International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

A MANET Security Using Routing Methodology

Shirsty Chandel[1], Prof. Ashish Tiwari[2]

[1]Computer Science & Engineering Department, Rajiv Gandhi Technical University, Airport Road, Gandhi Nagar Bhopal-462 033, India
[2]Vindhya Institute of Technology and Science, Umrikheda, Khandwa Road, Indore (M.P.), India

Abstract: ***Wireless networks are growing now in these days and different kind of wireless applications are developed using ad hoc configuration. Mobile ad hoc network is a kind of such wireless network. Due to its ad hoc nature and mobility support the routing protocol played essential role in network. The main responsibility of routing protocol is to create and maintain topology on demand basis. Therefore the ad hoc network is suffers from performance and security issues. Therefore the proposed study investigates the routing protocols supported by mobile ad hoc network and the routing based attack deployment techniques. After analysing them a solution for black hole attack security is provided. The proposed solution involves the implementation of secure route discovery protocol. In order to implement the proposed routing technique traditional AODV routing protocol is modified. The routing protocol is modified in such ways by which the routing path trust value is evaluated and compared for making a decision for malicious path detection. For creating the decisional threshold packet delivery ratio, energy and high sequence number is selected. The implementation and simulation of the proposed routing protocol is performed using network simulator 2. In addition of that the comparative performance study between AODV routing protocol and modified AODV routing protocol is performed. In the comparative study packet delivery ratio and throughput of network is found optimum and better than traditional routing protocol.***

Keywords: MANET, Black hole attack, MAC, AODV, QOS, NS2, Packet delivery ratio

1. Introduction

Mobile ad hoc is a popular communication network in research and development. Due ad hoc nature the main responsibility of data transmission and topology formation is depends on the routing technique. Therefore a number of different kinds of routing protocols are supportable in network. AODV is one of the most popular routing protocols in ad hoc network. The AODV routing protocol is an on demand vector routing protocol. According to the AODV routing strategy it does not collect the routing information periodically. This discovers path on demand basis. Therefore whenever a sender wants to send data to a target node the route discovery process is initiated. During this process first the source router broadcast a RREQ (route request) packet and when the RREQ packet riches to the target node. The target node sends the RREP (route reply) message to the sender. Source node receives the route reply from different routes and the routing table is updated. The first path is routing table is preferred for the routing purpose.

On the other hand when a malicious node deployed in network the malicious node start advertise, and promising to have the shortest path for the target node. The source router starts sending through the available shortest path. This leads the drop of all the data, thus performance of the network is degraded significantly.

Thus in order to detect the attack deployment and preserve the network performance a new routing protocol is introduced. The proposed routing technique usages the highest sequence number, remaining energy and packet delivery ratio for locating the malicious node. The utilization of the given network parameters using the routing protocol is reported in further sections.

2. Proposed Work

The mobile ad hoc network supports a number of different routing protocols. These protocols are used for finding the optimum route between source and destination. During study there are OLSR, AODV, DSDV and DSR routing protocols are found which frequently used in MANET simulation. In order to implement the proposed solution the AODV routing protocol is suggested to analyse. The AODV routing is an on demand vector routing protocol which find route when necessary. Additionally the routing protocol has higher performance over the studied routing algorithm.

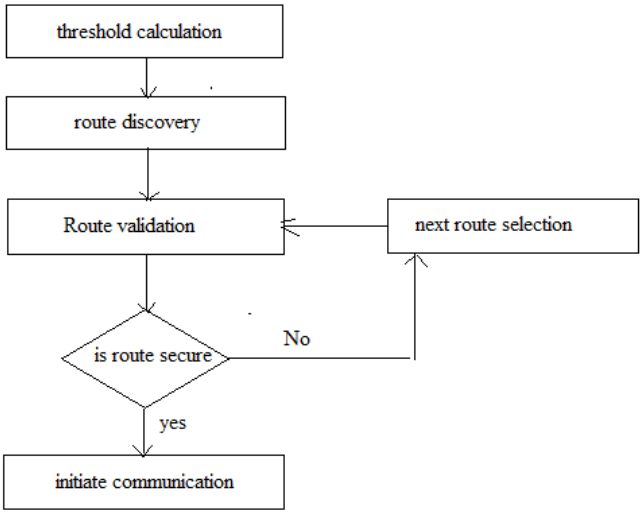

Figure 1: Proposed Routing Methodology

The proposed routing protocol is an extension of the traditional routing protocol, thus some of the properties of traditional routing is utilized. In addition of that some new properties are added to the newer routing protocol. Therefore the proposed system is works on the basis of the given figure. According to the above given diagram first the routing

protocol compute the threshold values and then the route discovery is performed. These threshold values are estimated in normal network conditions when malicious node is not present in network. Thus using different communication sessions the threshold values are calculated to make decisions of secure routing path discovery. The proposed routing protocol is waiting till the entire possible path among source and destination is not discovered. In other words the source waits for the replies from all the neighbours. After finding all the possible routes form the target node source router contains a list of possible routes and the shortest path. Now one by one the entire routing path among source and destinations are evaluated and the detection of malicious node is performed if exist in the concerning route. Therefore in order to describe the entire process of the proposed routing protocol the entire routing process can be divided in three different modules.

1. Threshold computation
2. Route discovery
3. Routing decisions

1. Threshold Computation

The threshold values are help in making the routing decisions for selecting the appropriate path. Most of time the malicious attacker is found in first routing path in routing path but for evaluation of first path and assuring the security for multiple malicious nodes in network a history table of sessions is created as the given manner in table .

Table 1: History Table

Node ID	Remain Energy	Packet Delivery Ratio	Last Sequence Number

Using the history table values the three different parameters as threshold is computed using the following formulas.

For energy

$$E_t = \frac{1}{n}\sum_{i=0}^{n} E_i$$

The energy is an essential network parameter the mobile ad hoc network devices are made with limited resources. When a malicious node is deployed in network the node replies all the nodes when it found the RREQ message. According to the literature for each device events the node consumes a fixed amount of energy thus if node frequently replies the request then the node losses their energy rapidly.

For packet delivery ratio

$$P_t = \frac{1}{n}\sum_{i=0}^{n} P_i$$

According to the black hole nodes properties when the malicious node find the data packets it drop the whole data. Therefore the node has the low packet delivery ratio as compared to other nodes in network and for sequence numbers

$$S_t = \frac{1}{n}\sum_{i=0}^{n} S_i$$

Sequence number is one of the most essential node properties of the network. Highest sequence number means the router contains the fresh route to the destination.

After computing the threshold values the route discovery process is taken place as given in the next section.

2. Route Discovery

As discussed previously the proposed routing protocol is an extension of traditional AODV routing protocol. Therefore the route discovery is performed in traditional process of AODV. In this manner first the source node broad cast the RREQ (route request) packets for the target node. As the RREQ found at the target node the RREP message is broad casted and different reply message from different sources are found at source node. Thus the source node routing table is updated and a number of different paths for data transmission is available. Now first path is selected and detection process is taken place in the below given manner.

3. Routing Decisions

In order to perform the detection of the malicious host in network the following process is taken place:

Suppose the network contains N nodes such that $N = \{N_1, N_2, \ldots N_n\}$ and for each node the remaining energy is denoted by E_i where the $i = \{1,2, \ldots, n\}$ similarly the node PDR is denoted using P_i and the sequence number of i[th] node is given by S_i. For evaluating the suspected node an array of node is created which is named as SS Now the node evaluation process is performed in the following steps.

Step 1: finding suspected node
For each node in routing path
{
If ($E_i \leq E_t$ *and* $S_i \geq S_t$)
{
Node marked as suspected;
SS.add (N_i);
}
}
Step 2: finding malicious node
For each node in suspected list
{
If ($P_i \leq P_t$)
{
// node marked as malicious node and eliminate the route
}
}

3. Network Setup

1. Simulation Setup

In this section provides the desired network configuration for simulation of security scheme implementation using AODV routing protocol.

Table 2: Network Setup

Simulation properties	*Values*	*Description*
Antenna model	Omni Antenna	In radio communication, an Omnidirectional antenna is an antenna which emits radio wave power regularly over all directions in a plane, using the emitted power reducing with elevation angle above or below the plane, reducing to zero on the antenna's axis. This emission pattern is often called as "doughnut shaped".
Dimension	1000 X 1000	That is size of the simulation screen where the mobile and base station
Radio-propagation	Two Ray Ground	This model, the shadowing fading factor is not considered. For that reason, for an exclusive distance, the Pr is a deterministic value.
Channel Type	Wireless Channel	This list of WLAN channels is the set of validly allowed Wireless LAN channels using IEEE 802.11.The 802.11 workgroup currently documents use in three different frequency ranges 2.4 GHz, 3.6 GHz and 4.9/5.0 GHz bands.
No of Mobile Nodes	30	Nodes in the simulation presents the devices that behaves like actual mobile devices and base stations
Routing protocol	AODV	The Ad hoc On Demand Distance Vector (AODV) routing algorithm is a routing protocol designed for MANET. AODV is capable of both unicast and multicast routing.
Time of simulation	50.0 Sec.	The total time when the simulation is visible and locating its positions.

4. Simulation Scenarios

After setting up desired network configuration the proposed simulation model is desired to introduce. Thus in order to simulate the effect of the black hole attack on unsecured network and the effectiveness of the proposed technique is given using the following simulation scenario:

Implementation of traditional AODV Routing

In this experimentation a mobile ad hoc network is prepared and configured using AODV routing protocol. After that a malicious node (black hole node) is deployed on the network. After deploy in the attack the malicious node initiate working and drops almost all the captured packets. And during this process the performance of the routing protocol using the obtained trace file is evaluated. The simulation scenario can be visualized according to the figure

Implementation of the Proposed Routing Technique:
In this simulation scenario the mobile ad hoc network is configured using the proposed routing protocol. After that a malicious node is deployed over the network. Finally the performance of evaluation of the proposed technique is evaluated in terms of throughput, end to end delay and packet delivery ratio.

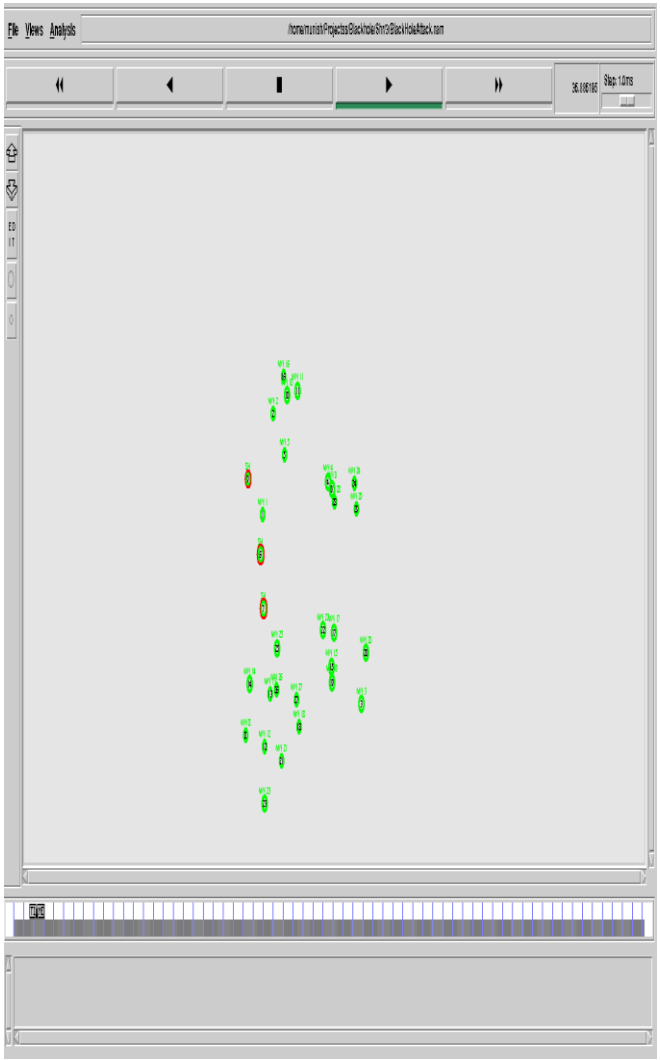

Figure 2: Traditional Method

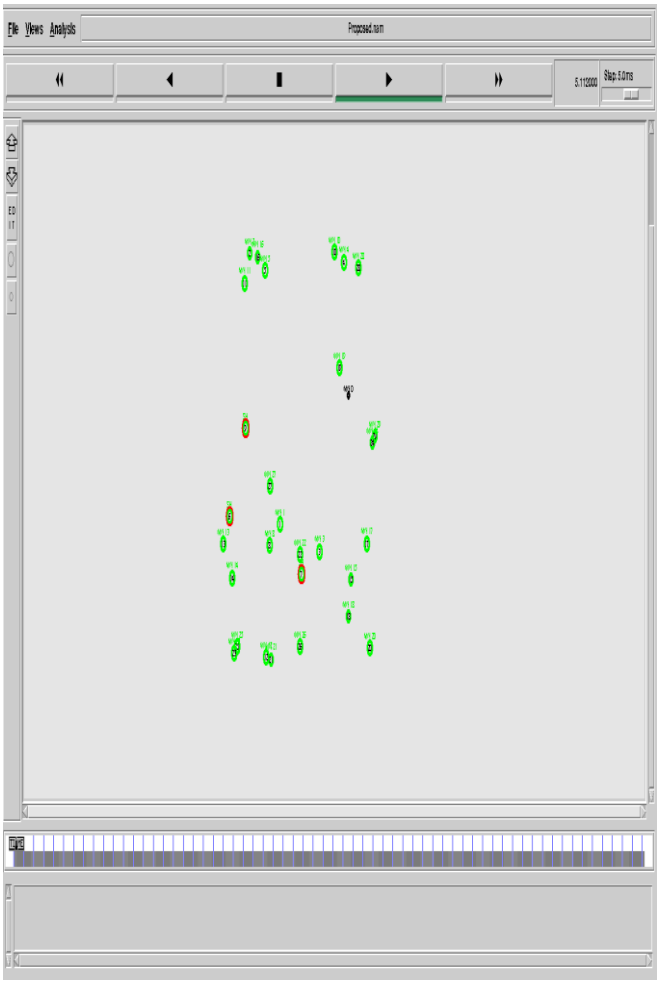

Figure 3: Proposed Method

1. Traditional AODV

1. Initially the network is functioning normally even when a malicious node is deployed on network.
2. When a network node tries to discover the route the malicious node starts working
3. If more than one session is active in network most of the traffic attracted towards the malicious node.

2. Proposed Routing Technique

1. Initially the network functioning normally even a malicious node deployed
2. The network acts as normal function during different communication sessions under attack conditions.

3. Performance Evaluations

The given chapter provides the detailed experimentations and their results evaluation. In order to perform the results analysis the comparison of the obtained results are performed in terms of throughput, packet delivery ratio and end to end delay.

4. End to End Delay

End to end delay on network refers to the time taken for a packet to be transmitted across a network from source to destination device. The end to end of both the methods during attack deployment is given using figure. In this diagram blue line represents proposed routing scheme and the green line shows the traditional AODV routing performance in terms of end 2 end delay. In this diagram the X axis shows the packets ID and the Y axis shows the end to end delay of network during black hole attack deployment. According to the obtained results the end to end delay of the proposed routing technique is less than the traditional AODV routing. Therefore the performance of the network is not much affected by the proposed routing scheme.

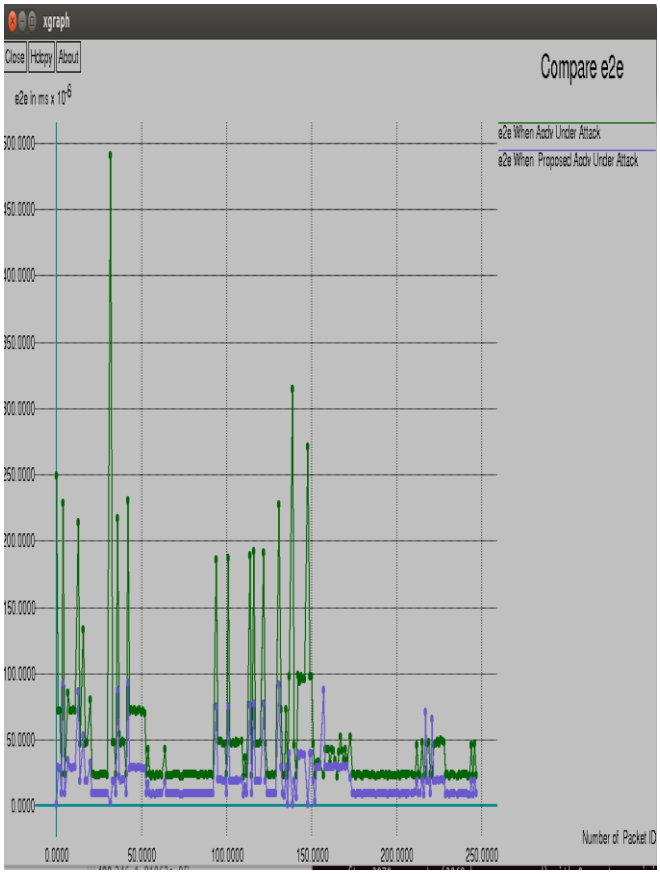

Figure 4: Comparative End 2 End Delay

5. Packet Delivery Ratio

Packet delivery ratio provides information about the performance of any routing protocols, where PDR is estimated using the formula given

$$packet\ delivery\ ratio = \frac{total\ delivered\ packets}{total\ sent\ packets}$$

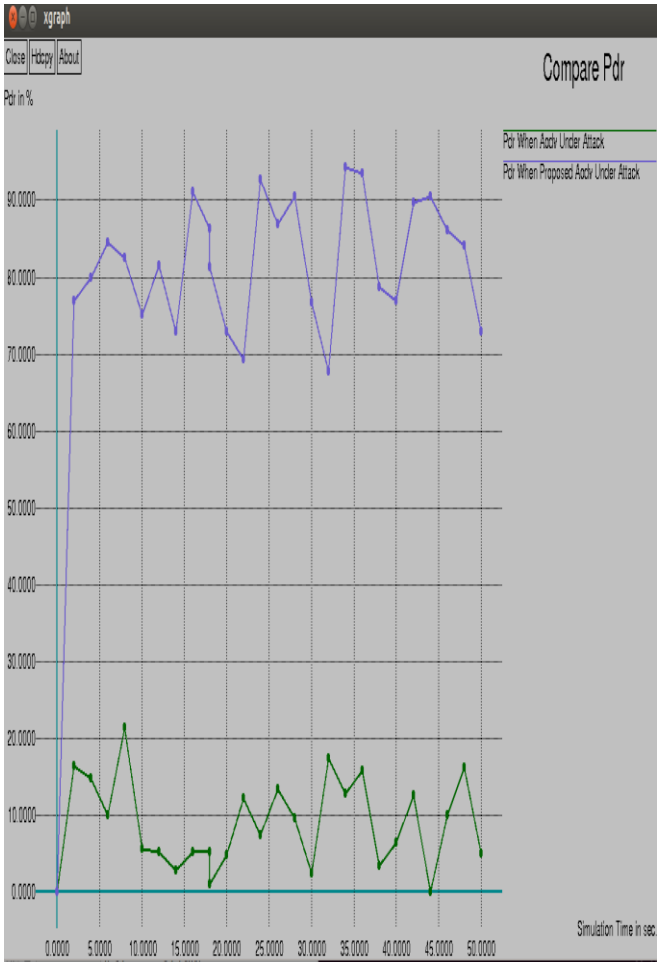

Figure 5: Comparative Packet Delivery Ratio

The comparative packet delivery ratio of both the routing protocols are given using figure 6.5, in this diagram the amount of packet successfully delivered by the proposed routing technique is given using blue line and the green line shows the packet delivery ratio of the traditional AODV routing protocol. For demonstrating the results X axis contains the simulation time in terms of second and Y axis shows the total percentage of packet delivered. According to the obtained results the performance of the proposed routing protocol is higher than the traditional routing protocol during attack conditions.

6. Throughput

Network throughput is the usual rate of successful delivery of a message over a communication medium. This data may be transmit over a physical or logical link, or pass by a certain network node. The throughput is calculated in terms of bit/s or bps, and occasionally in terms of data packets per time slot or data packets per second.

The given diagram 6.6 shows the comparative throughput between traditional AODV (represented using green line) and the proposed AODV routing (given using blue line). In this diagram the X axis shows the simulation time in seconds and the Y axis represents the throughput in terms of KBPS. According to the evaluated results the obtained throughput by the proposed routing protocol is much better than the traditional AODV routing protocol during black hole attack deployment.

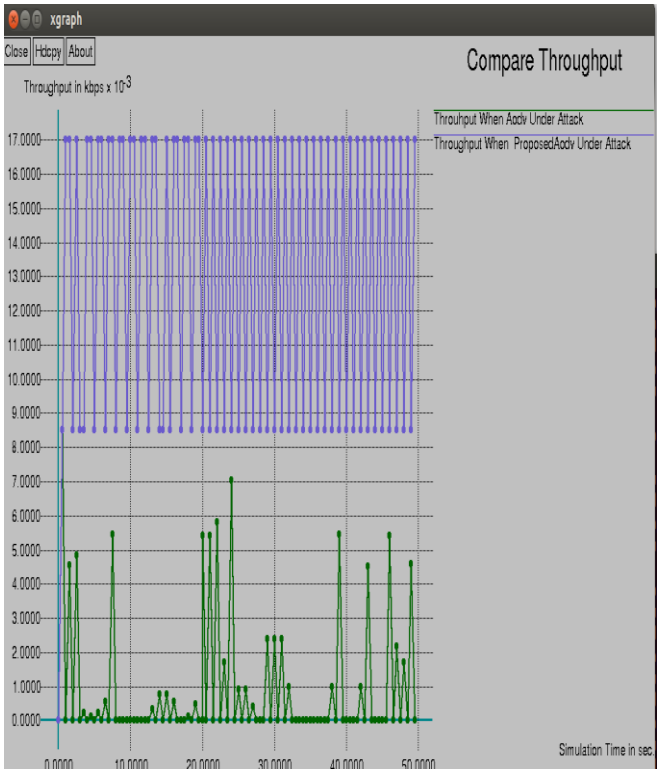

Figure 6: Comparative Throughput

5. Conclusions

Mobile ad hoc network is a kind of wireless network. That supports mobility and de-centralized manner of communication. The routing protocols are responsible for creating and managing the routes for communication. Thus the network is suffers from the performance and security issues. Most of security flaws are occurred in the network due to the routing strategy. The presented work introduces a security system for mobile ad hoc network. This security protocol provides the secure AODV routing technique against black hole attack.

In black hole attack the attacker deploy the attack using a malicious host. According to the routing technique secure routing protocol search the secure route between source and destination. Therefore, first a threshold value of network parameters is prepared using energy, sequence number and packet drop ratio. After route discovery most of the methods are evaluate only first route for attack detection, and if a malicious node found in path then again route discovery is performed. Thus leads additional time and control message exchange in network. Therefore the traditional system affects the performance in terms of energy and packet delivery ratio.

In order to simulate the entire issues and solution process a simulation using NS2 network simulator is provided. After implementation of the proposed routing protocol the performance of the network is evaluated in terms of packet delivery ratio, throughput and end to end delay. The performance results are summarizing in the given table 7.1.

Table 3: Performance Summary

S. No	*Parameters*	*Remark*
1	Packet delivery ratio	With respect to the traditional routing protocol the performance of proposed routing protocol is better and even not affected during black hole attack.
2	Throughput	The routing offers the next route adaptation policy for improving additional control message exchange rate. Thus network offers the better throughput in attack conditions.
3	End 2 end delay	The end to end delay of network is much better than the traditional routing protocol even when the attack is deployed in network.

According to obtained results and performance the routing protocol complete the proposed objective of study. The future extension of the presented protocol is given in next section.

6. Advantage

The mobile ad hoc network is a wirelessly group of nodes. In this network a node can any time leave or join the network thus a probability occurred a malicious node can join the network and active communication any time. In order to improve the security gap, the proposed routing technique offer the following advantages over the traditional routing protocol.

1. Able to locate the malicious attacker: the proposed technique is able to distinguish the malicious and trust worthy nodes among the available set of routers.
2. Able to preserve the network performance even when the malicious node active in network: the proposed technique is an immune system by which during route discovery process the intermediate routers are evaluated for their trust. Thus the effect of malicious node is node affected the network performance.
3. Reduces the amount of control message exchange: the proposed technique only send the control message when required thus the routing overhead in terms of control message exchange is reduced.
4. Improve the throughput, PDR and end to end delay of network: the proposed secure discovery algorithm evaluates the routing path by applying constrain to the routers. And only those routers are selected for communication which is efficient and secure.

7. Limitations

The proposed routing technique is able to find the trust values of each node which participating in the communication. Thus, there are only a single drawback is observed during design. The proposed routing technique performs additional computations for finding the trusted node in network. Thus additional memory and time is consumed which is also responsible for frequently energy consumption in the network nodes.

8. Future Works

The proposed routing technique offers high performance network and secure route discovery. The obtained results demonstrate the high throughput, high packet delivery ratio and less end to end delay. In near future additional literature is studied for enhancing secure routing by including technique various different attacks too. Additionally the method is optimized for energy preservation and efficient computing.

Acknowledgment

I express my deep sense of gratitude to **Mr Ashish Tiwari** Asst. Professor & head in the in the Department of Computer Science & Engineering, at Vindhya institute of technology and science, Indore. Whose kindness valuable guidance and timely help encouraged me to complete this volume on a very crucial issue related to the work.

A special thank of mine goes to **Mr. A. J. Siddiqui,** Executive Director of VITS, Indore. And to **CC Bapat,** Director of VITS for extending his support.

I wish to thank my husband for their undivided support and interest who inspired me and encouraged me to go my own way without whom I would be unable to complete my research.
At last but not the least I want to thank my friends who appreciated me for my work and motivated me and finally to god who made all the things possible.

References

[1] Ashok Desai, "Review Paper on Detection and Prevention Techniques of Gray-Hole Attack in Manet", IJCSMC, Vol. 2, Issue. 5, May 2013, pg.105 – 108
[2] Ketan S. Chavda, Ashish V. Nimavat, "Comparative Analysis of Detection and Prevention Techniques of Black Hole Attack in AODV Routing Protocol of MANET", International Journal of Futuristic Science Engineering and Technology Vol 1 Issue 1 January 2013 ISSN 2320 – 4486
[3] Swati Jain, Naveen Hemrajani, "Detection and Mitigation Techniques of Black Hole Attack in MANET: An Overview", International Journal of Science and Research (IJSR), India Online ISSN: 2319-7064
[4] Mohammad M. Shurman, Mamoun F. Al-Mistarihi, Khalid A. Darabkh, "Merging Dynamic Address Auto-configuration and Security Key Protocols in Mobile Ad Hoc Networks", MIPRO 2013/CTI
[5] Prof. D. S. Patil, Prof. A. M. Ghorpade, "Cope with black hole attacks in AODV protocol in MANET by end to end route discovery", IOSR Journal of Electronics & Communication Engineering (IOSR-JECE) ISSN : 2278-2834, ISBN : 2278-8735, PP : 21-26
[6] Rishi Raj Bharti, Shivendra Singh, "Performance Evaluation of Black hole Attack in MANET and Intrusion Detection System", International Journal Of

Scientific Research And Education, Volume 2, Issue 8, Pages 1546-1551, August-2014, ISSN (e): 2321-7545
[7] Fan-Hsun Tseng, Li-Der Chou and Han-Chieh Chao, "A survey of black hole attacks in wireless mobile ad hoc networks", licensee Springer. 2011, http://link.springer.com/article/10.1186/2192-1962-1-4/fulltext.html
[8] Performance Analysis of AODV, DSR and OLSR in MANET.
[9] Dr. A. A. Gurjar, A. A. Dande , Black Hole Attack in Manet's: A Review Study, International Journal of IT, Engineering and Applied Sciences Research (IJIEASR) ISSN: 2319-4413 Volume 2, No. 3, March 2013
[10] MANET: Vulnerabilities, Challenges, Attacks, Application, IJCEM International Journal of Computational Engineering & Management, Vol. 11, January 2011
[11] Mohit Kumar, Rashmi Mishra, An Overview of MANET: History, Challenges and Applications, Indian Journal of Computer Science and Engineering (IJCSE)
[12] MANET: Black Hole Node Detection in AODV, International Journal of Computational Engineering Research
[13] Mobile Ad Hoc Networking: Imperatives and Challenges IJCA Special Issue on "Mobile Ad-hoc Networks "MANETs, 2010