ISSN:0975-9646

Collaborative Black hole attack on MANET

Sushama Singh [1], Atish mishra[2] Dinesh Bhuriya [3], Upendra Singh [4]

[1, 4] *M Tech student PCST INDORE-INDIA*
[2] *Asst. Prof. PCST College INDORE-INDIA*
[3] *Lecturer Govt. Women's Polytechnic, Indore*

Abstract: A mobile ad-hoc network (MANET) is wireless and an autonomous system such that nodes are move randomly in network. Every node to maintain host and router in network layer. The principal of routing protocol is Ad-hoc on demand Distance Vector (AODV). It is used node to node routing. AODV is searching path from source to destination in ad-hoc network. The network layer in OSI model so use many types of attacks but introduce only collaborative black hole attack. Collaborative black hole attack is a group of black hole node. Such nodes use malicious nodes involve in network performance severely nodes dropping by all the data packets forwarding to receiver. In this paper we introduce trusted AODV routing protocol which trust value calculate using sin function. The result shows performance improvement as compared to standard AODV protocol.

Keywords: Mobile ad-hoc network, AODV, Collaborative Black hole attack, Trusted AODV, TANH, NS2, Energy, Throughput, Packet Delivery ratio.

I. INTRODUCTION

MANET is wireless and an autonomous system that means it's not recur communications. The wireless network is not used physically wired. In MANET nodes perform dynamically nature or randomly in ad-hoc network. The randomly nature of mobile ad-hoc network make it added exposed [1]. In MANET so many types of attacks such like black hole and collaborative black hole attacks. Black hole attack is a type of active attacks and use of malicious node in which receive to all data packets in ad-hoc network. In this way, the useful all packets in the ad-hoc network are dropped. When a group of black hole nodes with no difficulty employed at the side of routing in mobile ad-hock networks. This type of attack is identifying collaborative black hole attack [2]. Due to high mobility of approach routing is big dispute in ad-hoc network. The ad-hoc on demand distance vector routing is a reactive routing protocol. The routing protocol is identifying and transmit packet from source node to destination node. This routing protocol is using only sequence number.

In the proposed work, trust based routing protocol is defined in which trust computation is done using tangent hyperbolic function which calculate the trust value of their neighboring nodes promiscuously.

They have a rest of the paper is organized as follows Section II runs some background of related work. Section III working of cooperative black hole attack Section IV Trusted AODV Routing Protocol as our proposed work. Section V suggests simulation work and result. Finally, we conclude in section VI.

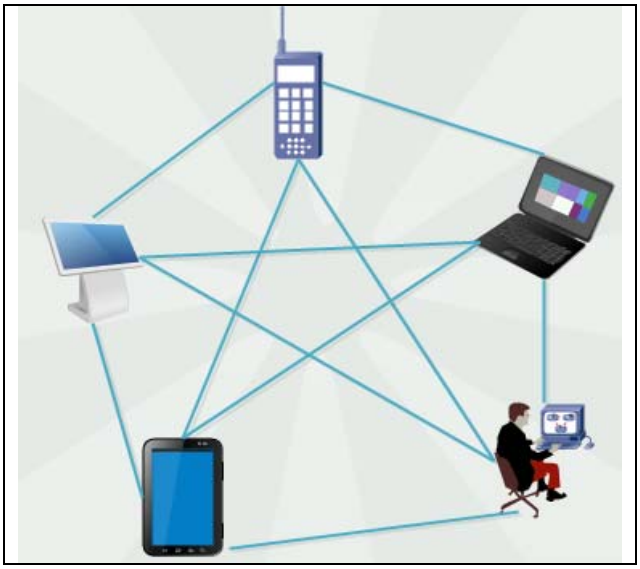

Fig.1. mobile ad-hoc network architecture

II RELATED WORK

In our previous research in [8] we have minimized the effect of black hole attacks in MANET using the concept of Tangent Hyperbolic function. In tanh(t) after calculate return value between -1 to +1 but in my propose solution assume only positive value (0 to +1) , if get t greater than and equal to 8 then mark node is Most reliable, t less than 8 and greater than equal to 4 then node is mark reliable and t value less than 4 then node is mark Unreliable.

In [1] in this paper authors minimized the effect of attacks in MANET using the concept of cryptographic routing algorithm. In cryptographic technique based on RSA and DES Algorithms. RSA involves a public key and private key. The public key can be known by everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted in a reasonable amount of time using the private key.

In [3] in this paper authors proposed an algorithm which is also base on RTT (Round Trip Time) as well as topological comparison, combination of both is referred as RTT-TC. These modifications are performed in Ad Hoc on demand distance vector (AODV) routing in MANET. The proposed solution firstly relies on Round Trip Time (RTT) which helps to identify suspected nodes and after that Topological comparison to exclude genuine neighbours from the list of suspected nodes.

In [7] in this paper author proposed a method based on route redundancy, route aggregation and round trip time. There are three phases in which proposed algorithm works. In the first phase, create a multipath to authenticate RREQ;

Second phase is used to aggregate which help to know the all possible paths of the source and destination. In last phase there is calculation of average time of all routes based on the number of hopes.

In [11] in this paper author proposed a method based Counter measuring techniques of these DOS attacks be as well presented.

In [13]. In this improve attack using RREQ and RREP techniques

III. Collaborative Black Hole Attack

Collaborative Black hole attack a cluster of black hole node without difficulty employed against routing in mobile ad-hock networks. These types of attack are called collaborative attack show on fig 2.

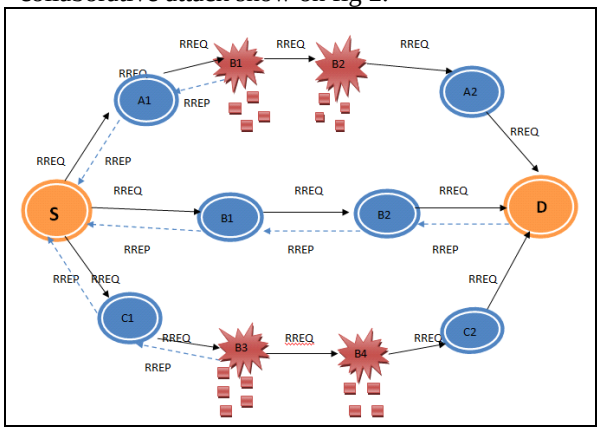

Fig 2 Collaborative Black hole attack

IV. Trusted AODV Routing Protocol

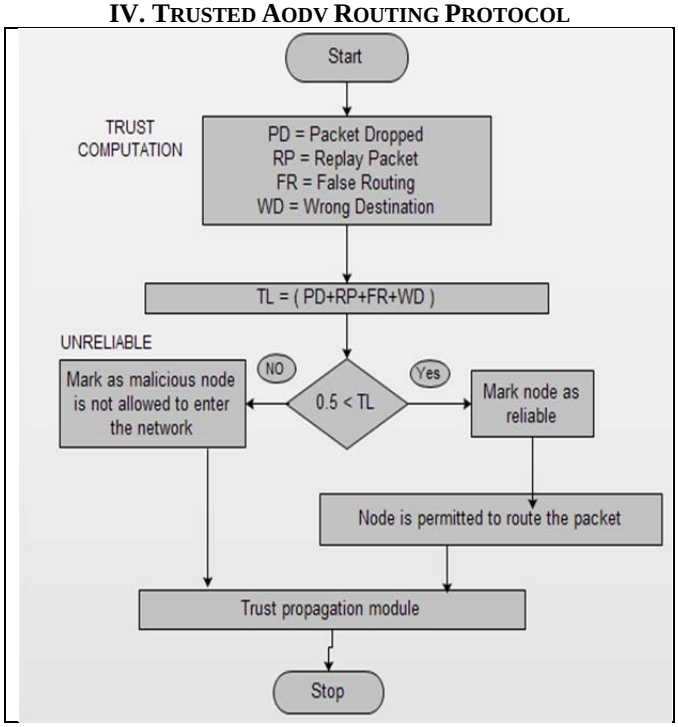

Fig 3. Flow chart for proposed model

THAODV is a trusted routing protocol based on trust model for mobile Ad-hoc network. THAODV has many relevant features similar to Nodes present trusted routing behaviors mainly according to the trust associations between them. A node that performs malicious behaviors will finally be detected and denied to the entire network. System routine is improved at every routing hop [5].

a) Trust class of a node:

AODV routing protocol is set in along through the ***trust function***. The contact between the nodes in the mobile Ad-hoc network depends on the support and the trust level with its neighbors. Base on the trust on neighbor and suitable threshold values the nodes can be sort in to the following.

I. **Unreliable:** It's have the non trusted node. Means node having minimum trust value.

II. **Reliable:** Its type's node has the trust level among the Most Reliable and Unreliable. Means a node is Reliable toward its fellow citizen means it has acknowledged some packets through that node.

Trust value	Action	Node behavior
TL>=0 && TL<0.5	Block	Unreliable node
TL<=0.5 && TL>=1	Allow	Reliable nodes

b) Threshold Value of a node:

Threshold values are defined for dissimilar types of neighbors to Become Reliable and Unreliable.

We propose a Trust estimation function for the estimate of trust value.

$$TL = \tanh(T)$$

Where

Tanh is a hyperbolic tangent function, which has value

$$\tanh x = (e^{x} - e^{-x})/(e^{x} + e^{-x})$$

T = Trust Parameter
TL = Trust Level
PD = Packet Dropped
RP = Replay Packet
FR = False Routing
WD = Wrong Destination

If T = (PD+RP+FR+WD) is high then TL is Low.
If T = (PD+RP+FR+WD) is Low then TL is High.

c) Trust status updating of a node:

After calculation result lies between -1 to +1, but we consider only 0 to +1 value.

Where

T= Trust Threshold level.

.

V. Simulation And Result

We perform a set of simulations base going on *NS-2* with extensions for mobile wireless networks. To evaluate the performance of THAODV we have taken following simulation parameters in our simulation [5].

Simulation Parameters

Simulation Parameters	Value
Number of nodes	42
Network size	1200*1200
Simulation duration	100(Sec)
primary Energy	100
txpower	0.9
repowers	0.8
Idle power	0.0
Sense power	0.0175
Source node	17
Destination node	17
Collaborative Malicious	4
Packet size	1024

As mention in above scenario we have compare the Energy, Throughput, Packet Delivery ratio of Collaborative Black hole attack AODV and THAODV which shows in 5.1,5.2 and 5.3 .

5.1 End to end Delay:

End to end Delay is the time taken for the packet to travel from source to the destination node. With increase in number of malicious nodes, End to end delay of CBAODV increases. End to end delay of THAODV also increases but is stable with respect to CBAODV.

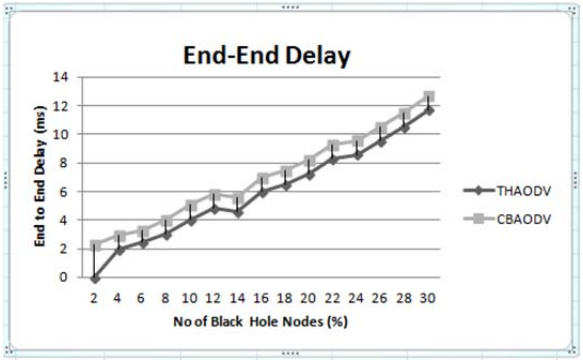

Fig. 4 End to End Delay for scenario of collaborative black hole attacks

5.2 Throughputs: Throughput is the average rate of victorious packets delivery over a communication channel [5].

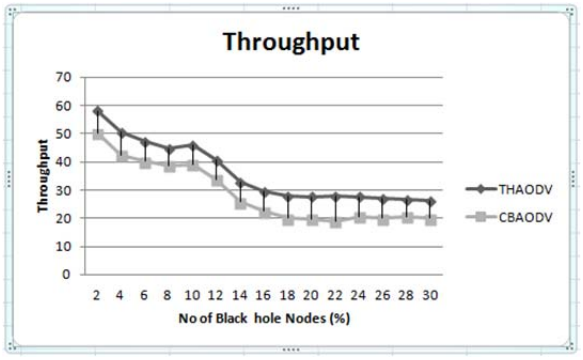

Fig .5 Throughputs for scenario of collaborative black hole attacks

5.3 Packet Delivery Ratio: The ratio between the number of packets originated by the "application layer" Constant Bit Rate source and the number of packets received by the Constant Bit Rate go under at the final destination [5].

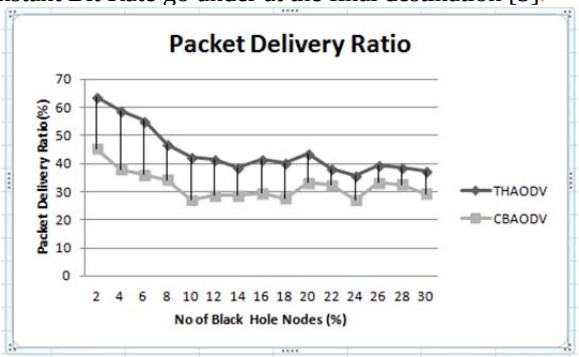

Fig .6 Packet Delivery Ratios for scenario of collaborative black hole attacks

VI. Conclusion

By using NS-2 simulation. We are finding some conclusion**.** Throughput of THAODV is better compare to Collaborative Black hole AODV, by increasing the moment a trace effect in throughput in together the case. Packet delivery ration is better compare to Collaborative Black hole AODV, when we raise the point in time the packet deliver ratio of both is increase and End to end delay of THAODV is better compare to Collaborative Black hole AODV As shown in fig. 4, 5, 6 .

VII. Future Work

In this paper we have calculate trust value of Collaborative Black hole attack by using different parameter and simulate by NS-2 tool. In future we will calculate trust value of other attacks on MANET.

References

[1] A Sharma, D bhuriya, U singh , "Secure data transmission on MANET by hybrid cryptography technique", IEEE 2015 International Conference on Computer, Communication and Control (IC4), 10-12 Sept. 2015 Pages1 – 5 .

[2] Alka Chaudhary, V.N. Tiwari," Design an Anomaly Based Fuzzy Intrusion Detection System for Packet Dropping Attack in Mobile Ad Hoc Networks", 978-1-4799-2572-8/14/$31.00_c 2014 IEEE..

[3] Mohammad Rafiqul Alam, King Sun Chan et al.",RTT-TC: Topological Comparison Based Method to Detect Wormhole Attacks in MANET", IEEE,2010 pages 991 – 994

[4] Animesh Patcha and Amitabh Mishra "Collaborative Security Architecture for Black Hole Attack Prevention in Mobile Ad Hoc Networks" , 0-7803-7829-6/03/$17.00 0 2003 IEEE.

[5] Reshmi Maulik and Nabendu Chaki "A Study on Wormhole Attacks in MANET", International Journal of Computer Information Systems and Industrial Management Applications ISSN 2150-7988 Volume 3 (2011) pp. 271-279.

[6] C. Perkins, E. Belding-Royer, and S. Das, "Ad Hoc On demand Distance Vector (AODV) Routing," IETF RFC 3561, July 2003.

[7] Soo Young Shin, Eddy Hartono Halim eet al., "Wormhole Attack Detection in MANETs using Route Redundancy and Time-based Hop Calculation", IEEE, 2012 pages 781 – 786.

[8] Ashish Sharma 1, Dinesh Bhuriya 2 , Upendra Singh 3 , Sushma Singh "Prevention of Black Hole Attack in AODV Routing Algorithm of MANET Using Trust Based Computing "/ (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (4) , 2014, 5201-5205 ISSN 0975-9646

[9] Liang Chiu-kuo, Wang Hsi-shu. An Ad Hoc On-Demand Routing Protocol with High Packet Delivery Fraction[C]// Proc. of 2004

IEEE International Conference on Mobile Ad-hoc and Sensor Systems.[S.1.]: IEEE Prees, 2004: 594-596.

[10] A. Jain and V. Tokekar. "Classification of denial of service attacks in mobile ad hoc networks," Proceedings of International Conference on Computational Intelligence and Communication Networks (CICN), pages 256–261, IEEE ,2011

[11] Hongmei Deng, Wei Li, and Dharma P. Agrawal, "Routing Security in Wireless Ad Hoc Network," IEEE Communications Magzine, vol. 40, no. 10, October 2002.

[12] Jian Yin, Sanjay Madria, "A Hierarchical Secure Routing Protocol against Black Hole", IEEE SUTC 2006 Taiwan, 5-7 June 2006.

[13] S. Buchegger, C. Tissieres, and J. Y. Le Boudec. "A test bed for misbehavior detection in mobile ad-hoc networks", –how much can watchdogs really do. Technical Report IC/2003/72, EPFL-DIICA, November 2003