ISSN:0975-9646

Ashish Sharma et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (4) , 2014, 5201-5205

Prevention of Black Hole Attack in AODV Routing Algorithm of MANET Using Trust Based Computing

Ashish Sharma [1], Dinesh Bhuriya [2] , Upendra Singh [3] , Sushma Singh [4]
[1] *HOD Govt. Women's Polytechnic, Indore*
[2] *Lecturer Govt. Women's Polytechnic, Indore*
[3,4] *SGSITS-INDORE*

Abstract: A mobile ad-hoc network is a decentralized network. It is a group of mobile nodes that are dynamically and arbitrarily located in such a manner that the interconnections between nodes are capable of changing on continual basis. In mobile ad-hoc network there are so many attacks. In this paper we are focus black holes attack. TAODV is a secure routing protocol based on trust model for mobile ad-hoc network. We have taken TAODV routing protocol approach to focus on analyzing and improving the security of Black hole in AODV routing protocol. AODV is a popular routing protocol for mobile ad-hoc network. Our aim is on ensuring the security against black hole attack. The metrics energy, throughputs and packet delivery ratio are used to determine the performance of AODV, AODV with black hole attack and Trusted AODV. By using simulation tool on ns2, the energy of Black hole is more as compare to TAODV and throughput of TAODV is better compare to black hole AODV, similar to packet delivery ration is better compare to black hole AODV.

Keywords: black hole attack; detection performance on network simulation; ad hoc on-demand distance vector routing protocol; trusted ad hoc on-demand distance vector routing protocol; mobile ad hoc networks.

1. INTRODUCTION

Networks are two types Centralized and Decentralized. In this paper we are emphasis on Decentralized network known as Ad-hoc network. Ad-hoc network is infrastructure less network. Ad-hoc network is a collection of mobile node and each node communication with the help of radio wave signals [1]. Ad-hoc network consists of mobility features. It mean`s each device move freely in any area within a decided network a range and fresh node may be join and leave the network range. It is consists of dynamic network topology but it's not belong to the fixed topology. So maintain difficult in secure communication.

Security is major issue on Ad-hoc network. In Ad-hoc network two types of attack one is active and another is passive attacks [2][3]. Active attacks like black hole attack, worm hole attack, Sybil attack, flooding attack, denial of service (DoS). A decentralized network is more open to that kind of attacks because communication is based on mutual trust between the nodes there is no authorization facility and limited resources etc. we are focus on mostly black hole attack. In black hole attack the malicious node drops all the data packets which reduce performance. There are three types of mobile Ad-hoc network. VANET (Vehicular ad-hoc network) are communication in inters vehicle. IVANET (An intelligent vehicular ad-hoc) is avoiding to vehicle collisions and accident etc. Iad-hoc network (Internet based mobile ad-hoc network) is ad-hoc network that interconnect specific internet gateway to mobile node.

The most important area of ad-hoc network is communicate vehicle to vehicle and ad-hoc networks can also be used for automated battle field and war games and resource operation, military, education commercial etc. ad-hoc networks are playing their role for connecting peoples.

Some disadvantages of ad-hoc networks are as follows, few resources, no central authentication on the network, scalability problems and dynamic topology. Ad-hoc network have many characteristics some are Dynamic topology: nodes are move free with different speed and network topology may change randomly, Energy constrained operation, Limited bandwidth, Security threats.

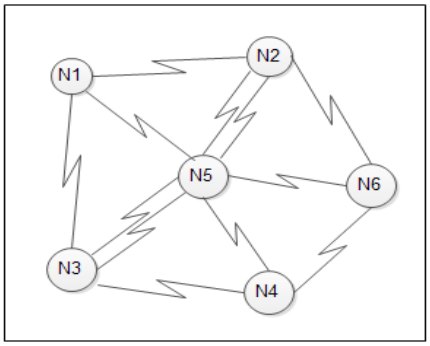


Fig.1. mobile ad-hoc network architecture

2. AODV ROUTING PROTOCOL:

The routing protocol play main role in identifying and packet transmit ion from source node to destination node, through intermediate nodes. Ad-hoc on demand distance vector routing (AODV) is a reactive routing protocol [4][5]. 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 messages which broad cast in the network can be divide into path discovery and path. AODV includes three messages route request (RREQ), rout reply (RREP) and another route error (RERR).

(a) RREQ:

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

Fig.2. RREQ

(b) RREP:

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

Fig.3. RREP

(c) RERR:

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. 2,3,4 and routing table related fields in Fig.5 .

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

Fig.5 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.

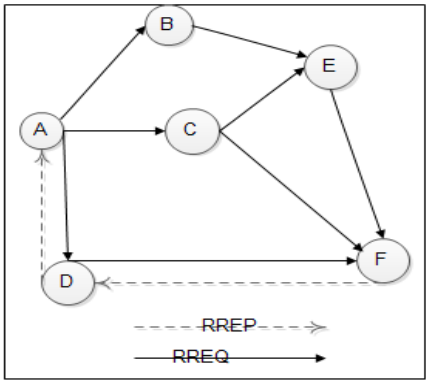


Fig.6

3. BLACK HOLE ATTACK:

Black hole attack is types of active attack in ad-hoc network in which malicious nodes receive during broad cast of RREQ message from source node and replay unicast of RREP message[6][7]. During replay packet RREP, malicious nodes send maximum sequence number compare to all neighbors' nodes and represent the best route of destination node, then source node send data packets through that nodes, and that nodes(malicious node) drop all packets this is called black hole attack.

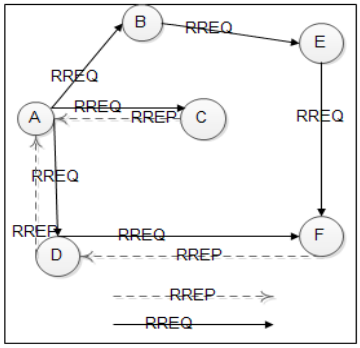


Fig.7

In Fig.7 assume A node is a source node, F node is destination node and C node is malicious node. When node A broad cast a RREQ message to all neighbor then node B, C and D receive it malicious node C RREP message with max sequence number compare all neighbor and claiming a route to destination. Source node A receive a RREP from node C ahead of the RREP B and D. then source node A assume to shortest route through node C and send all data packets to destination through node C but node C is drop all packets so it look like black hole attack.

4. TAODV ROUTING PROTOCOL

TAODV is a secure routing protocol based on trust model for mobile Ad-hoc network. TAODV has several salient features like Nodes perform trusted routing behaviors mainly according to the trust relationships among them. A node that performs malicious behaviors will eventually be detected and denied to the whole network. System performance is improved by avoiding generating and verifying digital signatures at every routing hop.

a) Trust Status 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.

I. **Unreliable:** The Unreliable is the non trusted node. Means a Unreliable 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.

II. **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.

III. **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.

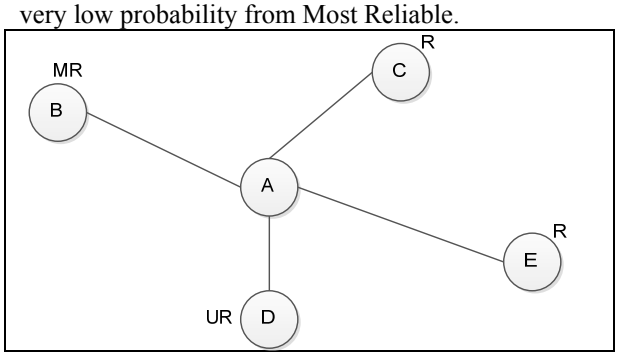


Fig 8

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.

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.

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

$$T = tanh\ (R1+R2)$$

Where

tanh is an hyperbolic tan function, which has value

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

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 updation of a node:

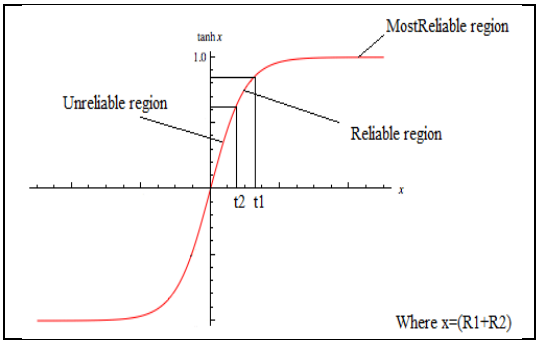
After receiving the RREP from all the neighbors, Source node check the trust status of neighbors and then decide the route. For updating the trust status we send **n** fake packets. In the basis of packet-processing we calculate the new trust status of the nodes and if it required then update it.

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 ≥ t1
A (node x → node y) = Reliable when t2 ≤ T < t1
A (node x → node y) =Unreliable when 0<T ≥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).

5. Simulation And Result

We performed a set of simulations based on *ns-2* with extensions for mobile wireless networks. To evaluate the performance of TAODV we have taken following simulation parameters in our simulation.

Simulation Parameters

Simulation Parameters	Value
Number of nodes	19
Network size	1100*1100
Simulation duration	50(Sec)
Initial Energy	100
txpower	0.9
repowers	0.8
Idle power	0.0
Sense power	0.0175
Source node	9
Destination node	8
Black Hole node	2
Packet size	1024
Node size	70

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

5.1 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 was investigated using simulations.

Times	Black Hole AODV (%)	Trusted AODV (%)
10 Sec	98.68	98.38
20 Sec	97.22	96.71
30 Sec	95.96	94.97
40 Sec	94.52	93.30
50 Sec	93.08	91.59

Compare Energy [Table 1]

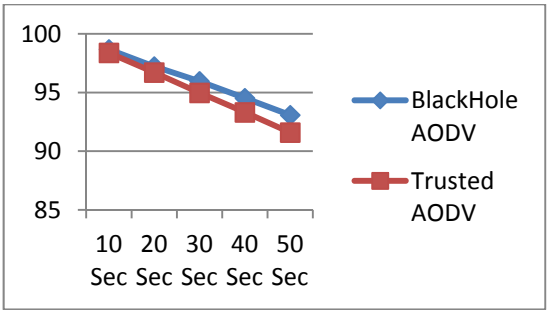


Fig. 9

5.2 Throughputs: Throughput is the average rate of successful message delivery over a communication channel.

Times	Black Hole AODV (%)	Trusted AODV (%)
10 Sec	8.80	80.16
20 Sec	8.51	79.48
30 Sec	7.97	79.08
40 Sec	6.93	78.25
50 Sec	2.36	78.27

Compare Generate Throughput [Table 2]

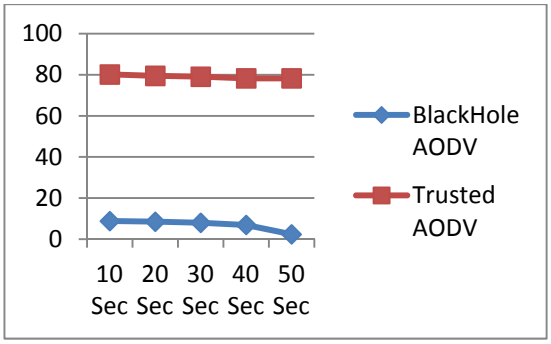


Fig .10

5.3 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.

Times	Black Hole AODV (%)	Trusted AODV (%)
10 Sec	1.17	38.17
20 Sec	4.35	45.11
30 Sec	5.28	54.68
40 Sec	5.85	61.94
50 Sec	6.21	69.21

Compare Packet Delivery Ratio [Table 3]

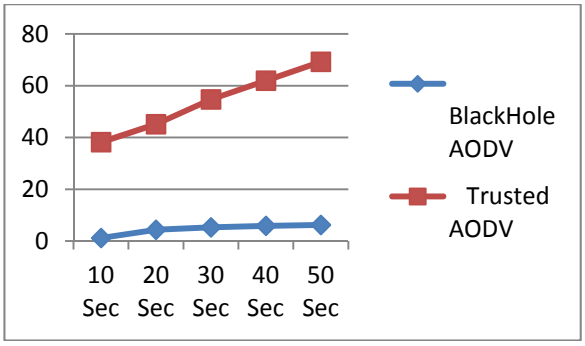


Fig .11

6. Conclusion:

By using simulation we find following conclusion**.** The energy of Black hole is more as compare to TAODV, when we increase the time the energy level of both is decrease. Throughput of TAODV is better compare to black hole AODV, by increasing the time a little bit effect in throughput in both the case. Packet delivery ration is better compare to black hole AODV, when we increase the time the packet deliver ratio of both is increase. As shown in fig.9-11. When we want more throughputs, more packet delivery ratio and less energy we use TAODV.

7. Future Work:

In this paper we have calculate trust value only on node level, by using different parameter and simulate by NS-2 tool. In future we will calculate trust value node as well as root level. We will also find out co-operative black hole attacks and compare the simulation result.

REFERENCES

[1] Mohit Kumar, Rashmi Mishra "An Overview of MANET: History, Challenges and Applications" Indian Journal of Computer Science and Engineering (IJCSE), ISSN: 0976-5166 Vol. 3 No. 1 Feb-Mar 2012.

[2] H. A. Esmaili, M. R. Khalili Shoja , Hossein gharaee "Performance Analysis of AODV under Black Hole Attack through Use of OPNET Simulator" , World of Computer Science and Information Technology Journal (WCSIT) ISSN: 2221-0741 Vol. 1, No. 2, 49-52, 2011

[3] Rajkumar Singh, "Ad-hoc On-Demand Distance Vector Protocol and Black Hole Attack in AODV" CS 399: Seminar, Term Paper, 10thApril 2012.

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

[5] IETF MANET Working Group AODV Draft, http://www.ietf.org/internet-drafts/draft-ietf-manet-aodv-08.txt, Dec 2002.

[6] Sowmya K.S, Rakesh T. and Deepthi P Hudedagaddi.,"Detection and Prevention of Blackhole Attack in MANET Using ACO". Proceedings IJCSNS International Journal of Computer Science and Network Security, VOL.12 No.5, May 2012 .

[7] Mohammad Al-Shurman and Seong-Moo Yoo, Seungjin Park, "Black hole Attack in Mobile Ad Hoc Networks" Proceedings of the 42nd annual Southeast regional conference ACM-SE 42, APRIL 2004, pp. 96-97.