International Journal for Rapid Research in Engineering Technology & Applied Science
Vol 4 Issue 8 August 2018
ISSN (Online): 2455-4723

Weight based Trust Approach against Black-hole Attack Detection

Monika Labana*, Mohit Jain**

Computer Science and Engineering, RGPV, INDORE - 452001, Madhya Pradesh, INDIA*

monica.it1990@gmail.com,bmctmohitcs@gmail.com***

Abstract- **The fast growth of mobile communication in recent years is especially observed in the field of mobile system, wireless local area network, and ubiquitous computing. Security is a main concern for protected communication between mobile nodes in an unfriendly environment. In hostile environments adversaries can bunch active and passive attacks against intercept able routing in embed in routing message and data packets. Ad hoc networks use mobile nodes to enable communication outside wireless transmission range. Attacks on ad hoc network routing protocols disrupt network performance and reliability. MANET has no clear line of defense, so, it is accessible to both legitimate network users and malicious attackers.The issues rise when the nodes are mobile and poor routing techniques allow a user to change or modify the information during data transmission because, during network communication the data is transmitted through the intermediate routers where any node can leave or join the network any time. Black-hole is one of the severe security threats in ad-hoc networks which can be easily employed by exploiting vulnerability of on-demand routing protocols. In this research work we proposed weight based trust approach against black-hole attack. In this approach we compute weight of all network nodes on the basis of threshold computation. Implementation is performed in NS2 environment and results are provided to demonstrate the effectiveness of our approach, using the packet delivery ratio, Network throughput, remain energy and end to end delay, as performance factors.**

Keywords: *Mobile ad-hoc Networks, Black-hole, NS2, AODV, Routing Protocol, Mobile nodes, RREQ, RREP*

I. INTRODUCTION

In recent years, the explosive growth of mobile computing devices, which mainly include laptops, personal digital assistants (PDAs) and handheld digital devices, has impelled a revolutionary change in the computing world: computing will not merely rely on the capability provided by the personal computers, and the concept of ubiquitous computing emerges and becomes one of the research hotspots in the computer science society. The Mobile Ad Hoc Network is one of the wireless networks that have attracted most concentrations from many researchers. In ad hoc networks the communicating nodes do not necessarily rely on a fixed infrastructure, which sets new challenges for the necessary security architecture they apply. In addition, as ad hoc networks are often designed for specific environments and may have to operate with full availability even in difficult conditions, security solutions applied in more traditional networks may not directly be suitable for protecting them. In concern of network security different attack harm the privacy of system gradually. One of the most popular and serious attacks in wireless ad hoc networks is Denial of Service attack and most proposed protocols to defend against this attack used positioning devices, synchronized clocks, or directional antennas.

Therefore the proposed work is dedicated to find the solution for mobile ad hoc network based routing attack. During investigation a number of different routing attacks are establish persons are much regularly deploy in network and hard to recover. Thus Black-hole attack is selected for investigation and solution development.

II. PROPOSED WORK

The given solution is based on the weight based trust methodology, which includes the mathematical formulation to resolve attack free network where system performance enhance as compared to other trust model. This methodology comprises with different perspective where we can summarize overall solution with following points. In this section, we introduced model to estimate the trust of the approach by finding different Thresholding factors.

1. **Initiate Network**
2. **Parameter Assignment**
3. **Algorithm formulation**

1. Initiate Network:

For securing network, the proposed algorithm is developing using different constraint. So that we basically we need to assume some constraints to progress further. For this we need to establish an idle network for demonstrating the concept, firstly we create a normal network where with different number of network e.g. 20, 40, 60, 80, 100, 125 and 150.

Initialize the Network, with N nodes where$N = 1, 2, 3, \ldots\ldots$,, in ideal condition

S initiates a RREQ message with the following components:

– The IP addresses of S and D

– The current sequence number of S and the last known sequence number of D

– A broadcast ID from S. This broadcast ID is incremented each time S sends a RREQ message.

The pair of the source S forms a unique identifier for the RREQ.

For route discovery, we process a route request RREQ to all other node except the node which is generating request. Therefore, source node wait for the route reply i.e. RREP which is coming from that node to its match broadcast ID and IP address.

Secondly, for processing proposed method, we use some networking different factors to process the algorithm from this we get the efficient output that outlines the secured network. In next point we assume some checking constraints which are used to build algorithm.

2. Assigning Parameter

In this section we describe assigned parameter need to process the proposed approach by we construct the algorithm

Network Node Energy: Node energy of a node indicates how the network is efficient and long life of the node in entire working network session. Energy less than a predefined average can affect the normal functioning of network. Therefore in order to serve the network longer it is required the cluster head node has the sufficient energy level. According to the definition of energy consumption the difference of two time based energy level is used for computing the energy consumption rate which is used for threshold computation. Thus suppose at time t_1 the node have the energy $E_I$and after a time difference Δt the new energy level becomesE_c at timet_2.

$$\Delta E = E_I - E_c \text{ ------- eq. (1)}$$

Buffer Length: In network processes the connected nodes are communicating each other using a fixed length of memory unit. This memory unit is known as the buffer of node. The buffer is basically holding the received and communicated data. Therefore to identify a node is busy or not the buffer length is measured. If buffer of node is a consumed mean full it means a node in a high processing load or suffers from congestion thus the node which having less filled buffer can serve better due to low work load. Therefore buffer length measurement is measurement of node work load. This here for the length of buffer the letter B is used and can be computed using given formula:

$$\Delta B = B_I - B_c \text{ ------- eq. (2)}$$

Where, B_I is initial buffer length and B_c is used or consumed buffer.

Packet Drop: Packet drop is the failure of one or more transmitted packets to arrive at their destination. The total number of packets dropped during the simulation is termed as the packet drop ratio. It can be also termed as the difference between the total number of packets send and the total number of packets received. Therefore, we can calculate dropped packet whenever network performance degraded. Following are the formula by which can estimate dropped packet:

$$P_{drop} = P_{send\ time} - P_{receive\ time} \text{ ------ } - \text{ eq. (3)}$$

By using following equation (1), (2) and (3), now we calculate threshold values for each equation and introduce also compute weight total weight using above parameters.

3. Formulate Algorithm

The proposed work is indented to secure network, therefore the AODV based routing protocol is modified to identify the malicious node in the network among the available routes between source and destination. Table 1 and 2 demonstrate the entire process of algorithmic calculation in a short summary:

Table 1: Threshold Computation

Input: Number of Nodes NN;
Output: Threshold Computation;

Process:

1. Populate Random mobile nodes in network;
2. A node in network broadcast route discovery request;
3. Wait for response generated by network;
4. Employee different Parameters
   i. Node Energy
   ii. Node Buffer Length
   iii. Packet Drop
5. For each node routing in routing table:
6. Assume buffer length for each node, B_i where $i = 1, 2, \ldots . n$ and buffer length of one node can be found by given equation,
   $\Delta B = B_I - B_c$
7. Buffer average of all node:

$$\alpha = \frac{1}{N}\sum_{i=1}^{n} \Delta B_i$$

8. Assume packet drop of each node during simulation scene $drop_i$ where $i = 1, 2, \ldots . n$ and packet drop can be compute using given equation,
   $P_{drop} = P_{send\ time} - P_{receive\ time}$
9. Average threshold of Packet Drops for each node:

$$\beta = \frac{1}{N}\sum_{i=0}^{n} P_{drop_i}$$

10. Assume node energy of each node, E_i where $i = 1, 2, \ldots . n$ and node can be compute using given equation,
    $\Delta E = E_I - E_c$
11. Average Threshold value of energy for each node

$$\gamma = \frac{1}{N}\sum_{i=1}^{n} \Delta E_i$$

12. Transmit the α, β, γ to the whole network

Description: The black hole attack is one of the well-known security threats in wireless mobile ad hoc network. Hence, the black-hole attack is severe threat that capture packet and drop by advertising shortest path. In our proposed algorithm, threshold detection is calculated using difference parameters i.e. node energy, buffer length and packet drop.

In table 1, we describe each steps of threshold calculation. In this algorithm, firstly, we have dispersed mobile nodes randomly in network. In this scenario, one source node broadcast route request in the form of packet i.e. RREQ. The RREQ packet contains different field like Source IP address, destination IP address, Broadcast ID, TTL values etc. This request reaches to every node excluding source node. As soon as request arrives to every node, then one node send reply as form of packet RREP. This reply is unicast that send by the packet field matched to destination node. Once, a route established, we can start communication between sources to destination via sending and receiving packets. These all are function are performed using modification of AODV routing protocol. After this process, we move to find threshold value of different nodes. This process is the initial process of finding malicious node in network.

Now, we calculate different factor values, on which basis we initiate the process of finding malicious nodes. Networks have the property where every node join or leave the network frequently whenever the network topology is changed. We calculated the node energy, buffer length and dropped packet by putting the values in build up formula. After calculation of the factor values after we find out the average value of all nodes by summation of all node dividing by number of nodes. These average values are broadcast to entire network.

Table 2: Weight Computation and attack detection

Input: Number of Nodes NN;

Output: Trusted Node;

Process:

1. Perform Normalization between 0 to 1 of the each node in network
2. For each routing found list of suspected node
3. **if** $(\alpha < \Delta B_i \&\& \gamma < \Delta E_i \&\& P_{drop_i} > \beta)$

   Suspected Node List

   else (no suspected list)

4. **endif**
5. Estimate whole weight of all Suspected Nodes using normalized value
   $W = (0.25) * \alpha + (0.5) * \beta + (0.25) * \gamma$
6. Calculate Average trust weight of all Nodes

7. Assume trust weight of each node W_j where $j = 1, 2, \ldots . n$ and average trust using weight can be compute using given equation,

$$\emptyset_w = \frac{1}{N}\sum_{j=1}^{n} W_j$$

8. for finding availability of attacker node
9. **if**$(\emptyset_w > weight\_node_{(i)})$

Malicious Nod

else

trusted Node

10:endif

III. IMPLEMENTATION

The simulation is being implemented in the Network simulator. Protocol used here is AODV.

This section provides the understanding about the simulation scenarios under which the experiments are performed. To demonstrate the security technique their two key simulation scenarios are proposed in this section. Both the simulation scenarios are conducted with different number of nodes that are 20, 40, 60, 80, 100, 125 and 150 nodes for both attacks.

In order to perform the experiments here we show simulation scenario of 20 node script of proposed and normal approach with their description in given figure 4.2 and 3.

1. Simulation when Black-hole is deployed: In this simulation, the network is configured when the attacker node is deployed with modification of AODV routing protocol. To comprise the network visualization the malevolent node is deployed in network and the network presentation is animated on the basis of the network trace file. The normal network nodes are illustrated using the green color and the malicious attacker is established shown in given in figure 1. In this configuration an attacker continuously drop the packets instead of forwarding them to the next hop; hence major amount of packets is dropped during attack deployed. In this situation Communication is happened between source node***9***and destination node ***18***.

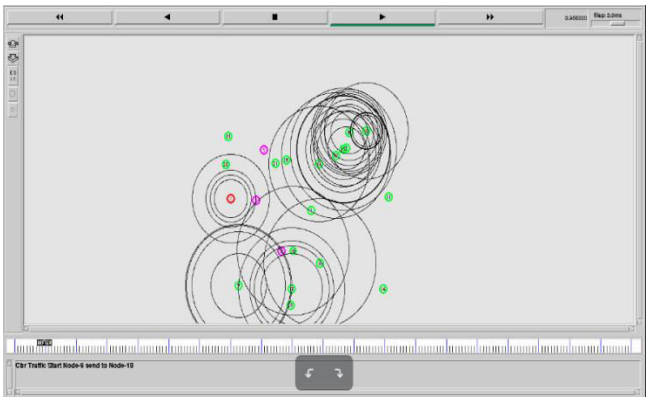

Figure 1: Simulation of Black-hole Attack under AODV Routing

2. Simulation using the Proposed Trust based Routing Technique*:* In this simulation scenario the proposed routing method which is developed with the help of AODV routing modifications are implemented using MANET environment. In this state we can't remove attacker node because this node is also a part of our network configuration. Therefore our aims to ignore/avoid the entire attacker node which is drop packets. The deployed attacker is normalized using the technique and their performance is estimated on the basis of the network trace files. The figure 2 demonstrates the simulation screen of the proposed secure routing technique for Black-hole Attack prevention.

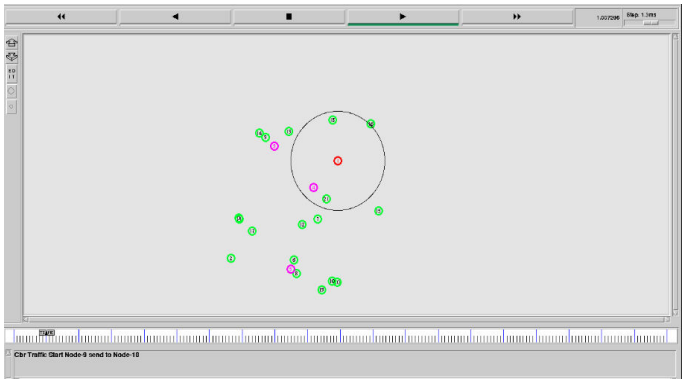

Figure 2: Simulation of Proposed Method under Improved AODV

Table 3: Simulation Scenarios

Parameters	*Values*
Antenna Model	Omni Antenna

Dimension	1000X1000
Radio-Propagation	Two Ray Ground
Channel Type	Wireless Channel
Traffic Model	CBR
Routing Protocol	AODV
Mobility Model	Random Waypoint

IV. RESULT AND DISCUSSION

This chapter provides the detail discussion about the obtained results and their obtained performance. In order to compute the performance of the proposed routing technique the different experiments on 20, 40, 60, 80, 100, 125 and 150 nodes are performed. Additionally the measured mean performance of the routing protocols is defined.

5.1End to End delay

End to end delay is the time taken by a packet to travel from source to destination. Delay depends on number of hops and congestion on the network. End-to-end delay of data packets includes all possible delays caused by buffering during route discovery, queuing at interface queue, retransmission delays at MAC layer, propagation and transfer time:

$$\text{E2E Delay} = \text{Receiving Time } (R_t) - \text{ Sending Time}(S_t)$$

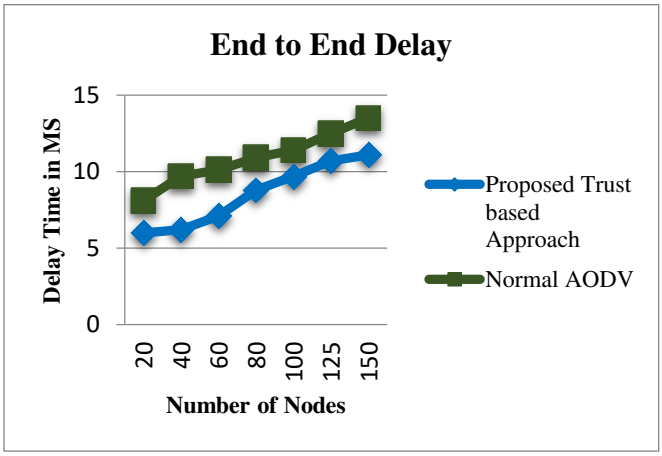

Figure 3 End to End Delays

Figure 3 shows the comparative End to End Delay when black-hole attack is deployed and the proposed trust based approach. In this figure the X axis contains different number of nodes and the Y axis shows the performance of network in terms of milliseconds. According to the formed results the proposed technique is minimized delay time during packet transmission as compared to black-hole attack which increase delay time for packet transmission. Form this graph we can conclude as if numbers of nodes are increases in a respective manner whenever delay time increase simultaneously for the comparison.

5.2 Packet Delivery Ratio

Packet delivery ratio is defined as the ratio of data packets received by the destinations which is generated by the sources. Mathematically, it can be defined as:

$$\text{Packet Delivery Ratio (PDR)} = \frac{S_1}{S_2} \text{X100}$$

Here, S_1 is the sum of data packets received by the each destination and S_2 is the sum of data packets generated by the source node. Graphs show the fraction of data packets that are successfully delivered during PDR versus the number of nodes.

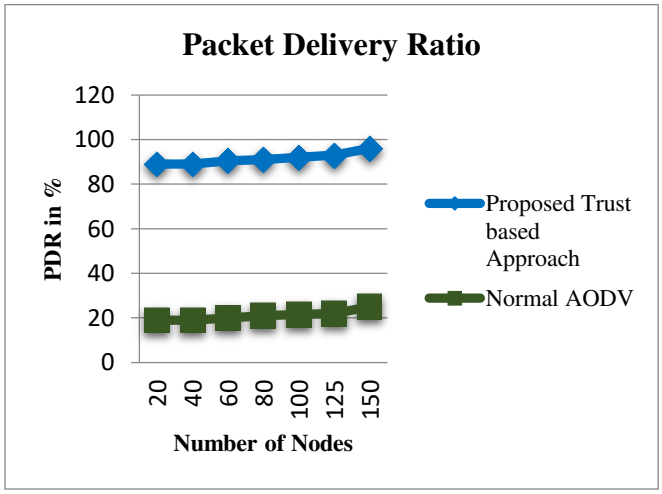

Figure 4 Packet Delivery Ratios

The comparative packet delivery ratio of the networks is given using figure 4, in this figure the X-axis shows the number of nodes for simulation in the network and the Y-axis shows the amount of packets successfully delivered to the destination in terms of the percentage. Additionally, green line shows that attacking performance on normal AODV and blue line show that proposed approach

performance. Proposed approach truly delivered high number of packet and similar that attacker node decrease the PDR performance that means most of the packet consumed continuously by the attacker node.

5.3 Throughput

It is defined as the total number of packets delivered over the total simulation scenario. This data may be delivered over a physical or logical link, or pass through convinced network nodes. The throughput is usually measured in bits per second (bit/s or bps), and sometimes in data packets per second or data packets per time slot.

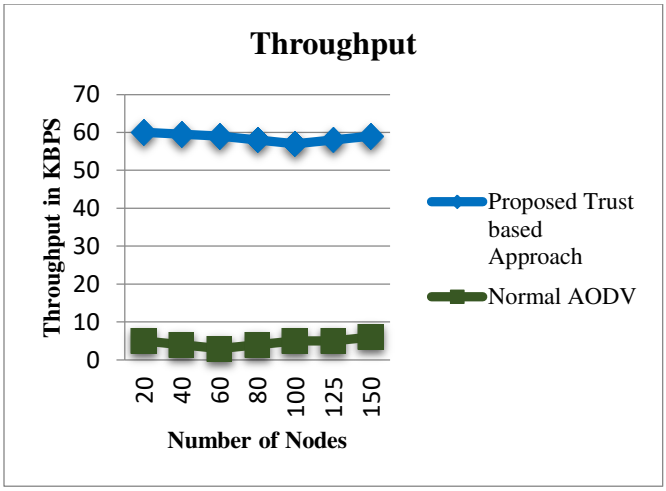

Figure 5: Compare Throughput

The comparative throughput of the network is demonstrated using figure 5, in this diagram different number of node demonstrated in X-axis and the Y axis shows the throughput performance in KBPS. The blue line of the graph shows the performance of the proposed trust based approach and green line shows the performance of the normal AODV based black-hole attack condition. According to results the proposed technique improve the throughput of the network during the attack conditions also therefore the approach is effectively avoid the attack effect as if there are number of attacker nodes are increased.

5.4 Remain Energy

The amount of energy consumed during the network events is termed as the energy consumption or the energy drop of the network. In networking for each individual event a significant amount of energy is consumed. The given figure 6 shows the energy level of all nodes

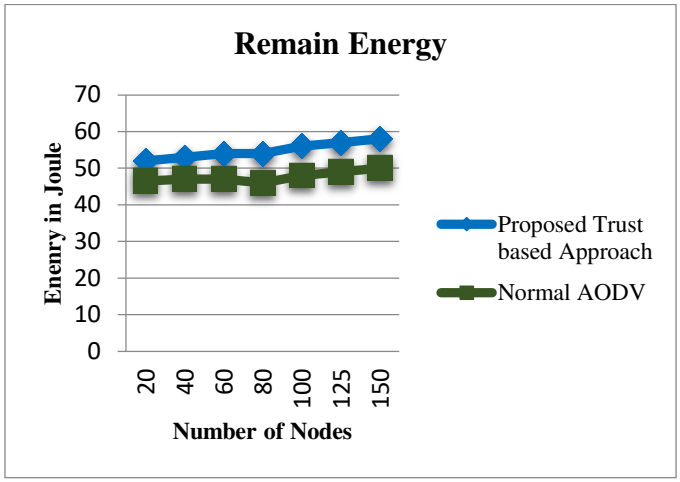

Figure 6 Remain Energy for Black-hole Attack

Figure 5.4 shows remain energy of the network for both simulation scenarios. The blue line of the diagram shows the amount of energy remains during communication events for attacking condition under AODV routing protocol. Additionally the blue line depicts the amount of remain energy and green line depicts black-hole attack simulation. In the Attack condition the network energy is frequently consumed as compared to the proposed routing protocol because the Black-hole attacks targeting the network by dropping the legitimate packets of the network. Therefore the proposed technique is effective and able to recover the network from the attack situations.

V. CONCLUSION

MANETs require a reliable, efficient, and scalable most importantly, a secure protocol as they are highly insecure, self-organizing, rapidly deployed and they use dynamic routing. The mobile ad hoc network is one of the most popular network technologies now in these days. In this paper, Black-hole attack is targeted for the investigation and research study. In black hole attack attacker node capture the packets and drop without forwarding them. Due to this behavior it is very complicated for the network to figure out this attack. Therefore, we proposed a secure routing algorithm which is based on different factor by we find specific value. From this value we use each node weight and found average value which will make the decision for malicious attacker behaviour. Therefore final checks show the availability of black-hole nodes. For configure the proposed concept we have modified AODV protocol for processing of work.

REFERENCES

[1] Priyanka Goyal, SahilBatra and Ajit Singh, "A Literature Review of Security Attack in Mobile Ad-hoc Networks", International Journal of Computer Applications, Volume 9– No.12, November 2010.

[2] KhushbooSawant and Dr. M.K Rawat, "Survey of DOS Flooding Attacks over MANET Environment", International Journal of Engineering Research and Applications, Volume 4, Issue 5, Version 6, PP.110-115, May 2014.

[3] S. A. Ade and P. A. Tijare, "Performance Comparison of AODV, DSDV, OLSR and DSR Routing Protocols in Mobile Ad-Hoc Networks", International Journal of Information Technology and Knowledge Management, Volume 2, No. 2, pp. 545-548, July - December 2010

[4] Nikhil Kumar, Vishant Kumar and Nitin Kumar, "Comparative Study of Reactive Routing Protocols AODV and DSR for Mobile Ad hoc Networks", International Journal of Computer Science and Information Technologies (IJCSIT), Volume 5, pp.6888-6891, 2014.

[5] M. S. karthikeyan, K. Angayarkanni, and Dr. S. Sujatha, "Throughput Enhancement in Scalable MANETs using Proactive and Reactive Routing Protocols", In Proceedings of the International Multi Conference of engineering and computer science, Volume 2, March 2010.

[6] Dokurer, S., Erten, M. Y., Akar, E. C., Performance analysis of ad-hoc networks under black hole attacks. InIEEE Southeast Con, pp. 148-- 153, Richmond, USA (2007).