International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-4, November 2019

Efficient Detection of Black Hole attack in Mobile Adhoc Networks using a TRUST based Scheme

Deepak Sharma

Abstract: ***In this paper, the security problem of black hole node in mobile adhoc networks (MANET) is discussed. Mobile adhoc network is a kind of network in which there is no fixed structure of the network. All the nodes are mobile i.e. they are free to move where ever they want to move. Mobility of the nodes and lack of any central administration in the network leads to complex security problem and black hole attack is one such security problem. In this paper, some of the best work which are already exist in this field and the limitations are disused in brief. A Relative TRUST based approach to eradicate the problem of black hole is proposed in this paper.***

Keywords: Mobile Adhoc Network (MANET), AODV Protocol, Black Hole, Promiscuous Mode, Congestion.

I. INTRODUCTION

Mobile adhoc network is a network of movable node in which there is no central authority for managing the network. MANET consist of mobile nodes which coordinate with each other to facilitate communication between the movable nodes in the network. There are so many routing protocol exits for MANET some of them are AODV, DSDV, and DSR. MANET have many advantages in areas where setting up a fixed infrastructure is not possible such as military function, disaster areas, small personal network (PAN). MANET have many security concern due to lack of central authority and no fixed infrastructure.

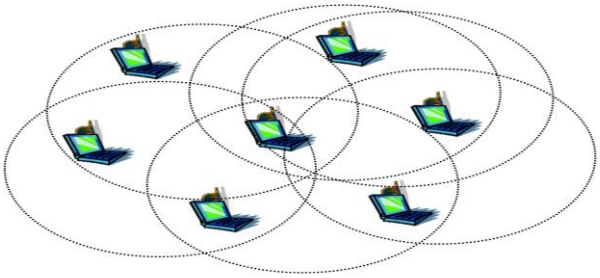

Fig. 1. Mobile Adhoc Network [MANET]

Manuscript published on November 30, 2019.
* Correspondence Author
Deepak Sharma*, Research scholar, MD University, Rohtak, India. Email: erdeepaksharmabwn@gmail.com

Security attacks in mobile adhoc network are always a point of attraction for the researchers all over the world from many years. Many computer scientist have written books about the eradication of the black hole problem but no method is claim the full removal of black hole attack till date. These security problems decrease the efficiency and throughput of the whole network by increasing the PDR. PDR stands for Packet drop ratio which is the ratio of packet dropped to the total number of packets sent during the session.

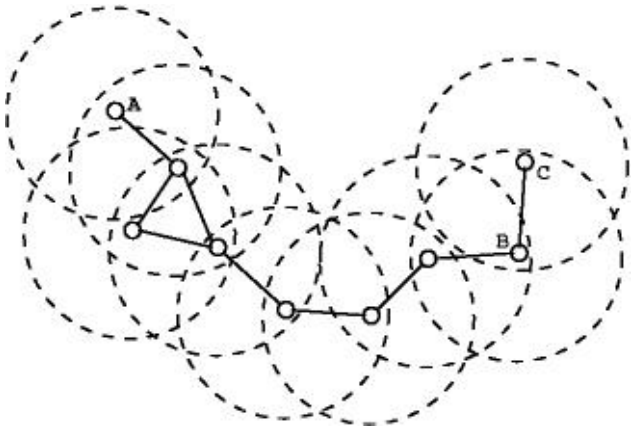

Fig. 2. Communication in MANET

In MANET, all the entities are free to move and there is no limitation on the nodes about maintain a particular location hence they can change their locations even if they are a part of the communication link which ultimately results in the breakage of the path and data loss. There is lack of central authority in MANET. This is the main advantage for the intruders who have the intension of disrupting the communication in the network.

Black hole is a particular type of security attack in which a node falsely claims of having a valid route to the destination, become a part of the communication path and then purposely drops the packet which ultimately results in data loss.

There are many routing protocols in MANET but AODV being the most famous and widely used protocol for routing in MANET. In AODV protocol we have three types of packets i.e. Route request packet (RREQ), Route reply packet (RREP), Route error packet (RERR).

When a nodes wants to communicate with another node it broadcast route request packet (RREQ) after receiving the RREQ packet nodes search in their routing table whether they have a valid route to the destination or not. If they have a valid route to the destination they will send a RREP packet to the sender that "YES! I have a valid route to the destination. If the nodes does not have a route they again broadcast the RREQ packet further. After receiving RREP packet, sender start transmitting the data from that route. Black hole attack is that in which an intruder node always try to became part of the communication path and always sends RREP packet to the sender and claims that it has a valid route to the destination even if it does not have any route to the destination.

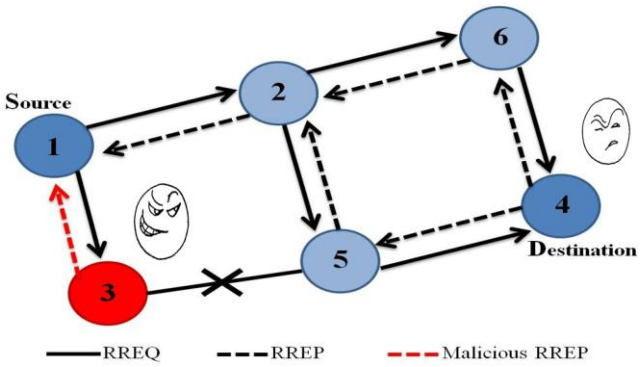

Fig. 3. Black Hole attack in MANET

In this paper, a TRUST based scheme is proposed and implemented to eradicating the problem of Black hole node in MANET. Also a brief overview about the already exiting work in this field is also discussed.

II. LITERATURE REVIEW

In this section we are focusing on the existing work which is proposed earlier and some basic overview about MANET.

Tamilselvan L et al. [6] proposed a Time-based Threshold Detection Scheme. According to the solution suggested in the paper, Sender node collects all the RREP packet in a table called as "Collect Route Reply Table (CRRT)" with the next hop details. When the first packet arrives, it sets the timer for which all the other RREP packets are collected. The "Sequence number" and "arrival time" of the packet is stored in the table for further processing.

After expiration of the timer sender has to select from a list of RREP packet. For selection of the route it verifies that whether there is any repeated next hop node because the chance of invalid path is less if any redundant next hop node is present. The PDR (Packet delivery ratio) is 90% whereas AODV is around 80%.

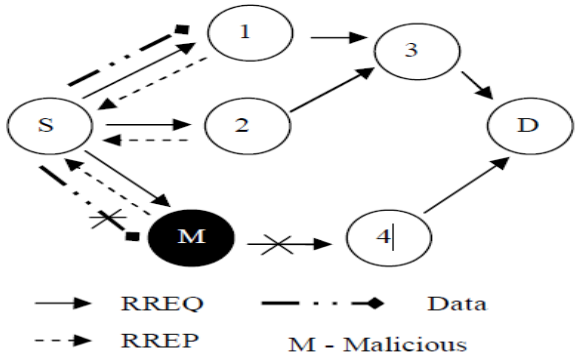

Fig. 4. Time-based Threshold Detection scheme

Nidhi Choudhary et al. [7] proposed an intelligent system for the removal of the problem of black hole node in MANET. They proposes an intelligent timer based scheme in which every node maintain a trust value corresponding to each neighboring node. Initially the trust value is set to a numerically large value for all the nodes. When a packet is forwarded by a node to its neighboring node it set a timer and start listening to the network in promiscuous mode until the timer expires. After the expiration of the timer the sender check that whether the same packet that has been transmitted earlier to that neighboring node was forward further by that node or not. If forwarded then no action shall be taken but if not forwarded then decrease its trust value. A node is advertised as black hole when its trust value is drop to a certain level.

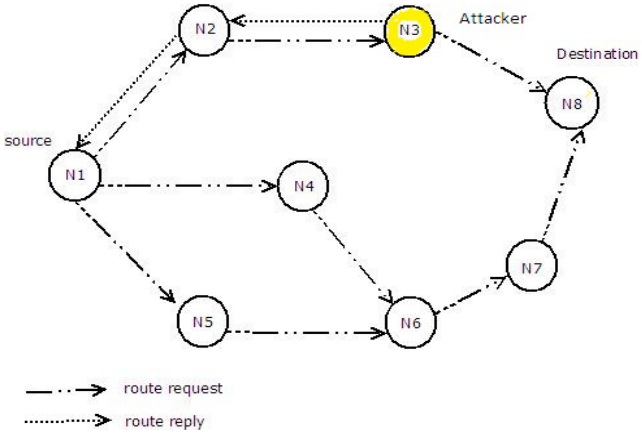

Fig. 5. Timer-Based Detection Mechanism

Al-Shurman M et al. [8] presented an alternative for detection of the black hole using the redundant nodes in different routes. In initialization, sender sends a RREQ packet and stores the RREP packet at least two or more route reply packets are received. On the basis of number of similar nodes in the path sender will choose a safe path.

Verify 75% to 98% of the routes and decrease the chance of black hole.

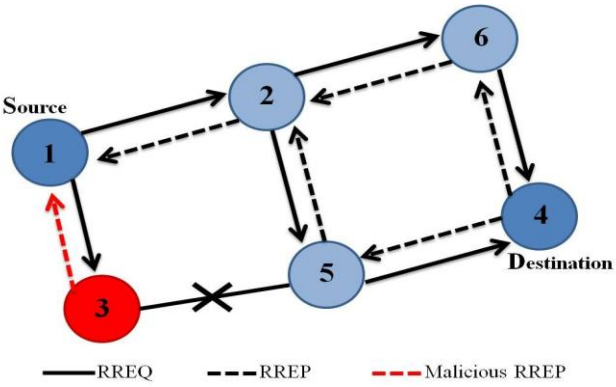

Fig. 6. Black Hole Attack in Mobile Ad Hoc

Anand A. Aware et al. [9] proposed an effective approach for eradicating the black hole Data integrity is also maintained using hash Function. In initialization the sender node always drops the first RREP route and choose the second shortest route. Hash function is used encrypting data for data integrity.

As founded by the author that throughput is relatively high as compared

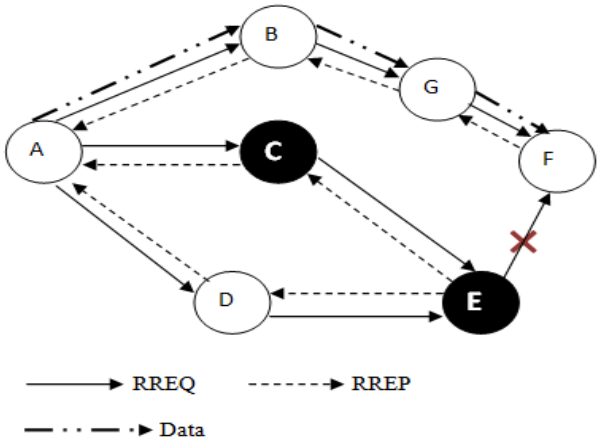

Fig. 7. Prevention using hash function

Apurva Jain et al. [10] proposed an effective trust based mechanism for eradicating the black hole. In starting every node initialized with a trust value=0.7 to all its neighboring nodes. After receiving the route replies from the nodes source node select the path from that replying node having maximum trust value. On successful delivery of a packet trust value increase and vice versa. Nodes with trust value < 0.7 advertised as black hole node. In some cases the results are relatively better but not for all scenarios.

Table- I: Trust Based Mechanism

Most Reliable	Unreliable	Reliable	Action
		> 0.7	**Request and check again**
	<0.7		**Disbelief the node**
> 0.7			**Trusted node**

III. COMPARATIVE ANALYSIS

Table- II: Comparative analysis

PAPERS	RESULT	LIMITATIONS
Tamilselvan L, Sankaranarayana n V, "Prevention of Black hole Attack in MANET".	PDR (Packet delivery ratio) is 90%.	The end-to-end delay increases when the intruder node is away from source node.
Nidhi Choudhary, Dr.Lokesh Tharani, "Preventing Black Hole Attack in AODV using Timer-Based Detection Mechanism".	PDR is better in some cases as compariso n to AODV.	On increasing the network size and intruders a decrease in PDR is analysed.
Al-Shurman M, Yoo S-M, "Park S, Black Hole Attack in MANET".	Verify 75% to 98% of the routes and decrease the chance of black hole.	End-to-end delay increases.
Anand A. Aware, Kiran Bhandari, "Prevention of Black hole Attack on AODV in MANET using hash function".	The throughput is relatively high.	End-to-end delay and Node Complexity Increases.
Apurva Jain, Urmila Prajapati, Piyush Chouhan, "Trust Based Mechanism with AODV Protocol for Prevention of Black-Hole Attack in MANET Scenario".	PDR and throughput are relatively High.	Node Complexity and implementation cost increases.

IV. PROPOSED APPROACH

A. Idea behind the Approach

In this work a TRUST based scheme is proposed to deal with the very famous security problem of Mobile Adhoc network i.e. Black hole attack. In this scheme every node maintain a trust value corresponding to each neighboring node. There are two values of trust one is autonomous trust which is based on node's behavior and other is indirect trust which is based on node's behavior with respect to the other neighboring nodes. Total trust value of a node is calculated on the basis of these two trust values. Every node is classified into two three categories based on their trust value. First is the Friend Node (Trust values (T) lies from b <T =<∞) second is Coordinator Node (Trust values (T) lies from a <T =<b) and the last one is suspicious Node (Trust values (T) lies from 0 <T=<a).

B. Working principle.

A TRUST based scheme is used in which trust values are calculated on the basis of node's behavior in the network with respect to other nodes. Every node maintain a TRUST value for all its neighboring node and keep updating that trust value. Initially, every node assigns maximum trust value (in this case 10) to all its neighboring node. Every time, in a communication whenever a node (N) forward a packet to its neighboring node (N+1) sets a timer (T). Until the timer (T) expires, Sender node (N) listen to the network n promiscuous mode to finding out whether the node (N+1) forwarded that packet further or not. If node (N+1) failed to successfully forward that packet then this will reflect in its TRUST value. Every node periodically calculate the trust values of its neighboring nodes and whenever a node's trust value drops to a significant level (in this case 0) then that node is advertised as a Black hole node and will be discarded for all future communication for a particular period of time. In this approach a new concept of relative trust value is used because some time what happened is due to congestion all the nodes in an area starts discarding packet.

This will leads to a drop in their trust values which might create a problem but in reality packet are dropped due to congestion and not due to the black hole phenomena. So, in these cases relative trust value help the sender to distinguish between a congestion and black hole condition.

C. Calculation of trust values

Two parameters are considered for calculation of autonomous trust. One of them is Packet successfully delivered (P_{SD}) and other is Packet Dropped (P_{DP}). Two parameters are considered for calculation of indirect trust. One of them is Average Packet Dropped (PD_{AVG}) and other is Packet Dropped (P_{DP}).

Final trust value of node called as total trust is calculated by adding up the values of absolute trust and relative trust of that node. Formulas for calculations of trust values are given in the table.

Table- III: Performance Analysis

TRUST VALUES	FORMULAS
Autonomous Trust	AT= AT + {P_{SD} X (0.01) - P_{DP} X (0.1)}
Indirect Trust	IT= IT+ {PD_{AVG} - P_{DP}} x 0.1
Final Trust	Final trust= AT + IT

D. Sample calculations

Sample calculations are shown in the table for network represented in figure 8. Take initial values of Absolute and Relative trust as 1.

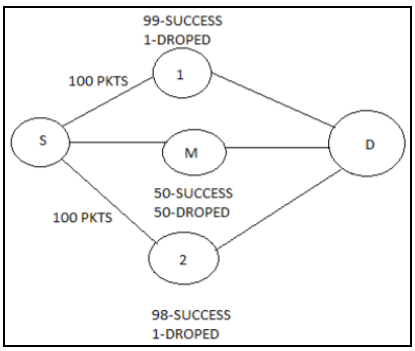

Fig. 8. MANET: Example

Table- IV: Sample Illustration

Node -1
AT= AT +{P_{SD}x(0.01)- P_{DP} *x(0.1)* }
AT=1.8
IT= IT+{PD_{AVG} - P_{DP} }x0.1
IT=2.66
Total trust= AT + IT =4.46
Node -2
AT= AT +{P_{SD}x(0.01)- P_{DP} *x(0.1)* }
AT=1.78
IT= IT+{PD_{AVG} - P_{DP} }x0.1
IT=2.56
Total trust= AT + IT=4.346
Node -M
AT= AT +{P_{SD}x(0.01)- P_{DP} *x(0.1)* }
AT= -3.5
IT= IT+{PD_{AVG} - P_{DP} }x0.1
IT= -2.24
Total trust= AT + IT= **-5.74**

E. Results and Analysis

Three Metrics are used for the comparison between the performance of the AODV and the proposed DS_AODV protocol. First is *Packet Delivery Ratio* (proportion between the packet received and the generated packets), second is *Throughput* and third is *Route Acquisition Time* (time taken by the sender in finding out a transmission path to the specific destination).

Table- V: Performance Analysis

Metrics	AODV	DS_AODV
Packet Delivery Ratio(PDR)	22.2256 %	60.5157 %
Throughput	0.0341304 Mbps	0.0613186 Mbps
Acquisition Time	0 Second	0 Second

V. CONCLUSION

In this work a TRUST based scheme is proposed to deal with the very famous Black hole attack in MANET. Also, some of the best works in this were also critically analyzed and briefly discussed.

This will help to eradicate the black hole problem in MANET. According to this approach, we claim to find the black hole in the network sooner. In future the results can be calculated for different scenario by varying Communication Range and Trust Threshold. Also results can be compared with AODV Protocol for analysis for additional parameters such as umber of Packet Dropped and End to end Delay etc.

REFERENCES

1. Rutvij H. Jhaveri, Sankita J. Patel, Devesh C. Jinwala, "DoS attacks in Mobile Adhoc Networks: A Survey", Second International Conference on Advanced Computing & Communication Technologies, IEEE, 2012.
2. Fidel Thachil, K.C. Shet, "A trust based approach for AODV protocol to mitigate Blackhole attack in MANET", International Conference on Computing Sciences, IEEE, 2012.
3. Nital Mistry, Devesh C. Jinwala and Mukesh Zaveri, "Improving AODV Protocol against Blackhole Attacks", International Multiconference of Engineers and Computer Scientists 2010, vol. 2, March 2010.
4. Vishnu K, Amos J. Paul , "Detection and Removal of Cooperative Black/Gray hole attack in mobile adhoc networks." , International Journal of Computer Applications, Vol. 1, No. 22, 2010.
5. Soufiene Djahel, Farid Na¨Õt-abdesselam, and Zonghua Zhang, "Mitigating Packet Dropping Problem in Mobile Ad Hoc Networks: Proposals and Challenges", IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 13, NO. 4, FOURTH QUARTER 2011.

6. Tamilselvan L, Sankaranarayanan V, Prevention of Black hole Attack in MANET. Paper presented at the 2nd International Conference on Wireless Broadband and Ultra Wideband Communications, Sydney, Australia, 27-30 August, 2007, IEEE.
7. Nidhi Choudhary, Dr.Lokesh Tharani, "Preventing Black Hole Attack in AODV using Timer-Based Detection Mechanism" SPACES-2015, Dept. of ECE, K L UNIVERSITY, IEEE, 2015.
8. Al-Shurman M, Yoo S-M, Park S, Black Hole Attack in Mobile Ad Hoc Networks. Paper presented at the 42nd Annual ACM Southeast Regional Conference (ACM-SE'42), Huntsville, Alabama, 2-3 April 2004.
9. Anand A. Aware,Kiran Bhandari, "Prevention of Black hole Attack on AODV in MANET using hash function" Published in: Reliability, Infocom Technologies and Optimization (ICRITO) (Trends and Future Directions), 3rd International Conference on 8-10 Oct. 2014,IEEE.
10. Apurva Jain, Urmila Prajapati, Piyush Chouhan, "Trust Based Mechanism with AODV Protocol for Prevention of Black-Hole Attack in MANET Scenario". Published in: Colossal Data Analysis and Networking (CDAN), Symposium on 18-19 March 2016, IEEE.
11. T. Clausen, J. Dean, C Adjih, "Generalized Mobile Adhoc Network Packet/Message Format", RFC-5444, July 2015.
12. Aarti,Dr. S.S Tyagi "Study of MANET: Characteristics, Challenges, Application and Security Attacks", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, ISSN: 2277 128X May 2013.

AUTHORS PROFILE

Deepak Sharma has completed his M.tech from C-DAC: Centre for Development of Advanced Computing, Ministry of Communications and Information Technology, Government of India affiliated from Guru Gobind Singh Indraprastha University, Delhi. He is currently pursuing a Ph.D. in Computer Science at M. D. University, Rohtak. His main research areas include Data mining, Mobile Adhoc Network (MANET), wireless sensor network (WSN) and Internet of things (IoT).