive. Malicious nodes leave all data packages which are not predestined for them. Meanwhile, some malevolent nodes which has intention to interrupt network connections, as well as to reserve their assets. If in any condition, dropping node is at a critical point, these attacks could prevent end-to-end communications amongst several nodes.
- ***Modification Attacks:*** Insider invaders afterwards reading the information in the package, amend it to interrupt the specific network. For instance modifying the value of hop-count of a routing package towards a lesser value. By diminishing the value of hop-count of a malevolent node could possibly entice additional network communication.
- ***Black Hole Attack:*** This attack is a type of DoS attack. In this attack, the malicious node transfers fabricated route replies in the direction of the source node requesting towards having the shortest path towards the destination node [10]. As soon as the source node create the route from the malevolent node, the malevolent node then discards or mis-utilize all or any specific sort of the network traffic being transmitted through it.

- ***Grey Hole attack:*** This is a special sort of black hole attack. In this the attacking node initially decides to front forward data packages and later it fails to do this. In this attack, selected data packages are left [11].

In AODV black hole attack the malevolent node "P" initially discover the active route present in between the specific sender "T" and destination node "S". The malevolent node "P" then send the route reply that

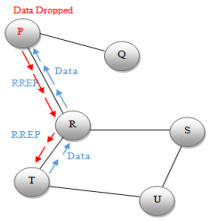

Fig: 3. Blackhole attack

Contains the address of spoofed destination as well as including small hop count and large sequence number than normal towards node "R". This node "R" directs this RREP to the specific sender node "T". Now this specific route is utilized by the sender to send the data and in this way data will arrive at the malicious node [11]. These data will then be dropped. In this way sender and destination node will be in no position any more to communicate in state of black hole attack. Wormhole attack: In this type of attack, an aggressor records data packages at one specific location in the network and then channels them towards another additional location. Routing could be interrupted as soon as the routing control messages are channeled. This passageway amongst two conspiring attackers is mentioned as a wormhole attack. These attacks are severe threats towards routing protocols in Mobile ad-hoc network.

COUNTERMEASURES AGAINST AODV

Lots of studies have been completed to deliver security on Adhoc on Demand Vector routing protocols against several threats. One of the utmost severe threats is Black hole Attack. Several solutions have been recommended for prevention along with detection from black-hole attacks in Adhoc on Demand Vector routing protocols. Some of them are given as follows:

Sanjay Ramaswamy et al. [10] suggested a solution for co-operative black-hole attacks by marginally modified Ad-hoc on Demand Vector Routing Protocol by means of presenting Cross Checking and Data Routing Information Table. This algorithm is dependent on a trust relationship between the nodes.

Vishnu K et al. [11] Deliberated a Backbone Network that is dependent upon choosing some powerful as well as trustworthy nodes in terms of range and battery power. These nodes that are denoted as Back Bone Nodes which would form a Back Bone network and also have distinct functions nothing like normal nodes. This technique identifies gray hole attack as well as black hole attack in Adhoc On Demand Vector routing protocol.

Deng et. al. [12] has anticipated a technique to avert black hole attacks in mobile ad-hoc networks. According to this technique, any specific node on getting a route reply data package, double-checks with the subsequent hop on the specific route towards the destination commencing an alternate path. If the subsequent hop either does not have a connection to the specific node which directed the route reply or does not have a specific route towards the destination then the node which has directed the RREP is deliberated as malevolent. This result could not avoid accommodating black hole attacks. Other than this technique there are several techniques that are utilized for the security of Adhoc on Demand Vector Routing Protocol.

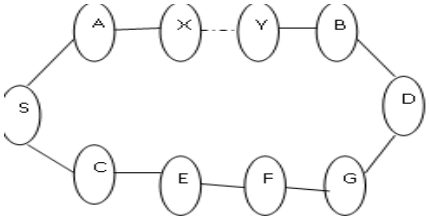

Fig: 4. Wormhole attack

3) Other Attacks

- ***Impersonation Attack:*** These are also known as spoofing attacks. The attacker assumes the identity of another node in the network, thus receiving messages directed to the node it fakes [12]. The attacker nodes impersonates a legitimate node and joins the network undetectable, sends

false routing information, masked as some other trusted node.

- ***Timing Attacks:*** In this an attacker entices other additional nodes via affecting itself to appear closer to those additional nodes than it actually is. This technique has been used by DoS attacks, rushing attacks, and hello flood attacks.
- ***Routing Table Poisoning Attack:*** Several dissimilar routing protocols uphold/maintain tables that hold data about several routes of the specific network. In poisoning type attacks, the invader node produces and directs fabricated traffic, or transforms genuine messages from other additional nodes, so as to generate false type entries in the tables of the contributing nodes. Additional possibility is to introduce a route request package with a high sequence number. This reasons for all additional legitimate route request packages having lower sequence numbers are to be removed. These attacks could result in selection of specific non-optimal routes, bottlenecks, formation of routing loops, and even segregating definite portions of the network.
- ***Location Disclosure Attack:*** In this attack, the privacy necessities of an ad-hoc network are bargained [4]. By the utilization of traffic analysis methods or by using modest monitoring and analytical methodologies an invader is capable to find out the position of a specific node, and the arrangement of the specific network.
- ***Rushing Attack:*** In this attack the invader (initiator) node inductees a Route Discovery for the destination node. If every single neighbor of the destination node obtains these route request messages initially, then afterwards the route is revealed by this specific process of route discovery which will embrace a hop through the assailant. Then the neighbor forwards that particular REQUEST towards the destination node. As soon as non-attacking type REQUESTs reached at these specific nodes, then they will probably abandon those genuine REQUESTs. As an outcome of which the initiator will perhaps be incapable to determine any working routes, those routes which does not embrace the invader holding at least 2 hops.

CONCLUSION & FUTURE SCOPE

There are a several types of security dangers in MANET against AODV routing protocol. It is a quite stimulating job as the nodes present in mobile adhoc networks are mostly self-organized and mobile. To design such method that will help in preventing the Adhoc on Demand Vector routing protocol from all types of threats is quite challenging. Even though, numerous researchers have operated through the safekeeping of Adhoc On Demand Vector however the area of investigation in this is yet open. Several techniques have been deliberated in the direction of providing security in Adhoc on Demand Vector against some specific attacks such as blackhole attack. Not all the attacks could be prohibited by utilizing a solitary method. So a combination of number of techniques had better be utilized to completely secure the Adhoc on Demand Vector Routing Protocol. In this paper we have described some of the possible attacks on AODV but the main focus of this review paper is on blackhole attack which is one of the big security threats in the network. Future scope of this paper lies in the work done on discovering and preventing blackhole attack on Adhoc on Demand Vector routing protocol in MANET.

REFERENCES

[1] Palanisamy, P.Annadurai, "Impact Of Rushing Attack On Multicast In Mobile Ad Hoc Network", (IJCSIS) International Journal Of Computer Science And Information Security, Vol. 4, No. 1 & 2, 2009

[2] G.Vijaya Kumar, Y.Vasudeva Reddyr, Dr.M.Nagendra, "Current Research Work on Routing Protocols for Manet: A Literature Survey", (IJCSE) International Journal on Computer Science and Engineering Vol. 02, No. 03, 2010, 706-713

[3] "Rutvij H.Jhaveri, Ashish D. Patel, Jatin D. Parmar, Bhavin I. Shah, "Manet Routing Protocol and Wormhole Attack against AODV", IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.4, April 2010.

[4] Karlsson, Jonny; Dooley, Laurence S. and Pulkkis, Goran, "Routing Security in Mobile Ad-hoc Networks". Informing Science and Information Technology Education 2012 Conference (InSITE'12), 22-27 June 2012, Montreal, Canada (Forthcoming), 2012.

[5] Ashwani Garg, Vikas Beniwal, "A Review on Security Issues of Routing Protocols in Mobile Ad-Hoc Networks", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 9, pp.145-148, September-2012.

[6] Preeti Bathla, 2Bhawna Gupta, "Security Enhancements in AODV Routing Protocol", IJCST Vol. 2, Issue 2, June 2011.

[7] Adnan Nadeem and Michael Howarth, "Protection of MANETs from a range of attacks using an intrusion detection & prevention system", Springer.

[8] Praveen Kumar, Jatin Sharma,Kriti Saini, "A survey on AODV routing protocol for Ad-hoc network", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue 3, March 2013.

[9] K. Sivakumar, Dr. G. Selvaraj, "Overview Of Various Attacks In MANET And Countermeasures For Attacks", Vol 2, Issue 1, Issn 2278-733x, January 2013.

[10] Sanjay Ramaswamy; Huirong Fu; Manohar Sreekantaradhya; John Dixon; and Kendall Nygard (2003). Prevention of cooperative blackhole attack in wireless Ad hoc networks. In Proceedings of 2003 International Conference on Wireless Networks, (ICWN'03), Las Vegas, Nevada, USA, pp. 570-575.

[11] Vishnu K and Amos J Paul, "Detection and Removal of Cooperative Black/Gray hole Attack in Mobile Adhoc Networks", International Journal of Computer Applications (0975 - 8887) Volume 1 – No. 22, 2010.

[12] Hongmei Deng, Wei Li, and Dharma P. Agrawal, "Routing Security in Wireless Ad Hoc Network", IEEE Communications Magzine, vol.40, pp. 70-75, 2002.

ABOUT AUTHOR

Swati is pursuing her Master's degree in "Wireless Communications" from Guru Nanak Dev University RC, Gurdaspur, Punjab. She received B.Tech degree in Electronics & Communication Engineering in 2014 from RIET, Phagwara. Her area of interest includes Environmental Sustainability in Wireless Communication Networks, Mobile Communications System. She is currently working on a project titled "Blackhole Attacks and its Reduction Techniques in MANET".