An Approach of Detecting Black Hole Attack in MANET using Modified TAODV Protocol

Rashika Indoria
Department of Computer Science & Engineering
ITM University
Gwalior

Deepak Motwani
Department of Computer Science & Engineering
ITM University
Gwalior

ABSTRACT
A wireless ad hoc network is a network where nodes can communicate with each other without the support of infrastructure. It can be set up easily and quickly with low cost. The network is called ad-hoc because each node in the network is ready to forward the data for other nodes and so the decision of which nodes transfer the data is made dynamically based on the network connectivity. A Mobile Ad-Hoc Network is a bunch of collected free mobile nodes which can communicate to each other with the help of radio waves. This advantage makes these networks highly robust. There are so many attacks in mobile ad-hoc network but in this paper we focus on black hole attack. We have taken Trust based AODV routing protocol idea with the addition of Fuzzy Logic to focus on examine and improving the security of routing protocol for MANET. Our aim is to ensure the security of data packet against the black hole attacks. The throughput, packet delivery are used to determine the performance of AODV and TAODV. We are using Simulation tool on NS2, the throughput of Proposed TAODV is better as compare to Previous TAODV and Packet Delivery ratio is also better as compare to previous TAODV. .

Keywords
MANET, Black Hole Attack, Trust Based AODV Routing Protocol, Fuzzy Logic, Load.

1. INTRODUCTION
A wireless network is a growing technology that allows users to access data and information electronically, irrespective of their geographic position that means a host or a device can be moved, while communication, in defined area. The Wireless networks are divided into two categories; the first one is infrastructure based network and second is infrastructure less (ad hoc) networks. Infrastructure based network uses the fixed and predefined structured. In this Paper We focused on Infrastructure less network that is AD-HOC Network. A wireless ad hoc network is a network where nodes can communicate with each other without the support of infrastructure. It can be set up easily and quickly with low cost. A Mobile Ad-Hoc Network is a bunch of collected free mobile nodes which can communicate to each other with the help of radio waves. This advantage makes these networks highly robust. There are two types of attack in AD-HOC Network; one is active attack and second attack is passive attack. Active attacks are black holes, worm hole, flooding attack, denial of service. We are focused on Black Hole Attack in this paper. In black hole attack, a harmful node uses its routing protocol in order to broadcast itself for having the accurate and the shortest way to the destination node or to the packet it wants to stop.

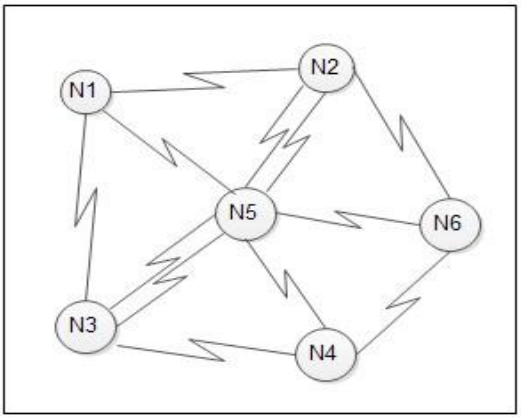

Fig.1. Mobile Ad-Hoc Network Architecture

2. AODV ROUTING PROTOCOL
AODV which is known as Ad-hoc on Demand Distance Vector routing protocol is a widely used routing protocol for mobile ad-hoc network (MANET). Ad-hoc On-demand distance vector (AODV) is a modified version of classical distance vector routing algorithm. AODV is a reactive routing protocol that means it establishes a route to a destination only on demand. AODV keep away from the counting-to-infinity problem of other distance-vector protocols by using sequence numbers on route updates, a technique pioneered by DSDV. AODV is competent of both unicast and multicast routing. In AODV, there are mainly three type of message is there. Route request (RREQ), rout reply (RREP), and Route error (RERR).

2.1 RREQ

Type	**Flags**	**Reserved**	**Hop count**
RREQ(Broadcast) id			
Destination IP address			
Destination sequence number			
Source IP address			
Source sequence number			

Fig.2. RREQ

2.2 RREP

Type	**A**	**Reserved**	**Hop count**
Destination IP address			
Destination sequence number			
Source IP address			
Source sequence number			

Fig.3. RREP

2.3 RERR

Type	N	Reserved	Destination count
Unreachable destination IP address			
Unreachable destination sequence number			
Additional unreachable destination IP			
Additional unreachable destination sequence			

Fig.4. RERR

Every mobile node in aodv maintains a routing table and updates the content field while receiving a routing message from the node. All the fields in the routing table related to these RREQ, RREP, and RERR shows in Fig. 2, 3, 4 and related routing table 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

In AODV protocol, the network is awaiting until a connection is required. At this stage the mobile node that requires a connection broadcasts a request for new connection. Other AODV nodes forward this requested message, and record the node that they heard it from, creating an explosion of temporary routes for replying back to the requested mobile node. When a mobile node gets such a message and already has a route to the desired node, it sends a message backwards through a temporary route to the requesting node. The required node then starts using the route which has the minimum number of hops through neighbor nodes. When a link fails, a routing error message is sent back to the requested mobile node, and the process repeats until desired operation is performed. In fig.6 shows the working of AODV routing algorithm.

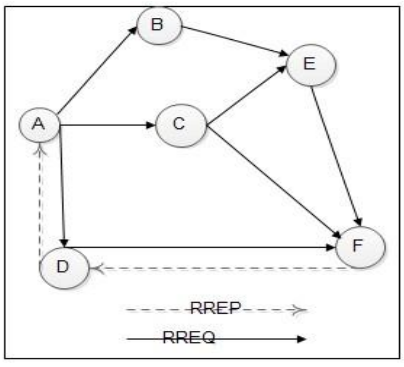

Fig.6.

3. BLACK HOLE ATTACK

Black holes is a type of networking attack where incoming and outgoing traffic is peacefully or silently discarded or dropped, without letting know the source that the data did not reach its planned receiver. A black hole problem means that one malicious node utilizes the routing protocol to claim itself of being the shortest path to the destination node, but drops the routing packets but does not forward packets to its neighbors. A single black hole attack is easily happened in the mobile ad hoc networks.

A black hole node pretends to have enough routes to all destinations requested by all the nodes and absorb the network traffic. When a source node transmit the RREQ message for any destination, the black hole node instantly responds with an RREP message that includes the highest sequence number and this message is recognize as if it is coming from the destination or from a node which has a fresh enough route to the destination. The source assumes that the destination is behind the black hole and discards the other RREP packets coming from other nodes. The source then starts to send out its data packets to the black hole trusting that these packets will reach the destination. A malicious node sends RREP messages without checking its routing table for a fresh route to a destination

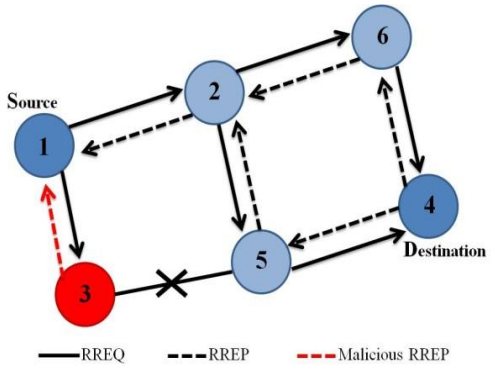

Fig.7.

4. LITERATURE SURVEY ON EXISTING TECHNIQUE

Ashish Sharma , Dinesh Bhuriya ,Upendra Singh , Sushma Singh The Author Proposed a different algorithm that is TAODV. The new Trust based AODV algorithm is used in this paper. The basic method which author proposed is the algorithm uses sequence number. This AODV algorithm includes three message- Route Request that is (RREQ), Route reply that is (RREP) and route error that is (RERR). This algorithm maintains routing table and keep on updating the table content field while recover a routing message. In this paper, author proposed three factor of TAODV algorithm that is unreliable node, reliable node and most reliable node. During these three phases, the route discovery will be there.

Neelam khemariya, Ajay khunteta. Author proposed an efficient approach which is for the detecting and removing of the black hole attack in the Manet describe. The proposed

Algorithm is implemented on aodv routing protocol. This algorithm can detect the single black hole attack and cooperative black hole attack. The beauty of the algorithm describe in this paper it is not only detect the black hole nodes in the case when the node is not non-functioning but it can also identify the black hole point in case when the point is not functioning. These two implementation made the approach very secure and efficient.

Jaspinder kaur, Birinder Singh proposed modification in traditional Aodv protocol to prevent black hole attack. The basic idea for this proposed work is to use of fake message that is using fake route request packets. The fake route request packets contain the IP Address of the node which doesn't exist in the network. As a result the malicious node will reply back this later is detected as the harmful node. The source

node get various available path are there, and the source node never select that path in which the node exist with the help of this technique we can easily detect the black hole attack in the network.

Manita, Vinay kumar Nassa, Mr. Kapil Chawel author proposed the modified Aodv protocol to handle the black hole attack and grey hole attack. This paper modifies the AODV Routing protocol by using ant Colony Optimization. This modified Aodv detect the black hole and grey hole attack and also recover from these attack. The packet delivery ratio is increased and this delay gets reduced and the throughput is also getting increased.

Manisha Sao, Sushil Kashyap, Dr.Vishnu kumar Mishra. The main motive of this research work is to improve the main advantage of this protocol that is routes are established on demand and destination sequence number are used to search out the newest route to the destination. In this paper author proposed a method which is called route discovery method. In this method basically the sender node broadcast the method to its neighbor so that the receiver node respond for this method but the sender node is not directly connected with the receiver node so that the neighbor of this node connects the sender to the receiver and then the RERP message forwarded by the receiver and all the sending of nodes are basically done by the sequence number. The AODV plays an important role in it.

Roopal Lakhwani, Sakshi Suhane, Anand Motwani proposed an agent based aodv protocol which includes both detecting and removing of black holes attacks. This paper describes the routing security issue of MANET and Black holes attacks. Author proposed a feasible solution for this in this protocol. In the Protocol "An Agent based AODV" is designed to achieve the objective. The Modification in this algorithm is adding Send Reply () function and RerReply () function which helps to detect the malicious nodes and stop them to participate in the network. This paper shows significant improvement in packet Delivery ratio of Aodv in presence of black hole attack.

5. TAODV ROUTING PROTOCOL AND PROPOSED WORK

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.

5.1 Trust Status of a Node

In this proposed work, we modified the AODV along with a factor known as TRUST which is later on known as Trust based AODV. The communication between the nodes depends on the trust level of the node with its neighbor. The whole process of communication and transfer of data packets depends on the trust value. We categorize these nodes in three types. They are as follows:

5.1.1 Unreliable

The non trusted node is called unreliable which means node which has minimum or Zero trust level. That node who joins the network or who is the initiator for the transfer of data packet is treated as unreliable.

5.1.2 Reliable

Reliable nodes are those nodes which have the trust level between the unreliable node and reliable node. That means a node is said to be reliable which has received some data packets through that node.

5.1.3 Most Reliable

Most trusted nodes are most reliable nodes or in other words nodes which have the maximum trust value or trust level can be treated as most reliable. In this trust logic, higher trust level means nodes are receiving or transferring maximum packets successfully through this particular node.

In our proposed method, we have taken traffic or we can say Load factor because in our previous work, we got to know that the trust value of nodes are minimum that means nodes are unreliable. We thought it was because of that malicious node of black hole which is dropping the packet and data is not received by the receiver by the receiver but in our proposed work, we have one new reason for the minimum trust value of the node that is Traffic or simply we can say Load in the network. This possibility is also there that due to the high traffic in the network, data packets are not able to receive by the receiver. For this new idea, we are using fuzzy logic in our proposed idea because with the help of fuzzy logic we don't have to look for the formulas or equation, the whole process will be calculated in -1 to +1.

Considering the attacker has the property to attract the network traffic and drop it. The proposed algorithm utilizes this behavior for detecting the avoiding the paths through such nodes.

Step 1: let the node S wants to send a packet to D and an attacker A.

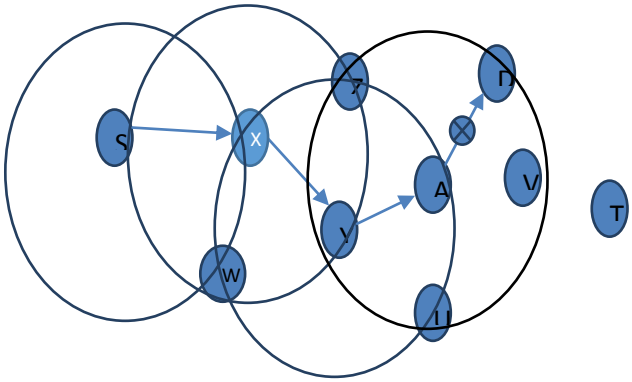

Fig.8.

Step 2: As shown in figure it's clear that even the source S is transmitting to D via "X,Y,A" the transmission of S to X can also be received as node W and the transmission of the X to Y is also received on W and Z.

Step 3: Now if the nodes are normally behaving they should forward the packets to next node until the destination reached, hence when the node W receives the transmission from S it waits to hear the re-transmission from X also. If it doesn't it assumes that the node X is misbehaving and dropping the packets however this may not be true if the node moves out of the W's receiving range or is not able to transmit the packet due to higher network load.

Step 4: Hence every time the node observes the transmission by neighbor's node as forwarder of data packet (not

originator) it believes that the node is not malicious and it increments the local trust (LT) value for that node.

Step 5: now when a node receives the RREQ or RREP from other node it performs as

Let *LT* is its Local Trust Table and it contains the local trust values (LT_{val}) of n different nodes.

$LT_{val,\ i}$ = Local Trust value of i^{th} node where $1 \leq I \leq n$.

LT_{max} =max (LT_{val}), maximum trust value in the LT

LT_{min} =min (LT_{val}), minimum trust value in the LT

Then the normalized (rescaled, -1 to +1) local trust can be given as:

$$LT_{val,i}^{norm} = 2 * \left(\frac{LT_{val,i} - LT_{min}}{LT_{max} - LT_{min}}\right) - 1$$

Now each nodes estimate the network load as follows:

NL=Network Load calculated by i^{th} node where $1 \leq I \leq n$.

Pkt_{data} = Number of data packets received by i_{th} node

Pk_{rreq} =Number of routing packets received by i^{th} node

$NL_{max=}$Maximum Network Load

$NL_{min=}$Minimum Network Load

$$NL = \frac{Pkt_{rreq}}{Pkt_{data}}$$

Then the normalized (rescaled, -1 to +1) local trust can be given as:

$$NL^{norm} = 2 * \left(\frac{NL - NL_{min}}{NL_{max} - NL_{min}}\right) - 1$$

Let it receives the RREQ or RREP from m^{th} node

It checks the normalized local trust values for m^{th} node and normalized network load (NL^{norm})

After that it calculates the final for m^{th} node according to fuzzy Rules:

$LT_{val,m}^{norm}$	NL^{norm} =>	*Negative*	*Zero*	*Positive*
Negative		*Low*	*Low*	*Med*
Zero		*Low*	*Med*	*Med*
Positive		*High*	*High*	*High*

$$trust_m^{final} = fuzzyLogic\left(LT_{val,m}^{norm}, NL^{norm}\right)$$

The value of trust_mˆfinal decides whether to forward/receive/reply/response the packet or drops it. This is the formula for the calculation of Trust value of the nodes.

6. SIMULATION RESULT

In our proposed work, we performed simulation based on NS2 with the extensions for mobile wireless network. We have taken some simulations parameters in our simulations to evaluate the performance of TAODV.

Simulation Parameters

Simulation Parameters	Value
Number of nodes	50
Simulation duration	500ms
Routing Protocol	AODV
Propagation Model	Radio Mode
MAC	MAC Type

We have compared the Average Delay, Throughput, Packet Delivery ratio of Black hole AODV and TAODV which shows as follows:

Average Delay: The delay of a network which explain how long it takes for a bit of data to travel across the network from one node or endpoint to another.

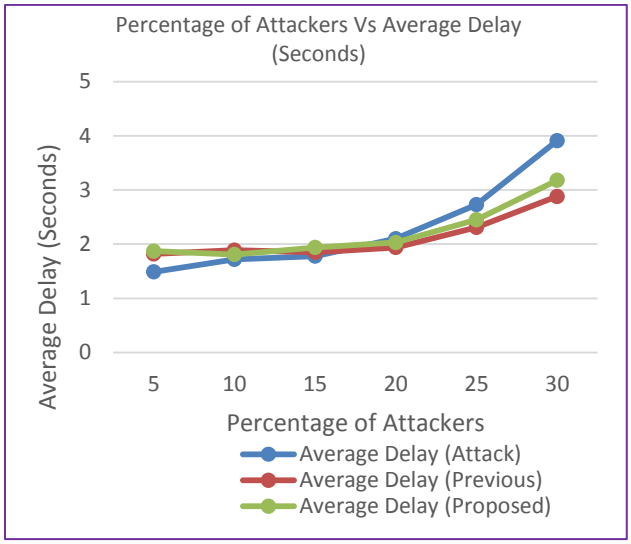

Fig.9

Throughputs: In networking Throughput is how many parts of data a system can process in a given amount of time or we can say the amount of data transferred from one place to another or processed in a specified amount of time.

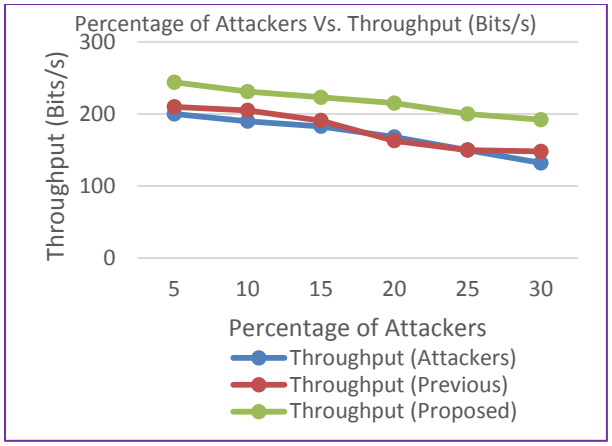

Fig.10

Packet Delivery Ratio: Packet ratio that are successfully delivered to a destination as compared to the number of packets that have been sent out by the sender. The greater value of packet delivery ratio means the better performance of the protocol.

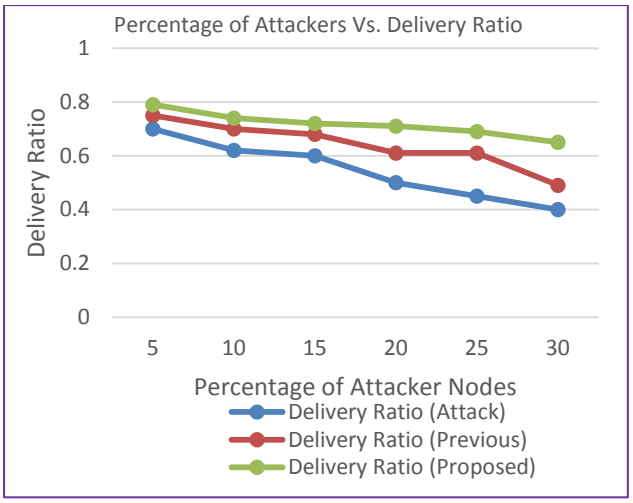

Fig.11

7. CONCLUSION

After completion the simulation the result will be like this. The throughput of proposed work is more as compared to previous work that means the delivery of data packets are successful. Packet Delivery ratio is better compare to previous. As shown in fig.9-11.when we want maximum throughput, more delivery ratio and less delay then we will use this modified TAODV.We find this following conclusion after using this proposed TAODV.

8. FUTURE WORK

We have calculated the trust value only on node level in this paper by using different parameter and simulate by NS2 tool. In future we can calculate trust value node as well root level.

9. REFERENCES

[1] Tameem Eissa & Shukor Abdul Razak & Rashid Hafeez Khokhar & Normalia Samian "Trust-Based Routing Mechanism in MANET: Design and Implementation" Springer Science+Business Media, LLC 2011.

[2] J Jan von Mulert, Ian Welch , Winston K.G. Seah "Security Threats and Solutions in MANETs: A Case Study using AODV and SAODV" Elsevier 2012.

[3] Mohamed Amnai, Youssef Fakhri, Jaafar Abouchabaka, "Evaluation of Impact of Traffic VBR and Mobility on the Performance of AODV Routing Protocols in Mobile Ad hoc Networks", IEEE, 2010.

[4] Mariannne. A. Azer, "Wormhole Attacks Mitigation in Ad Hoc Networks", IEEE 2011, pp 561-568.

[5] Mohamed Amnai, Youssef Fakhri, Jaafar Abouchabaka, "Evaluation of Impact of Traffic VBR and Mobility on the Performance of AODV Routing Protocols in Mobile Ad hoc Networks", IEEE, 2010

[6] Jayanta Biswas, Mukti Baraiand, and S.K.Nandy "Efficient Hybrid Multicast Routing Protocol for Ad-Hoc Wireless Networks" IEEE.

[7] Ashish Sharma , Dinesh Bhuriya ,Upendra Singh , Sushma Singh" Prevention of Black Hole Attack in AODV Routing Algorithm of MANET Using Trust Based Computing" in International Journal of Computer Science and Information Technologies, Vol. 5 (4) , 2014.

[8] Subash Chandra Mandhata, and Dr.Surya Narayan Patro", "A counter measure to Black hole attack on AODV- based Mobile Ad-Hoc Networks", IJCCT, 2011

[9] Iman Zangeneh, Sedigheh Navaezadeh, Abolfazl Jafari, "Presenting a New Method for Detection and Prevention of Single Black Holes Attack in AODV Protocol in Wireless Ad Hoc Network", in International Journal of Computer Applications Technology and Research Volume 2– Issue 6, 686 - 689, 2013.

[10] Jaspinder Kaur,Birinder Singh, "Detect and Isolate Black Hole Attack in MANET using AODV Protocol," in International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 3, Issue 2, February 2014.

[11] Neelam Khemariya, Ajay Khuntetha,"An Efficient Algorithm for Detection of Blackhole Attack in AODV based MANETs"in International Journal of Computer Applications (0975 – 8887) Volume 66– No.18, March 2013.

[12] Muneer Bani Yassein, Yaser Khamayseh, Bahaa Nawafleh, "Improved AODV Protocol to Detect and Avoid Black Hole Nodes in MANETs,"in The Sixth International Conference on Future Computational Technologies and Applications.

[13] Roopal Lakhwani, Sakshi Suhane,Anand Motwani, "Agent based AODV Protocol to Detect and Remove Black Hole Attacks," in International Journal of Computer Applications (0975 – 8887) Volume 59– No.8, December 2012.