IEEE International Conference on Computer, Communication and Control (IC4-2015).

Detecting and Avoiding of Worm Hole Attack and CollaborativeBlackhole attack on MANET using Trusted AODV Routing Algorithm

Neeraj Arya[1] SGSITS,
Indore, India
neerajaryagate2010@gmail.com

Upendra singh[2]
PCST, Indore
Indore, India
upendrasingh49@gmail.com

Sushma singh[3]
PCST, Indore
Indore, India
sushmasingh12gs@gmail.com

***Abstract*--- A mobile ad-hoc network is a wireless network such that nodes are move dynamically in network. In OSI network layer there is lot of attack but introduce only collaborative black hole and worm hole attack. A group of black hole node easily employed against routing in mobile ad-hock networks called collaborative black hole attack. When two malicious node is create a tunnel is called worm hole attack. This paper instigate to detect and avoided of worm hole attack and collaborative black hole attack using trusted AODV routing algorithm**.

Keywords: MANET; AODV; Worm Hole Attack;CollaborativeBlack hole attack;TAODV

I.INTRODUCTION

A mobile ad-hoc network is wireless network that means it's not recurred infrastructure. In mobile ad-hoc network nodes are move dynamically nature. The dynamic natures of MANET make it more vulnerable [1]. In MANET one of very possible attack is collaborative black hole attack and worm hole attack. Black hole attack is a malicious node which absorbs all data packets in itself similar to a hole. This sucks in everything. In this way, all useful packets in the network are dropped. When a group of black hole node easily employed against routing in mobile ad-hock networks. These types of attack are called collaborative black hole attack[2]. When two malicious node is create a tunnel is called worm holeattack [3]. Due to high mobility of mode routing is big challenge in ad-hoc network.

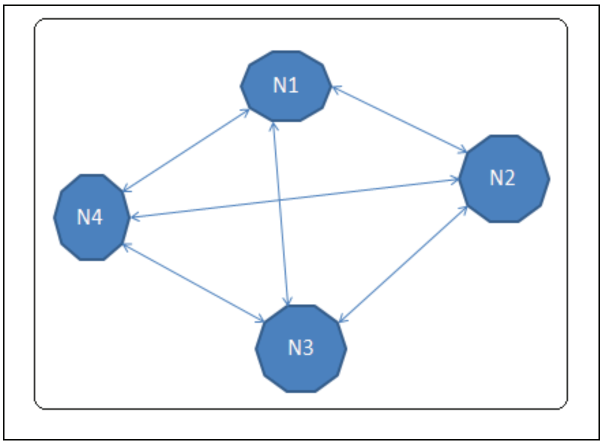


Fig.1. mobile ad-hoc network architecture

II.AODV ROUTING PROTOCOL

The routing protocol play main role in identifying and packet transmit from source node to destination node, through intermediate nodes. Ad-hoc on demand distance vector routing(AODV)is a reactive routing protocol. AODV is provide a dynamic network connection and less memory consumption, less processing, loads. AODV protocol is used sequence number to distinguish. Routing message are fresh routing messageswhich broad cast in the network can be divide into path discovery and path. AODV includes three messages route request (RREQ) fig 2, rout reply (RREP) fig 3 and another route error (RERR) fig 4 [4][5]. [6] Proposes a scheme to improve packet delivery fraction of the ad hoc on demand distance vector (AODV) protocol and compare it with performance of several routing protocol.

type	flags	Reserved	Hop count
RREQ(Broadcast) id			
Destination IP address			
Destination sequence number			
Source IP address			
Source sequence number			

Fig.2. RREQ

type	A	reserved	Hop count
Destination IP address			
Destination sequence number			
Source IP address			
Source sequence number			

Fig.3. RREP

type	N	reserved	Destination count
Unreachable destination IP address			
Unreachable destination sequence number			
Additional unreachable destination IP address(if needed)			
Additional unreachable destination sequence number (if needed)			

Fig.4. RERR

Each mobile node maintains a routing table and updates the content fields while receiving a routing message. All field related to RREQ, RREP and RERR show in Fig.And routing table related fields in Fig.5

Destination IP address
Destination sequence number
Hope-count
Next-hope
First-hope
Valid bit
Count

Fig5. Fields of AODV routing table

When a source node needs to send data to a destination, first check if destination address directly present in source node routing table if found it send data otherwise source node would broad cast a RREQ to all neighbor nodes. In the network then all intermediate node get RREQ, would first judge update route table then if intermediate node is destination so send RREP packet otherwise that node re broad cast RREQ message to neighbor that's step repeat until found destination node. If found destination node then generates RREP packets send to source.

In AODV routing protocol routing process must be based on sequence number. In fig.6 display the working of AODV routing algorithm [4][5].

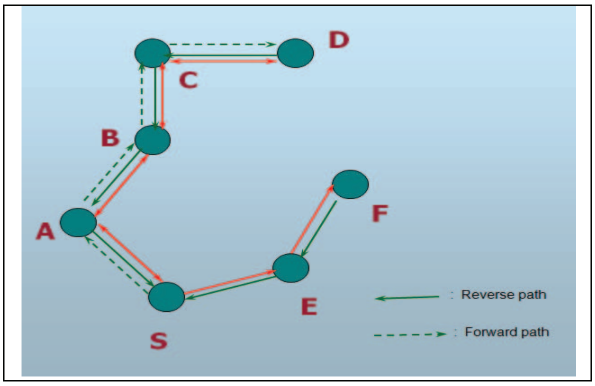


Fig.6 Workingof AODV

III. WORM HOLE ATTACK ANDCOLLABORATIVEBLACK HOLE ATTACK

A. *Collaborative Black hole attack*

A group of black hole node easily employed against routing in mobile ad-hock networks. These types of attack are called collaborative attack show on fig 7.

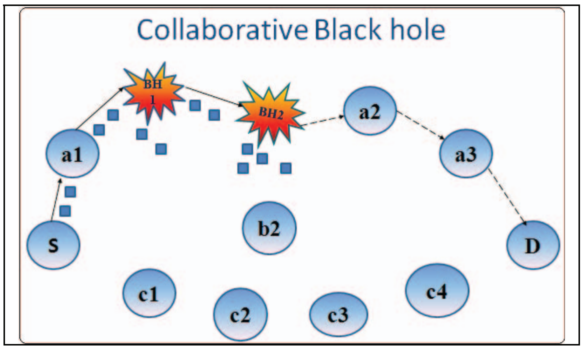


Fig 7 Collaborative Black hole attack

B. *WORM HOLE ATTACK:* Two malicious node is create a tunnel is called worm hole attack.Means twocollude nodes that are far apart are linked by a tunnel giving an illusion that they are neighbors. Each of these nodes accept route request and topology control messages from the network and send it to the other colluding node via tunnel which will then replay it into the network from there. By using this additional tunnel, these nodes are able to advertise that they have the shortest path through them. Once this link is established, the attackers may choose each other as multipoint relays, which then lead to an exchange of some topology control messages and data packets through the wormhole tunnel and Worm hole node drop all the packets [3]. Worm hole and collaborative black hole attack show on fig 8.

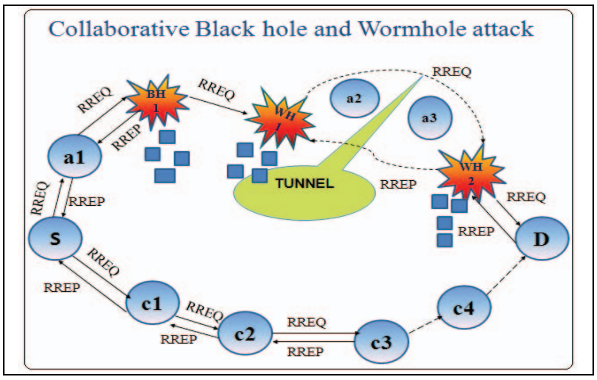


Fig 8Worm Hole attack and Collaborative Black hole attack

IV.TRUSTED AODV ROUTING PROTOCOL

Trusted AODV is a trusted routing protocol based on trust model for mobile Ad-hoc network. Trusted AODV has manyrelevant features likeNodes perform trusted routing behaviors mainly according to the trust relationships among 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 category of a node:*

In this work the AODV routing protocol is embedded along with the ***trust function***. The communication between the nodes in the mobile Ad-hoc network depends on the cooperation and the trust level with its neighbors. Based on the trust on neighbor and appropriate threshold values the nodes can be categorized in to the following.

1) *Unreliable:*The Unreliable is the non trusted node. Means anUnreliable node is a node with minimum trust level. Initially when any node joins the network, then this trust relationship with its all the neighbors are low or negligible that node is treated as Unreliable.

2) *Reliable:*These are the nodes which have the trust level between the Most Reliable and Unreliable. Means a node is Reliable to its neighbor means it has received some packets through that node.

3) *Most Reliable:*Most Reliable are most trusted nodes or the nodes with highest trust level can be treated as Most Reliable. Here the higher trust level means neighbors had received or transfer many packets successfully through this particular node.

During the route discovery phase of the AODV Routing protocol, the trust value is also computed for all the neighbors of any node. The result of trust estimation function is the Trust-status of all of neighbors as Most Reliable, Reliable or Unreliable.

To detect the malicious behavior of nodes, in this scheme each node maintains a Trust table. Trust table is used to store the Trust status of any node with its neighbors. The Trust table has two columns. First the identifier or name of its entire neighboring node and second its relationship status with the neighbor node that could be Most Reliable, Reliable or Unreliable. This table is referred every time when any node receives the packets. Initially when node joins the networks they are considered as an Unreliable. There is very high probability of attack from Unreliable but very low probability from Most Reliable [5].

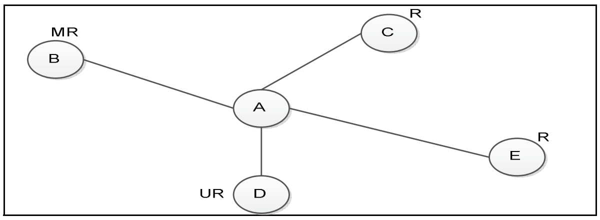


Fig 9

TABLE I. TRUST TABLE FOR NODE A:

Neighboring Nodes	Trust status
B	Most Reliable
C	Reliable
D	Unreliable
E	Reliable

Here node **B** is Most Reliable, node **C** and node **E** are reliable and node **D** is Unreliable as shown is Fig 8. We choose a route which goes from Most Reliable node that is**B**among all the nodes**.** In such condition, if there is no node which has Most Reliable status so we give priority to Reliable nodes but we never give chance to any Unreliable node to form a route [5].

B. Threshold Value of a node:

Different threshold values are defined for different types of neighbors to Become Most Reliable, Reliable and Unreliable. **T***ur*, **T***r* and **T***mr* are the threshold values for the Unreliable, Reliable and the Most Reliable respectively [5].

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

$$\boxed{T = \tanh(R1+R2)}$$

Where
tanh is an hyperbolic tan function, which has value

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

T = Trust value
R1= Ratio between the number of packets actually forwarded and number of packets to be forwarded.
R2 = Ratio of number of packets received from a node but originated from others to total number of packets received from it.

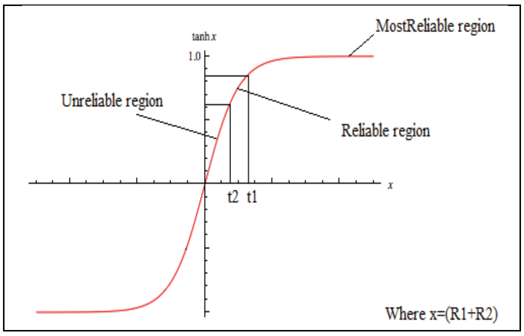
C. Trust status updating of a node:

After receiving the RREP from all the neighbors, Source node check the trust status of neighbors and then decide the route. For updating the trust status we send **n** fake packets. In the basis of packet-processing we calculate the new trust status of the nodes and if it required then update it.The threshold trust level for an Unreliable node to become a Reliable to its neighbor is represented by **T***r* and the threshold trust level for a Reliable node to become a Most Reliable of its neighbor is denoted by **T***mr*. The Trusts are represented as

A (node x → node y) = Most Reliable when $T \geq t1$
A (node x → node y) = Reliable when $t2 \leq T < t1$
A (node x → node y) =Unreliable when $0<T \geq t2$

Where
A= Trust,
T=Threshold
And t1, t2, t3 are the threshold values which will be decided in implementation part.

D. Graph representation of trust values of a node:



In the above graph value of **x** is always greater than **0**, because**R1** and **R2** will always remain positive so **T** belongs from (0 1).

V. SIMULATION AND RESULT

We performed a set of simulations based on *NS-2*with extensions for mobile wireless networks. To evaluate the performance of Trusted AODVwe have taken followingsimulation parameters in our simulation[5].

SIMULATION PARAMETERS

Simulation Parameters	**Value**
Number of nodes	38
Network size	1500*1000
Simulation duration	75(Sec)
Initial Energy	100
Txpower	0.9
Repowers	0.8
Idle power	0.0
Sense power	0.0175
Source node	17
Destination node	17
Collaborative Malaysia's	2
Worm Hole	2
Packet size	1024

As mention in above scenario we have compare the Energy, Throughput, Packet Delivery ratio of Worm Hole Attack and CollaborativeBlack hole attack AODV and Trusted AODV which shows in 5.1,5.2 and 5.3 .

A. *Energy:*In ad-hoc network energy is playing a vital role because many nodes are breakdown due to less of energy. The energy behavior of the different nodes wasinvestigated using simulations [5].

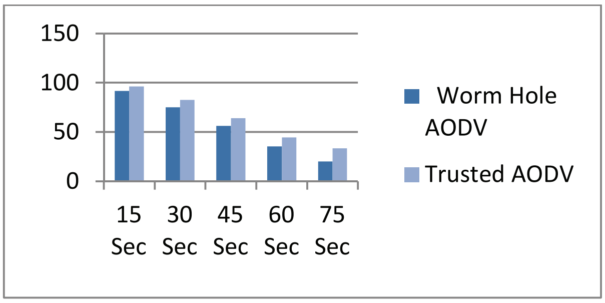


Fig.10

B. *Throughputs:*Throughput is the average rate of successful message delivery over a communication channel [5].

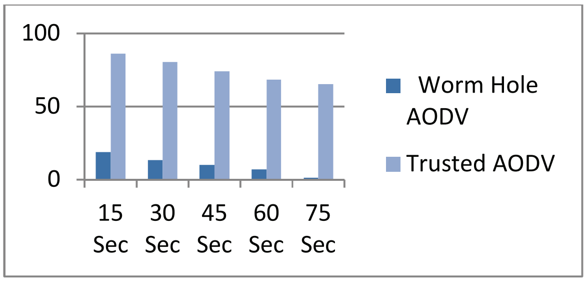


Fig .11

C. *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 [5].

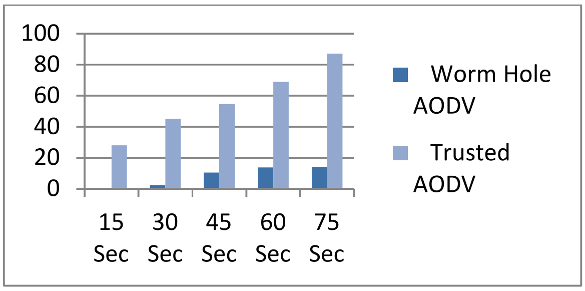


Fig .12

VI. Conclusion

By using simulation on NS-2 we find following conclusion**.** Theenergy of Worm Hole Attack and CollaborativeBlack hole attack AODVis more as compare to Trusted AODV, when we increase the time the energy level of both is decrease.Throughput of Trusted AODV is better compare to Worm Hole Attack and CollaborativeBlack holeattack AODV, by increasing the time a little bit effect in throughput in both the case.Packet delivery ration is better compare to Worm Hole Attack and CollaborativeBlack holeattack AODV, when we increase the time the packet deliver ratio of both is increase.As shown in fig. - .When we want more throughputs, more packet delivery ratio and less energy we use Trusted AODV.

VII. Future Work

In this paper we have calculate trust value of Worm Hole Attack and CollaborativeBlack 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]. AlkaChaudhary, 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..

[2]. AnimeshPatcha 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.

[3]. ReshmiMaulik and NabenduChaki "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.

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

[5] 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

[6] 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.