Network Security against Black Hole Attack using Trust Management for MANET Environment

*** Jaya Kushwah**
**** Deepika Jain**
***** Dr. Harish Patidar**

ABSTRACT

Wireless networks are picking up prominence to its crest today, as the users need wireless network regardless of their geographic position. There is an expanding danger of attacks on the Mobile Ad-hoc Networks (MANET). Black hole attack is one of the security risk in which the movement is diverted to such a node, to the point that really does not exist in the system. It's a similarity to the black hole in the universe in which things vanish. The extent of this proposal is to think about the impacts of Black hole attack in MANET utilizing Proactive routing protocol i.e. Specially ad-hoc On Demand Distance Vector (AODV) and Trust construct Ad-Hoc on Demand Distance Vector (AODV). Near investigation of Black Hole attack for protocol is considered. The effect of Black Hole attack on the execution of MANET is assessed discovering which protocol is more defenseless against the attack and what amount is the effect of the attack on protocol. The estimations were taken in the light of parcel Packet Delivery Ratio, throughput, end-to-end delay and Residual Energy. Simulation is done in Network simulator 2 (NS-2.35).

Keywords: MANET, AODV, Black Hole, Routing Protocols, Trust Management and NS-2.35.

* Jaya Kushwah, Research Scholar, LNCT, Indore, jiyakushwah0@gmail.com
** Deepika Jain, Assistant Professor (CSE), LNCT, Indore, Deepikajainbpl@rediffmail.com
*** Dr. Harish Patidar, HOD (CSE), LNCT, Indore, Harish.cs@lnctindore.com

I. INTRODUCTION:

Mobile Ad-hoc NETWORK (MANET) is a self-arranging system of mobile nodes associated by wireless connections and considered as network without foundation. Routing protocol assumes a significant part for viable correspondence between mobile nodes and works on the fundamental supposition that nodes are completely agreeable. Research in wireless demonstrates that the wireless MANET shows a bigger security issue than customary wired and remote systems. There are numerous routing attacks caused because of absence of security. The routing attack that will be tended to is the black hole attack. In Black hole attack a malicious node publicizes itself as it is having the briefest way to the goal. In MANETs, the nodes are allowed to move haphazardly and arrange themselves arbitrarily. In MANET, system's remote topology may change quickly and capriciously. MANETs are typically setup in circumstances of crisis for impermanent tasks. These kinds of systems work without any settled foundation, which makes them simple to setup. [1].

Ad hoc On-Demand Distance Vector (AODV) is a standout amongst the most well-known ad-hoc routing protocols utilized for mobile ad-hoc networks. AODV is an on-request routing protocol that finds a route just when there is a request of information exchange exist for mobile nodes. In AODV routing protocol, a mobile node that desires to speak with other node first communicates a RREQ (Route Request) message to locate a crisp course to a coveted target mobile node. In the event that a mobile node find a sufficiently new route, it uncast a RREP (Route Reply) message back along the spared way to the source mobile node or it generally re-communicates the RREQ message in Ad-Hoc arrange.

A malicious node in the system accepting a RREQ message answers to source node by sending a false RREP message that contains attractive parameters to be decided for packet delivery to receiver node. In the wake of promising (by sending a wrong RREP to affirm it has a way to a receiver node) to source nodes that has genuine way to forward information, a malicious node begins to lose all the network traffic it gets from source node.

Security in Mobile Ad-Hoc Network (MANET) is the most important concern for the basic functionality of network. Availability of network services, confidentiality and integrity of the data can be achieved by assuring that security issues have been met. MANET often suffer from security attacks because of its features like open medium, changing its topology dynamically, lack of central monitoring and management, cooperative algorithms and no clear defense mechanism. These factors have changed the battle field situation for the MANET against the security threats.

In the last few years, security of computer networks has been of serious concern which has widely been discussed and formulized. Most of the discussions involved only static and networking based on wired systems. However, mobile Ad-Hoc networking is still in need of further discussions and development in terms of security [21]. With the emergence of ongoing and new approaches for networking, new problems and issues arises for the basics of routing. With the comparison of wired network Mobile Ad-Hoc network is different. The routing protocols designed majorly for internet is different from the mobile Ad-Hoc networks (MANET). Traditional routing table was basically made for the hosts which are connected wired to a non dynamic backbone [22]. Due to which it is not possible to support Ad-Hoc networks mainly due to the movement and dynamic topology of networks.

Due to various factors including lack of infrastructure, absence of already established trust relationship in between the different nodes and dynamic topology, the routing protocols are vulnerable to various attacks [23].

II. PROBLEM STATEMENT

In this work we concentrate to one unique active attack called black hole attack. In black hole attack the router will promote in the system that it has a new route to the goal and after that may drop every one of the packets that it gets. Here, Intermediate nodes can prompt conflicting , If the source succession number is old and transitional node have esteem higher than a source node then malicious node exploit this high arrangement number and sending counterfeit Route answer to the source without having real route and drops all the accepting packets. It gives genuine the harm. In black-hole attack, a particular malicious node which does not exist in the system diverted all network traffics. Since traffics vanish into the extraordinary node LIKE the issue vanishes into Black hole in universe.

III. NETWORK SECURITY IN MANET

Major vulnerabilities which have been so far researched are mostly these types which include selfishness, dynamic nature, and severe resource restriction and also open network medium. Despite of the above said protocols in MANET, there are attacks which can be categorized in Passive, Active, Internal, External and network-layer attacks, Routing attacks and Packet forwarding attacks.

MANET work without a centralized administration where node communicates with each other on the base of mutual trust. This characteristic makes MANET more vulnerable to be exploited by an attacker from inside the network. Wireless links also makes the MANET more susceptible to attacks which make it easier for the attacker to go inside the network and get access to the ongoing communication [9, 21]. Mobile nodes present within the range of wireless link can overhear and even participate in the network.

a. Flaws in MANETS

MANETs are very flexible for the nodes i.e. nodes can freely join and leave the network. There is no main body that keeps watching on the nodes entering and leaving the network. All these weaknesses of MANETs make it vulnerable to attacks and these are discussed below.

b. Non Secure Boundaries:

MANET is vulnerable to different kind of attacks due to no clear secure boundary. The nature of MANET, nodes have the freedom to join and leave inside the network. Node can join a network automatically if the network is in the radio range of the node, thus it can communicate with other nodes in the network. Due to no secure boundaries, MANET is more susceptible to attacks. The attacks may be passive or active, leakage of information, false message reply, denial of service or

changing the data integrity. The links are compromised and are open to various link attacks. Attacks on the link interfere between the nodes and then invading the link, destroying the link after performing malicious behavior.

There is no protection against attacks like firewalls or access control, which result the vulnerability of MANET to attacks. Spoofing of node's identity, data tempering, confidential information leakage and impersonating node are the results of such attacks when security is compromised [10].

c. Compromised Node:

Some of the attacks are to get access inside the network in order to get control over the node in the network using unfair means to carry out their malicious activities. Mobile nodes in MANET are free to move, join or leave the network in other words the mobile nodes are autonomous [11]. Due to this autonomous factor for mobile nodes it is very difficult for the nodes to prevent malicious activity it is communicating with. Ad-hoc network mobility makes it easier for a compromised node to change its position so frequently making it more difficult and troublesome to track the malicious activity. It can be seen that these threats from compromised nodes inside the network is more dangerous than attacking threats from outside the network.

d. No Central Management:

MANET is a self-configurable network, which consists of Mobile nodes where the communication among these mobile nodes is done without a central control. Each and every node act as router and can forward and receive packets [12]. MANET works without any preexisting infrastructure. This lack of centralized management leads MANET more vulnerable to attacks. Detecting attacks and monitoring the traffic in highly dynamic and for large scale Ad-Hoc network is very difficult due to no central management. When there is a central entity taking care of the network by applying proper security, authentication which node can join and which can't. The node connect which each other on the basis of blind mutual trust on each other, a central entity can manage this by applying a filter on the nodes to find out the suspicious one, and let the other nodes know which node is suspicious.

e. Problem of Scalability:

In traditional networks, where the network is built and each machine is connected to the other machine with help of wire. The network topology and the scale of the network, while designing it

is defined and it do not change much during its life. In other words we can say that the scalability of the network is defined in the beginning phase of the designing of the network. The case is quite opposite in MANETs because the nodes are mobile and due to their mobility in MANETs, the scale of the MANETs is changing. It is too hard to know and predict the numbers of nodes in the MANETs in the future. The nodes are free to move in and out of the Ad-Hoc network which makes the Ad-Hoc network very much scalable and shrinkable. Keeping this property of the MANET, the protocols and all the services that a MANET provides must be adaptable to such changes.

IV. BLACK HOLE ATTACK IN AODV

Two types of black hole attack can be described in AODV in order to distinguish the kind of black hole attack.

a. Internal Black hole attack

This type of black hole attack has an internal malicious node which fits in between the routes of given source and destination. As soon as it gets the chance this malicious node make itself an active data route element. At this stage it is now capable of conducting attack with the start of data transmission. This is an internal attack because node itself belongs to the data route. Internal attack is more vulnerable to defend against because of difficulty in detecting the internal misbehaving node.

b. External Black hole attack

External attacks physically stay outside of the network and deny access to network traffic or creating congestion in network or by disrupting the entire network. External attack can become a kind of internal attack when it take control of internal malicious node and control it to attack other nodes in MANET. External black hole attack can be summarized in following points

1. Malicious node detects the active route and notes the destination address.
2. Malicious node sends a route reply packet (RREP) including the destination address field spoofed to an unknown destination address. Hop count value is set to lowest values and the sequence number is set to the highest value.
3. Malicious node send RREP to the nearest available node which belongs to the active route. This can also be send directly to the data source node if route is available.
4. The RREP received by the nearest available node to the malicious node will relayed via the established inverse route to the data of source node.

5. The new information received in the route reply will allow the source node to update its routing table.

6. New route selected by source node for selecting data.

7. The malicious node will drop now all the data to which it belong in the route.

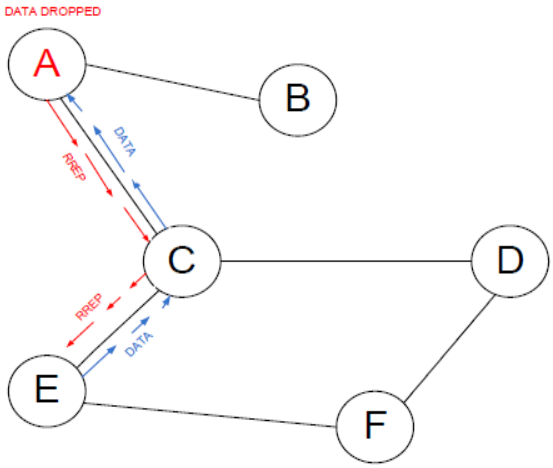

Figure 1: Black hole attack specification

In AODV black hole attack the malicious node "A" first detect the active route in between the sender "E" and destination node "D". The malicious node "A" then send the RREP which contains the spoofed destination address including small hop count and large sequence number than normal to node "C". This node "C" forwards this RREP to the sender node "E". Now this route is used by the sender to send the data and in this way data will arrive at the malicious node. 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.

V. IMPLEMENTATION AND RESULT

To assess the execution of a protocol for an ad-hoc network, it is important to investigate it under functional condition. We have actualized our pragmatic work in a ns2 test system. The issue is researched by methods for gathering information, examinations and reenactment which gives a few outcomes, these outcomes are investigated and choices are made on their premise. Utilizing ns2, we can actualize our new protocol and contrast its execution with ordinary AODV.

We have executed work i.e. Creation MANET Scenario in NS-2 and afterward to make AODV routing protocol with the utilization of various execution grids Like Packet Delivery Ratio, End to End delay, Residual Energy and Overall Throughput.

In this work right off the bat we have computed the consequence of basic AODV Protocol utilizing NS2 then we have made the situation of AODV protocol with Black hole attack and figure the outcome and do examination of aftereffects of both with or without attack AODV protocol scenario. Presently again made AODV protocol with Black Hole Attack utilizing our proposed methodology and figure the Result .In this MANET scenario or topology for this situation it comprises of with Normalized AODV, AODV under black hole attack, and TAODV under black hole attack and dynamic node with 300sec simulation time.

For this work to be done effectively we have utilized MANET situation with Normalized AODV , AODV under black hole attack, TAODV under black hole attack. The recreation situation and parameters utilized for playing out the definite investigation of Black hole attacks on MANET routing protocol is mentioned. We have come to the outcomes with the assistance of different execution frameworks for the time being we have utilized after execution grids.

Packet Delivery Ratio: The ratio between the number of packets originated by the "application layer" CBR sources and the number of packets received by the CBR sink at the final destination. This evaluates the ability of the protocol to discover routes.

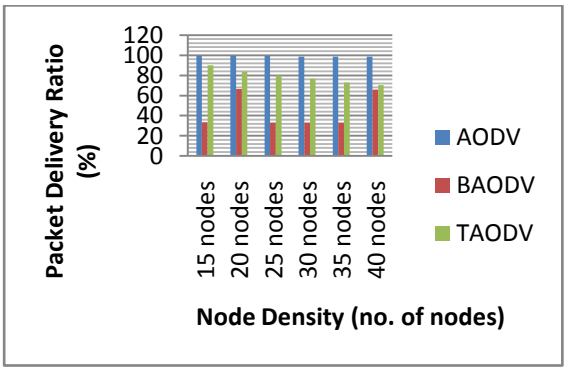

Figure 2: Packet Delivery Ratio comparisons for AODV, BAODV and TAODV

Throughput: The average rate at which the data packet is delivered successfully from one node to another over a communication network is known as throughput. The throughput is usually measured in bits per second (bits/sec). A throughput with a higher value is more often an absolute choice in every network.

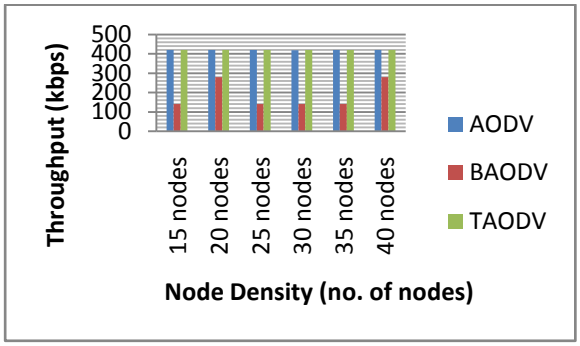

Figure 3: Throughput Comparison for AODV, BAODV, TAODV

End to end Delay: The End-to-End delay is the time needed to traverse from the source node to the destination node in a network. The end-to-end delay is measured in second. The delay assesses the ability of the routing protocols in terms of use- efficiency of the network resources. Less end 2 end Delay ensure the better performance in the network.

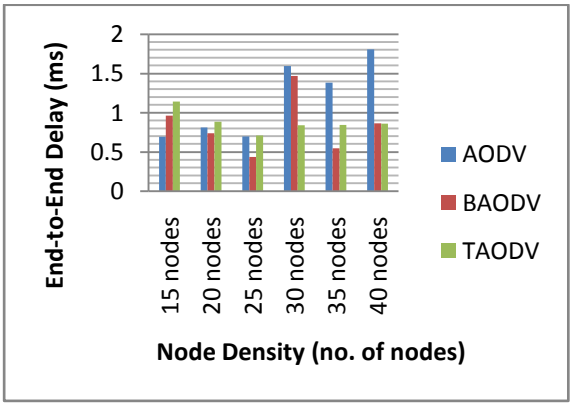

Figure 4: End-to-End Delay Comparison for AODV, BAODV and TAODV

Residual Energy: It is the total amount of energy Consumed by the Nodes during the completion of Communication or simulation. If a node is having 100% energy initially and having 70% energy after the simulation than the energy consumption by that node is 30%.The unit of it will be in Joules.

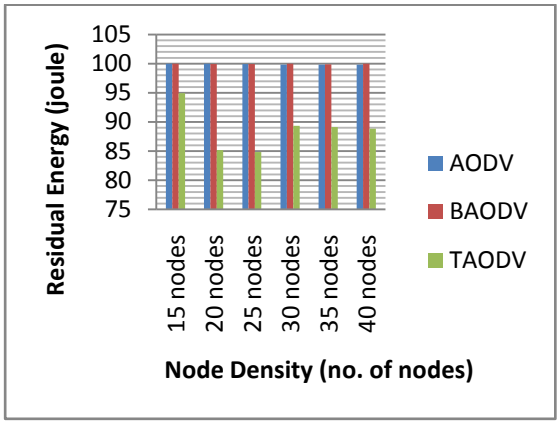

Figure 5: Residual Energy Comparison for AODV, BAODV and TAODV Routing protocol

VI. CONCLUSION

MANET can send a system where a customary system framework condition can't in any way, shape or form be conveyed. Security of MANET is one of the imperative highlights for its organization, the identification and counteractive action of black hole attack in the system exists as a testing errand. In this work we investigated the impact of black hole attack in the execution of AODV protocol and keep the system from black hole attack utilizing TAODV convention. The reproduction has been finished utilizing the system test system (NS-2.35). The performance metrics like packet delivery ratio, throughput and normal end to end delay has been estimated and dissected with the static node thickness. From the reenactment comes about plainly when the black hole node exists in the system, it can be affected and diminished the execution of AODV routing protocol. In this work, we reenacted AODV protocol with various density, i.e. 20 nodes, 40 nodes, 60 nodes and furthermore same similar situations subsequent to bringing single black Hole Node into the network. Besides, we simulated Secure AODV according to calculation for identification of black hole attack. At last compare the outcomes of arrangement and typical AODV under attack by shifting distinctive network parameters utilizing same situations in NS - 2.

REFERENCES

1. M. Umaparvathi Dharmishtan K. Varughese “Two Tier Secure AODV against Black Hole Attack in MANETs” European Journal of Scientific Research.
2. Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya, John Dixon and Kendall Nygard “Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks”.
3. Fan-Hsun Tseng1, Li-Der Chou1and Han-Chieh Chao2,3,4” A survey of black hole attacks in wireless mobilead hoc networks”.
4. Nishant Sitapara ,Prof. Sandeep B. Vanjale”Detection and Prevention of Black Hole Attack in Mobile Ad-Hoc Networks”.
5. Hongmei Deng, Wei Li, and Dharma P.Agrawal (2002) “Routing Security in Wireless Ad Hoc Network” IEEE Communications Magzine,vol. 40, Issue: 10,(70-75).

6. Al-Shurman, M. Yoo, S. Park, "Black hole attack in Mobile Ad Hoc Networks" ACM Southeast Regional Conference, 2004, pp. 96-97.
7. Payal N. Raj and Prashant B. Swadas (2009)"DPRAODV: "A dynamic learning system against black hole attack inAODV based Manet" International Journal of Computer Science Issues (IJCSI), Vol. 2, Issue 3, pp: 54-59.
8. E. A. Mary Anita and V. Vasudevan," Black Hole attack Prevention in multicast routing Protocols For MANETs Using Certificate Chaining", IJCA, Vol.1, No.12, pp. 22–29,2010
9. Wei Gong1,2, Zhiyang You1,2, Danning Chen2, Xibin Zhao2, Ming Gu2, Kwok-Yan Lam2,"Trust Based Malicious Nodes Detection in MANET" . 978-1-4244-4589-9/09/$25.00 ©2009 IEEE
10. N. Bhalaji1, Dr. A. Shanmugam2," Defense Strategy Using Trust Based Model to Mitigate Active Attacks in DSR Based MANET" . Journal of Advances in Information Technology, Vol. 2, No. 2, May 2011
11. Latha Tamilselvan & Sankaranarayanan, V. (2007)" Prevention of Blackhole Attack in MANET" The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications (AusWireless 2007) Pages 21-27.
12. Pooja Jaiswal, Dr. Rakesh Kumar "Prevention of Black Hole Attack in MANET", IRACST – International Journal of Computer Networks and Wireless Communications (IJCNWC), ISSN: 2250-3501 Vol.2, No5, October 2012.
13. Y. Khamayseh, A. , Bader, W. Mardini and M. BaniYasein, "A New Protocol for Detecting Black Hole Nodes in Ad Hoc Networks "International Journal of Communication Networks and Information Security (IJCNIS) Vol. 3, No. 1, April 2011.
14. Bounpadith Kannhavong, Hidehisa Nakayama, Yoshiaki Nemoto, and Nei Kato; "A Survey Of Routing Attacks In Mobile Ad Hoc Networks", IEEE Wireless Communications October 2007, University of Washington.
15. K. Lakshmi1, S.Manju Priy , A.Jeevarathinam, K.Rama, K.Thilagam, "Modified AODV Protocol against Black hole Attacks in MANET" Lecturer, International Journal of Engineering and Technology, 2010.
16. Stefano Basagni1, Marco Conti2,Silvia Giordano3,Ivan Stojmenovic 4"Mobile Ad Hoc Networking".
17. Ankur O. Bang 1, Prabhakar L. Ramteke2 "MANET: History, Challenges and Applications" International Journal Of Application Or Innovation In Engineering & Management (IJAIEM).
18. Priyanka Goyal1, Vinti Parmar2, Rahul Rishi3" MANET: Vulnerabilities, Challenges,Attacks,Application" IJCEM International Journal of Computational Engineering & Management, Vol. 11, January 2011.
19. aspal Kumar, M. Kulkarni, Daya Gupta "Effect of Black Hole Attack on MANET Routing Protocols" University of Delhi, India.
20. Mobile Ad-hoc Networks (manets) By Donatas Sumyla.
21. International Journal of Technology Research and Management ISSN (Online): 2348-9006 Vol 1 Issue 6 December 2014 "A survey on Detection and Prevention Techniques for Black hole Attack in MANET Architecture"
22. Sevil en, John AClark, Juan E. Tapiador "Security Threats in Mobile Ad Hoc Networks" University of York, YO10 5DD, UK.
23. Clifton Lin "AODV Routing Implementation for Scalable Wireless Ad-Hoc Network Simulation" (SWANS) cal36@cornell.edu.
24. Vijayalaskhmi M.1, Avinash Patel "QoS Parameter Analysis on AODV and DSDV Protocols in a Wireless Network"International Journal of Communication Network & Security, Volume-1, Issue-1, 2011.