International Journal of Contemporary Technology and Management

Volume V, Issue XII, December 2016 ISSN (Online) 2278-8034

Avoidance of routing protocol based black hole and wormhole attack in mobile ad hoc network

Swati Gothwal,
Gothwal.swati14@gmail.com
M. Tech Scholar
SVITS Indore

Gaurav Vinchurkar,
Gvinchurkar11@gmail.com
Asst. Professor
SVITS Indore

Abstract -**In a mobile ad hoc network the key responsibility of communication is dependent on the routing protocols. In this network the routing protocols are helps to discover the routes, and also work to maintain the routes. On the other hand the routes are main target of attackers to deploy the crucial kinds of attacks. In literature a number of different kinds of routing based attack models are available. Among them black hole and wormhole are much popular attack types. Both the attacks are self-advertising based attack deployments and a significant loss can produce to the network. Therefore in this presented work the detailed investigations about both the attacks are performed and a new lightweight solution for avoiding these attacks is introduced. The proposed technique is able to distinguish both of the attack conditions and also able to avoid the effects of the attacks. In order to identify the attack conditions the routing protocol usages a feck request process, additionally the sequence number is used to track the attacker node and their routes. In order to implement the proposed concept using the routing protocol the AODV routing protocol is modified and the attackers are successfully avoided from the malicious routes. The implementation of the proposed routing technique is performed using NS2 simulator and their performance is computed under both the attack conditions. The performance of the network demonstrates the proposed technique is efficient and also helps to recover the network from the routing based attacks. The experiments show that the proposed technique reduces the network end to end delay and optimizes the throughput, packet delivery ratio and energy consumption. Thus the proposed routing protocol is adoptable and efficient for working with the MANET.**

Keywords: MANET, AODV modification, NS2 simulation, Black hole, wormhole

I. INTRODUCTION

In this era of wireless devices, Mobile Ad-hoc Network (MANET) has become an indivisible part for communication for mobile devices. Therefore, interest in research of Mobile Ad-hoc Network has been growing since last few years. Security is a major concern for protected communication between mobile nodes in a hostile environment. In hostile environments adversaries can bunch active and passive attacks against intercept able routing in embed in routing message and data packets. Security has always been a key issue with wireless networks since there are no physical boundaries. Experience has shown numerous vulnerabilities to a variety of attacks even when security measures are in place. In the combined Internet-MANET environment also security is an important issue keeping in view the Internet connectivity and attack on the MANET protocols [1]. Wireless networks are gaining popularity to its peak today, as the users want wireless connectivity irrespective of their geographic position. There is an increasing threat of attacks on the Mobile Ad-hoc Networks (MANET). Black hole attack is one of the security threat in which the traffic is redirected to such a node that actually does not exist in the network. MANETs must have a secure way for transmission and communication which is quite challenging and vital issue [2]. In order to provide secure communication and transmission, researcher worked specifically on the security issues in MANETs, and many secure routing protocols and security measures within the networks were proposed. Therefore the proposed work is dedicated to find the solution for mobile ad hoc network based attacks. During investigation a number of different routing attacks are establish persons are much regularly deploy in network and hard to recover. Thus the wormhole and black-hole attack is selected for investigation and solution development.

II. PROPOSED WORK

The proposed work is intended to construct a routing based attack model using the black hole and wormhole attack characteristics and also prepare a solution by which not only the security of network becomes effective the performance of the routing is also enhanced. This chapter provides the key work performed for achieving the required solution.

A. System overview

The mobile ad hoc network is wireless technology where the communication is performed using the relay nodes. During the relaying the information the data is forwarded using the intermediate network nodes. In addition of that for keep in track all the network functioning not a single node is available, therefore the topology development and their formation is

performed dynamically. Due to the node's dynamicity or mobility the network nodes can any time leave or join the network. Thus the network is suspected to join by some malicious node. In this network the routing protocols are responsible for all the communication scenarios for example route discovery, data forwarding and the route maintenance. Therefore in most of the MANET attacks the routing protocols are used for attack deployments.

In order to overcome the routing based security issues in MANET two different routing based attacks are considered. In this context the first one is black hole attack and second is wormhole attack. The black hole attack is a kind of self-advertising attack similarly the wormhole attack too. In black hole attack a single attack join the network and promising to provide the shortest path among the source and destination. The source believes on the attacker and tries to send the data using the attacker node. During this the attacker node destroys all the data and not a single packet is delivered to the destination. On the other hand the wormhole attack is deployed with the help of more than one node. In most of the cases the wormhole attack is deployed by the two attackers using the high speed data link. As the black hole node these nodes are also promised to deliver data more efficiently but due to higher traffic in the high speed link the congestion situation is occurred in network and the delay in network is increases additionally the significant data loss is occurred.

In order to provide the effective solution for both the crucial attack a common algorithm is designed in this work. The proposed algorithm promises to avoid the malicious links in network and find most secure route among the source and destination. The next section provides the proposed technique and their formulation for finding the optimal secure route among source and destination.

B. Proposed routing

The proposed work is indented to secure the routing technique, thus the traditional AODV routing technique is modified to identify the malicious routes among the available routes between source and destination. Additionally find the secure route for secure communication. The process of secure route discovery and identification of attacker node is described using two main phases.

Detection of black hole attack

In order to understand the process of black hole attack detection first we follow an example: suppose in the network a source node S wants to send data to a destination node D. then in order to find the secure route the two trusted nodes T_1 and T_2 is used to verify the nodes trust. In this context the source node S ask about the trustworthiness of target node from the T_1 and T_2. Both the nodes are initiate the fake request to the targeted node, and wait for the 2*NTT time. Here NTT is network time to travel is assumed and its value is 30 MS. When the reply from the target node generated these nodes store the sequence number of packets and time to arrive of the reply message. Now need to cross check by the source node thus the node also send the request message to target node and it also maintain the sequence number and time of reply. Finally the comparison is made between all the recorded information by the actual source node and two trusted node T_1 and T_2. In this context the two cases are occurred.

1. Getting reply within time but sequence numbers are same of this nodes thus the attacker exist
2. Reply get beyond time but sequence number is different it means the attacker exist
3. Else the malicious node is not exist the communication will be secure.

The entire process of black hole node avoidance is given by the following table 2.1.

Input: source Node S, two trusted entity T_1 and T_2
Process: 1. Source S start trust evaluation using T_1 and T_2 2. T_1 send the fake request to target node and wait for 2*NTT 3. *if reply received then* a. Store sequence number and time of arrival 4. T_2 send the fake request to target node and wait for 2*NTT 5. *if reply received then* a. Store sequence number and time of arrival 6. Source also send the fake request to target node and wait for 2*NTT 7. *if reply received then* a. Store sequence number and time of arrival 8. If $response\ time \leq 2 * NTT \&\& sequnce\ number\ same$ a. Attack detected 9. If $response\ time \geq 2 * NTT \&\& sequnce\ number\ diffrent$

a. Attack detected

10. If
$response\ time \leq 2 * NTT \ \&\& \ sequnce\ number\ diffrent$

a. Secure node

11. End if
12. Initiate communication

Table 2.1 black hole detection

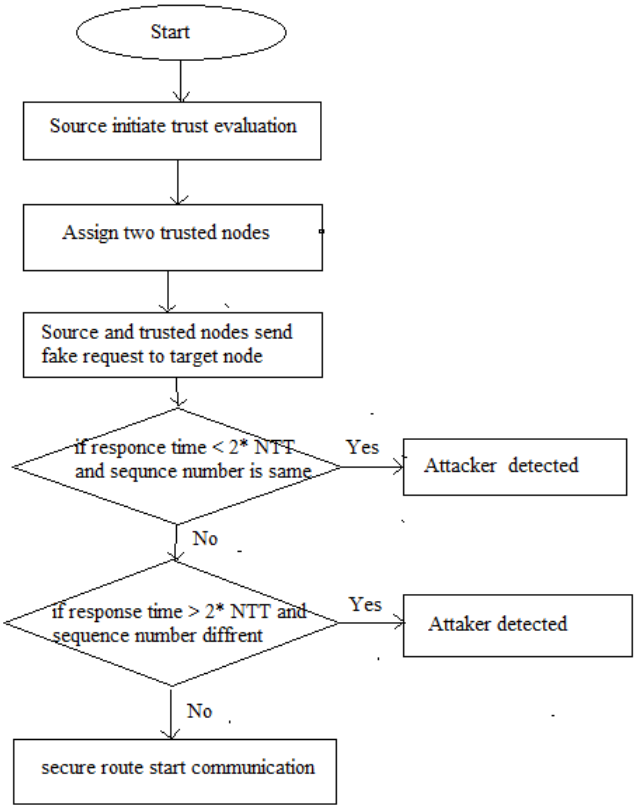

Figure 2.1 black hole node detection

Wormhole detection

In order to detect the wormhole link in the network path the RTT based technique is used. Therefore first the threshold for evaluation is prepared. In order to do this a normal network is constructed and using this network the experiment is performed for finding the mean traverse time between two nodes. That is computed using the following formula:

$$RTT = \frac{(reply\ receiving\ time\ -request\ \ sending\ time)}{2 * hop\ count}$$

Find the average of multiple sessions of experiments thus the threshold RTT is prepared. Suppose the N number of times the experiment is performed then the threshold RTT is:

$$T_{RTT} = \frac{1}{N}\sum_{i=1}^{N} RTTi$$

Now the condition is applied

1. If individual RTT is higher than threshold then there is wormhole link is available
2. Else route is secure

This process can also be described using the algorithm steps using table 2.2.

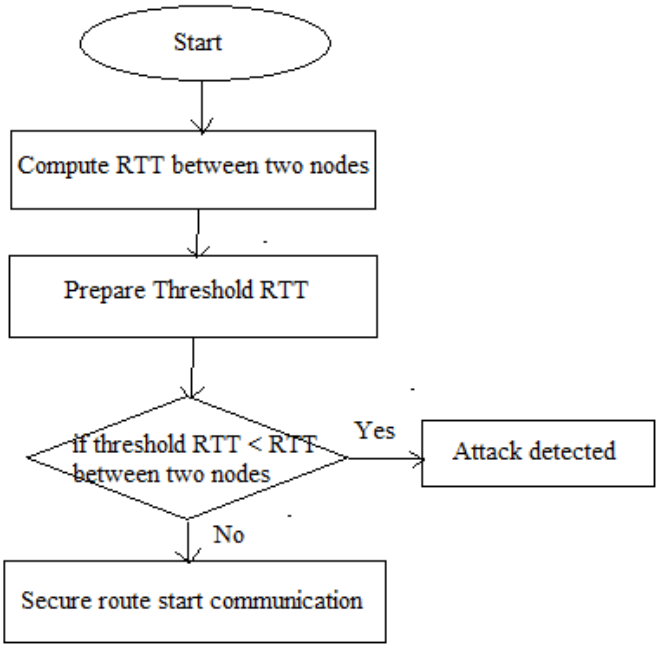

Figure 2.2 wormhole detection

Input: network nodes

Output: secure route

Process:

1. Prepare the network in ideal conditions
2. Compute the RTT using the following formula

$$RTT = \frac{(reply\ receiving\ time\ -request\ \ sending\ time)}{2 * hop\ count}$$

3. If experiment is performed for N times then

$$T_{RTT} = \frac{1}{N}\sum_{i=1}^{N} RTTi$$

4. If RTT $between$ two $nodes \geq T_{RTT}$
   a. Attacker exist
5. Else
   a. Secure route
6. End if

Table 2.2 wormhole attack detection

III. Simulation Setup & Scenario

This section describes the network setup and the required experimental scenarios that are performed for simulation and performance analysis.

A. Network Simulation Setup

This section describes the utilized parameters for preparing the required network and their experimental environment. The table 3.1 reports the required network parameters, their values and their brief description.

Simulation properties	Values
Antenna model	Omni Antenna
Simulation area	750 X 550 or 1000 X 1000
Radio-Propagation Model	Two Ray Ground
Channel Type	Wireless Channel
No of Mobile Nodes	20, 40, 60, 80, 100
Routing Protocol	AODV

Table 3.1 Network Simulation Setup

B. Simulation Scenario

To simulate the effect of network attacks and to demonstrate the effectiveness of the proposed solution two major scenarios are implemented for both attacks.

1. **Simulation of wormhole attack in normal network:** in this case the network is configured with the help of AODV routing technique and then the wormhole attack is deployed in network. During this experiment the network performance is measured and that is used for results analysis. The wormhole attack under normal network conditions is demonstrated using figure 3.1.
2. **Simulation of wormhole attack using proposed routing technique:** in this case the proposed routing protocol is configured with the network and the wormhole link is deployed. During the attacker node deployment the network performance is measured and used for performance study. Similarly the wormhole attack using the proposed technique is demonstrated using the figure 3.2.
3. **Simulation of black hole in normal network:** the figure 3.3 contains the network which is configured with the help of AODV routing protocol. After that the black hole node is deployed in the network and their performance is measured. The computed performance is used for further results analysis.

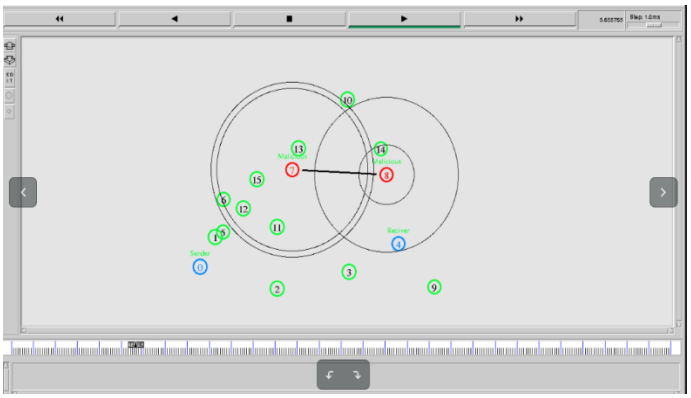

Figure 3.1 wormhole in attack normal network

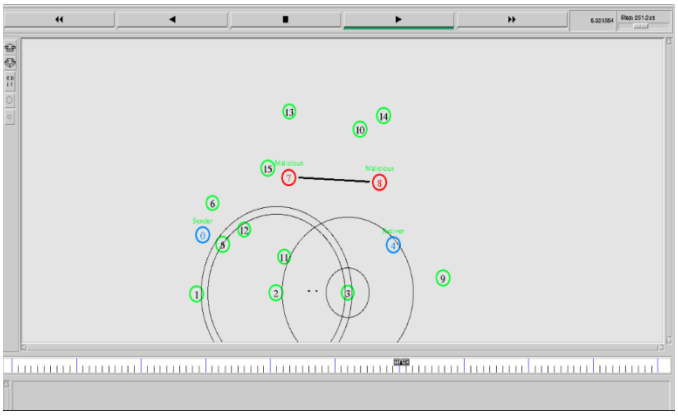

Figure 3.2 wormhole attack in proposed

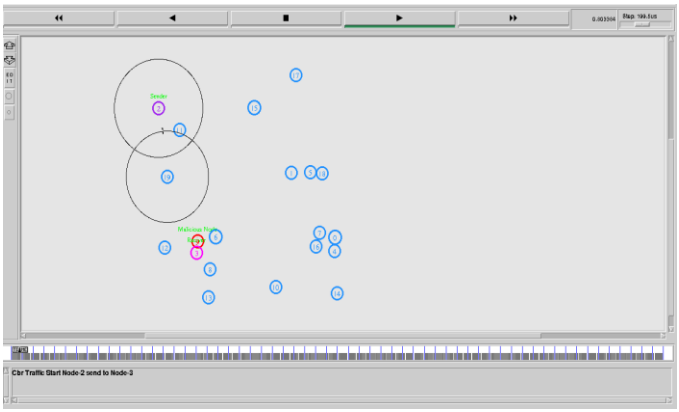

Figure 3.3 network under black hole attack

4. **Simulation of black hole using proposed technique:** in this scenario the network is configured with the help of proposed routing technique. Than after the attacker node is deployed in the network. During this experiment the performance of network is measured and preserved for the further results analysis. The described network scenario of the proposed simulation is given using figure 3.4.

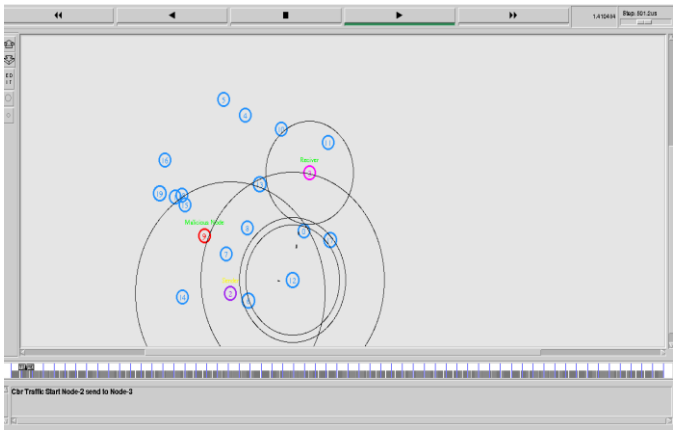

Figure 3.4 proposed network under black hole

IV. RESULT DISCUSSION

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

A. Remain Energy

The significant amount of energy consumed by the node, when the nodes are involve in sending, receiving or forwarding the data packets. Therefore the amount of remaining energy from the initial node energy is measured as the performance factor. During both the attack (black hole and wormhole) conditions the consumed energy is measured and reported in this section. The figure 4.1 shows the remain energy of network under the black hole conditions. Additionally the figure 4.2 shows the remain energy during the wormhole

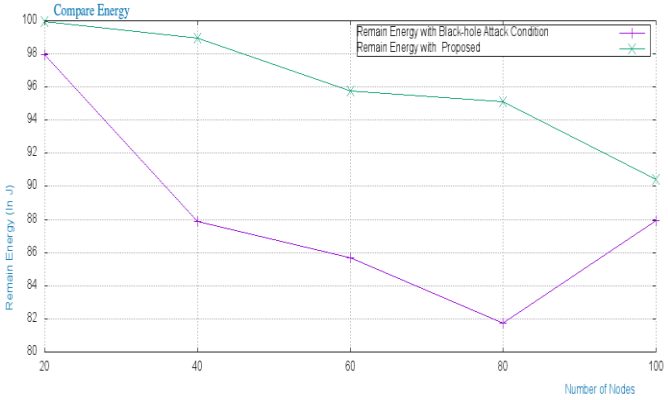

Figure 4.1 remain energy in Black Hole Attack

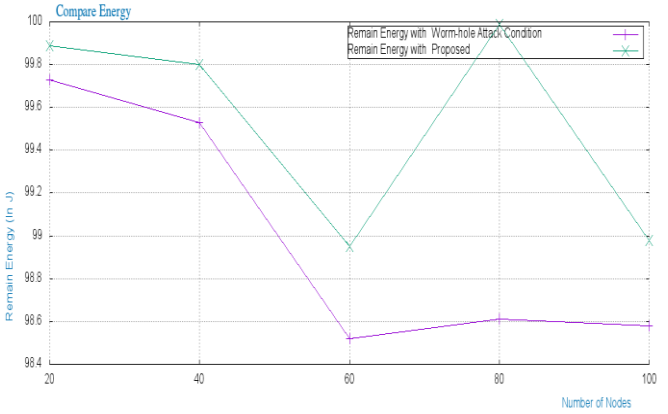

Figure 4.2 remain energy Wormhole

Attack conditions. In order to represent the remain energy for both the attacks and the comparative remain energy after preventing the attack using the proposed approach is also demonstrated using this figure. In these graphs the Y axis of the diagram shows the remains energy of network in terms of Jules and the X axis shows the number of nodes during the experiments. According to the obtained results during the attack in normal AODV routing technique the energy of the nodes are consumed more frequently as compared to the proposed routing technique under both the routing attack conditions. Therefore the proposed technique is able to reduce the energy consumption of network nodes under the attack conditions. Thus the method is adoptable for recovering network performance under routing based attacks.

Table 4.1 remain energy Tabular Form

Number of Nodes	*For Black-hole Attack*		*For Wormhole Attack*	
Energy Consumption	Proposed Approach	Attack Condition	Proposed Approach	Attack Condition
20	100	68	99.9	96.7
40	99	88	99.8	99.5
60	95.8	85.8	98.5	99
80	95	82	100	98.6
100	90.2	88	99	98.6

B. Packet Delivery Ratio

The Packet delivery ratio is also termed as the PDR ratio. The packet delivery ratio provides information about the performance of any routing protocols using the successfully delivered packets to the destination. The PDR can be computed using the following formula:

$$Packet\ Delivery\ Ratio = \frac{Total\ Delivered\ Packets}{Total\ Sent\ Packets}$$

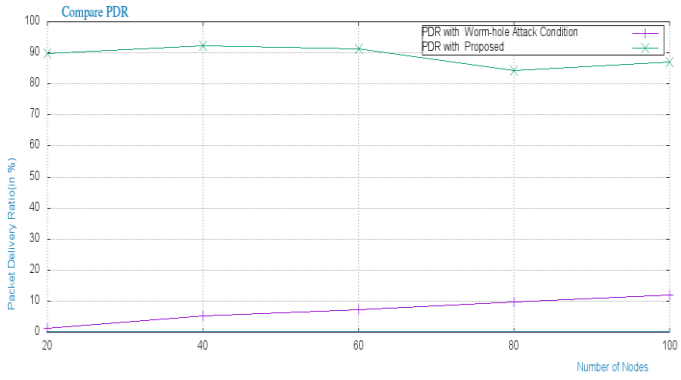

Figure 4.3 Packet Delivery Ratio Wormhole

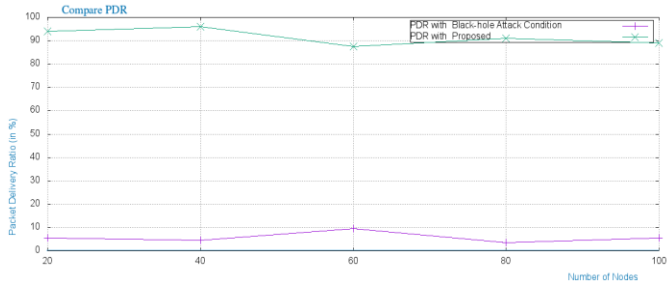

Figure 4.4 Packet Delivery Ratio Black Hole

The figure 4.3 shows the network performance in terms of packet delivery ratio under wormhole conditions. According to the given results the normal network demonstrates too few packet delivery ratios. Because during the attack deployment the network is not able to deliver the data packets to their destination and due to this a significant amount of packets are dropped in network. On the other hand the proposed technique shows the higher packet delivery ratio because the proposed technique able to distinguish the secure route among the all available path thus it is make secure for the wormhole attack. In the next figure 4.4 the packet delivery ratio during the black hole deployment is estimated. In this diagram the traditional AODV shows the low packet delivery ratio because the malicious node drops all the received packets. On the other hand the proposed technique avoids the black hole attack thus the network performance is not affected due to this. In order to provide the performance measurements both the figures 4.3 and 4.4, X axis of diagram contains the number of nodes are used for experimentation and the Y axis contains the amount of packets successfully delivered in terms of percentage.

Table 4.2: PDR Tabular Form

Number of Nodes	*For Black-hole Attack*		*For Wormhole Attack*	
(Packet Delivery Ratio in %)	Proposed Approach	Attack Condition	Proposed Approach	Attack Condition
20	95	5	90	1
40	96	5	91	5
60	89	10	90.8	8
80	91	4	85	5
100	90	5	88	11

C. End to End Delay

End to end day on network refers to the time taken, for a packet to be broadcast across a network from resource to purpose device, this delay is calculated using the beneath given formula.

$$E2E\ Delay = Receiving\ Time - Sending\ Time$$

The end to end delay of the network under the black hole and wormhole attack deployment is demonstrated in figure 4.5 and 4.6 respectively. In this diagram the X axis contains the

number of nodes in the given experiment and the Y axis contains the end to end delay of network. The computed end to end delay in network is given in terms of MS (milliseconds). According to the obtained results the normal network under the black hole attack demonstrate the higher end to end delay as compared to the proposed routing technique. Additionally the end to end delay of network is increases as the amount of nodes in network is increases. On the other hand the effect of this phenomenon is not much produced in the proposed technique. Thus the proposed technique is secure and efficient as compared to the traditional technique of routing under black hole attack deployments.

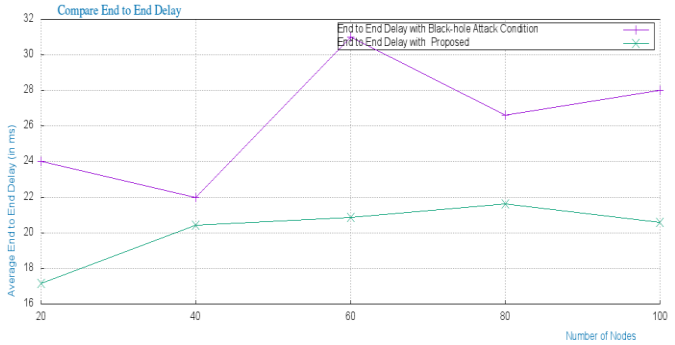

Figure 4.5 End to End Delay for Black-hole

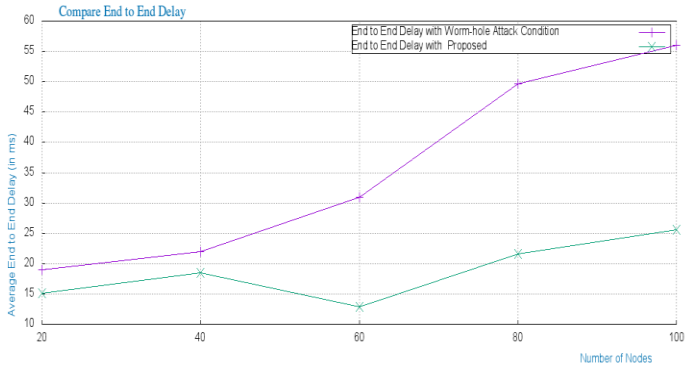

Figure 4.6: End to End Delay Wormhole Attack

Table 4.3: End to End Delay Tabular Form

Number of Nodes	***For Black-hole Attack***		***For Wormhole Attack***	
(End to End Delay in Millisecond)	Proposed Approach	Attack Condition	Proposed Approach	Attack Condition
20	17	24	15	19
40	21	22	18	23
60	23	31	13	31
80	21.9	26.8	22	50
100	20.8	28	26	51

D. Throughput

Network throughput is the regular rate of successful message delivery above a communication channel. This data might be delivered above a physical or logical link, or pass during a certain network node.

$$\text{Received data (MBPS)} = (\text{bytes/ time})^* \, 8/10^6$$

$$\text{Throughput (MBPS)} = \text{bytes\_recv\_per\_unit\_of\_time}^* \, 8/10^6$$

The throughput is regularly considered in bits per second (bit/s or bps), and sometimes in data packets per second or data packets per time slot. The figure 4.7 and 4.8 is a line graph which shows the performance of network under the wormhole attack conditions. The Y axis of the diagram includes the performance of network in terms of KBPS (kilobyte per seconds). In addition of that the X axis shows the number of nodes in the experimental network. According to the performance the network throughput is significantly reduced during the attack conditions in normal conditions because the network packets are not completely reached at the required destination. On the other hand the proposed technique is able to reduce the effect of wormhole attack thus the network throughput is effectively utilized even when the attack nodes are present in the network.

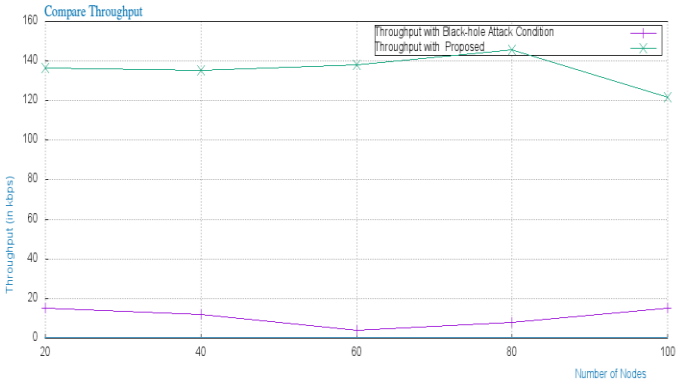

Figure 4.7Throughput Black Hole Conditions

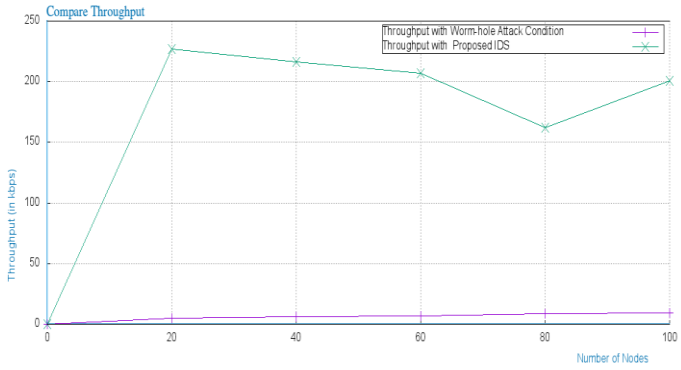

Figure 4.8 Throughput Wormhole Attack Conditions

Table 4.4: Throughput Tabular Form

Number of Nodes	***For Black-hole Attack***		***For Wormhole Attack***	
(Throughput in %)	Proposed Approach	Attack Condition	Proposed Approach	Attack Condition
20	138	17	230	10
40	138	16	220	12
60	139	4	210	14
80	143	9	160	16
100	121	18	200	18

V. CONCLUSION

This chapter summarizes the entire work performed for finding the secure routing technique. Therefore the performed experiments and their observations are reported here as conclusion of work additionally the future directions of the proposed work is provided as the future extensions of the proposed technique.

A. Conclusion

The mobile ad hoc network is one the most popular network technology. Due to its properties that is very valuable for different kinds of applications. The key properties of the network are their wireless mode of operation, mobility support, dynamic topology, inbuilt power source and others. Due to this, the network is rapidly deployable and configurable. In case of disasters and army applications that is frequently used. On the other hand due to these properties the network is also suffers from the issues of performance and security. Due to high mobility, changing topology, network partitioning and others the significant performance loss is observed. In addition of due to the dynamic nature of topology is also affecting the security of network.

In this concern work the security is the key area of investigation and development. In this context the black hole and wormhole attacks are considered as the attack model. Both the network attacks are self-advertising techniques of attack deployment. Additionally these attacks are significantly affecting the performance of network. Both the attacks are deployed using the routing manipulation and the week routing strategy therefore a secure technique of routing need to develop for avoiding these attacks. The proposed solution is a threshold based technique where two key parameters for identifying the malicious route or activity in network is used. In first the TTL (time to leave) is key parameter for justifying the black hole attack conditions and for recognizing the wormhole attack the TTL and sequence number is used for detection of malicious host.

The implementation of the proposed technique is provided using the NS2 network simulator. Additionally to implement the proposed routing concept the AODV routing protocol is modified. After implementation of the proposed work the following network parameters are used to demonstrate the effect of attacks and the avoidance effect. The performance is summarized using table 5.1.

S. No.	Parameters	Attack Condition	Proposed Method
Black hole attack			
1	Energy Consumption	82.36 ↓	96 ↑
2	Packet delivery ratio	5.8 ↓	92.2 ↑

4	End to End Delay	52.72 ↑	20.74 ↓
5	Throughput	12.8 ↓	135.8 ↑
Worm hole attack			
1	Energy Consumption	98.48 ↓	99.44 ↑
2	Packet delivery ratio	6 ↓	88.96 ↑
3	End to end delay	34.8 ↑	18.8 ↓
4	Throughput	14 ↓	204 ↑

Table 5.1 performance summary

According to the obtained performance of the network the proposed technique found efficient and enhances the network performance by reducing the energy consumption, by improving the end to end delay, packet delivery ratio and throughput. Therefore the proposed work is suitable for preventing the routing based attacks in the mobile ad hoc network. This section provides the summary of work; the next section includes the future extension of the proposed work.

B. Future work

The proposed work is acceptable for the routing based security issues and their solution formulation. But he following extensions is required to improve the proposed work for future usage.

1. Experimentation with different other routing based attack models
2. Includes more parameters for extending solution for other attacks
3. Measure the effect of the proposed technique over the cluster based networks

REFERENCE

[1] Vikas Solomon Abel, "Survey of Attacks on Mobile Ad-hoc Wireless Networks", International Journal on Computer Science and Engineering (IJCSE), PP. 826 - 829 Vol. 3 No. 2 Feb 2011.

[2] IrshadUllah and Shoaib Ur Rehman, "Analysis of Black Hole Attack on MANETs Using Different MANET Routing Protocols", Master Thesis, School of Computing Blekinge Institute of Technology, June, 2010, Sweden.

[3] Neeraj Arya, Upendrasingh, Sushmasingh, "Detecting and Avoiding of Worm Hole Attack and Collaborative Black hole attack on MANET using Trusted AODV Routing Algorithm", IEEE International Conference on Computer, Communication and Control, MGI Indore, INDIA. September 10 -12, 2015.

[4] Mukesh Kumar Garg, Dr. Ela Kumar, "Routing Issues for Trust Based Framework inMobile Ad Hoc Networks", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)Volume 2, Issue 2, February 2013,Available online at: http://www.homelanxtreme.com/wired-vs-wireless.htm

[5] Navpreet Kaur and SangeetaMonga, "Comparisons of Wired and Wireless Networks: A Review", International Journal of Advanced Engineering Technology, Vol. V, Issue II, April-June, PP. 34-35, 2014.

[6] Navpreet Kaur and SangeetaMonga, "Comparisons of Wired and Wireless Networks: A Review", International Journal of Advanced Engineering Technology, Vol. V, Issue II, April-June, PP. 34-35, 2014.

[7] "What is Wireless Network", online available at: http://www.home-network help.com/wireless-network.html

[8] "How Wireless Networks Work", online available at: http://www.webopedia.com/DidYouKnow/Computer_Science/wireless_networks_explained.asp

[9] Fan Wu, "Economic Incentive Mechanisms for Wireless Ad Hoc Networks Principal Investigator", Natural Science Foundation of China (NSFC), 2012.

[10] Mario Gerla, Ling-Jyh Chen, Yeng-Zhong Lee, Biao Zhou, Jiwei Chen, Guang Yang, Shirshanka Das, "Dealing with node mobility in ad hoc wireless network", Computer Science Department, UCLA, Los Angeles, CA 90095, USA

[11] "Ad Hoc Networks", ARC Communications Research Network, available online: http://www.acorn.net.au/telecoms/adhocnetworks/adhocnetworks.html

[12] ImrichChlamtac, Marco Conti, Jennifer J.-N. Liu, "Mobile ad hoc networking: imperatives and challenges", Ad Hoc Networks 1 (2003) 13–64

[13] M.S. Corson, J.P. Maker, and J.H. Cernicione, Internet-based Mobile Ad Hoc Networking, IEEE Internet Computing, pages 63–70, July-August 1999.

[14] Amitabh Mishra and Ketan M. Nadkarni, Security in Wireless Ad Hoc Networks, in Book The Handbook of Ad Hoc Wireless Networks (Chapter 30), CRC Press LLC, 2003.

[15] Lidong Zhou and Zygmunt J. Hass, Securing Ad Hoc Networks, IEEE Networks Special Issue on Network Security, November/December 1999.

[16] Yongguang Zhang and Wenke Lee, Security in Mobile Ad-Hoc Networks, in Book Ad Hoc Networks Technologies and Protocols (Chapter 9), Springer, 2005.

[17] Lecture Notes, "Broadband Computer Networks," by Prof.ZhishengNiu, Tsinghua University, 2003.

[18] Ankur O. Bang and Prabhakar L. Ramteke, "MANET: History, Challenges and Applications", International Journal of Application or Innovation in Engineering & Management (IJAIEM), Volume 2, Issue 9, September 2013. Cisco. Cisco Internetworking. Cisco Press, 2002.

[19] Charles E. Perkins, Ad Hoc Networking, Addison Wesley, 2001.

[20] Xiaoyan Hong, Kaixin Xu, and Mario Gerla, Scalable routing protocols for mobile ad hoc networks, 2002.

[21] Tseng Y.C., Shen C.C, and Chen W.T. Mobile ip and ad hoc networks: An integration and implementation experience, Technical report, Dept. of Computer Science and Inf. Engineering, Nat. Chiao Tung Univ., Hsinchu,, Taiwan, 2003.

[22] A. Valarmozhi, M. Subala and V. Muthu, "Survey of Wireless Mesh Network", International Journal of Engineering and Innovative Technology (IJEIT), Volume 2, December 2012.

[23] Dr. Uwe Roth, Highly dynamic destination-sequenced distance vector routing. http://wiki.uni.lu/secanlab/Highly+Dynamic+DestinationSequenced+DistanceVector+Routing.html

[24] Danny D. Patel, Energy in ad-hoc networking for the pico radio. Technical report.

[25] Guoyou He. Destination-sequenced distance vector (DSDV) protocol, Technical report, Helsinki University of Technology, Finland.

[26] Ravinder Ahuja, Alisha Banga Ahuja, and PawanAhuja "Performance Evaluation and Comparison of AODV and DSR Routing Protocols in MANETs under Wormhole Attack", In Proceedings of the 2013 IEEE Second International Conference on Image Information Processing, pp. 699 - 702, ICIIP-2013.

[27] Fenglien Lee, "Routing in Mobile Ad Hoc Networks", University of Guam Guam 96923, USA, available online at: http://cdn.intechopen.com/pdfs-wm/12861.pdf

[28] Nikhil Kumar, Vishant Kumar, Nitin Kumar, "Comparative Study of Reactive Routing Protocols AODV and DSR for Mobile Ad hoc Networks.

[29] Charles E, Perkins and Elizabeth M. Royer. Ad-hoc on-demand distance vector routing, Technical report, Sun Micro Systems Laboratories, Advanced Development Group, USA.

[30] Ning. P. and Sun. K. How to misuse AODV: a case study of insider attacks against mobile ad-hoc routing protocols. Technical report Computer Science Department, North Carolina State Univ., Raleigh, NC, USA, 2003

[31] D. Djenouri, O. Mahmoudi, D. Llewellyn-Jones, M. Merabti, "On Securing MANET Routing Protocol against Control Packet Dropping", In IEEE International Conference on Pervasive Services, pp. 100-108, 2007.

[32] Donald Welch," Wireless Security Threat Taxonomy", Proceedings of the 2003 IEEE Workshop on Information Assurance United States Military Academy, West Point, NY June 2003

[33] Andrew Simmonds1, "An Ontology for Network Security Attacks" Springer-Verlag Berlin Heidelberg 2004.

[34] NICHOLS, R. K., and LEKKAS, P. C. Wireless Security Models, Threats, and Solutions. McGraw–Hill, 2002. ISBN: 0-07-138038-8.

[35] ZHOU, L., AND HAAS, Z. J. Securing Ad Hoc Networks. IEEE Network 13, 6 (1999), 24–30.

[36] DharaBuch, DeveshJinwala, "Detection of Wormhole Attacks in Wireless Sensor Networks", IEEE Conference on Advances in Recent Technologies in Communication and Computing, pp 7-14, 2011.

[37] Majid Meghdadi, SuatOzdemir and InanGuler , "A Survey of Wormhole based Attacks and their Countermeasures in Wireless Sensor Networks", IETE TECHNICAL REVIEW, VOL 28, ISSUE 2, Mar-Apr 2011.

[38] Mani Arora, Rama Krishna Challa," Performance Evaluation of Routing Protocols Based on Wormhole Attack in Wireless Mesh Networks", Second International Conference on Computer and Network Technology, pp 102-104, 2010.

[39] Rama Krishna Challa ,Mani Arora, Divya Bansal, "Performance Evaluation of Routing Protocols Based on Wormhole Attack in Wireless Mesh Networks", IEEE Second International Conference on Computer and Network Technology, PP 102-104, 2010.

[40] Marianne Azer, Sherif El-Kassas, Magdy El-Soudani, "A Full Image of the Wormhole Attacks Towards Introducing Complex Wormhole Attacks in wireless Ad Hoc Networks", International Journal of Computer Science and Information Security (IJCSIS), PP 41-52, Vol. No. 1, May 2009.

[41] "Analysis on Impact of Black Hole Attack on AODV and AOMDV", CHAPTER 2, available online: http://shodhganga.inflibnet.ac.in/bitstream/10603/24748/7/07_chapter2.pdf.

[42] Juan-Carlos Ruiz, JesúsFriginal, David de-Andrés, Pedro Gil, "Black Hole Attack Injection in Ad hoc Networks".

[43] Fan-Hsun Tseng1, Li-Der Chou1 and Han-Chieh Chao, "A survey of black hole attacks in wireless mobile ad hoc networks", Tseng et al. Human-centric Computing and Information Sciences 2011

[44] NeetikaBhardwaj, Rajdeep Singh, "Detection and Avoidance of Black-hole Attack in AOMDV Protocol in MANETs", International Journal of Application or Innovation in Engineering & Management (IJAIEM), PP. 376 – 383, Volume 3, Issue 5, May 2014

[45] Hu, Y. Perrig, A., and Johnson D., Packet Leashes: "A Defense against Wormhole Attacks in Wireless Network", In Proceedings of the 22nd IEEE International Conference Computer and Communications, Volume 3, pp.1976–1986, April 2003.

[46] P. V. Tran, L. X. Hung, Y. Lee, S. Lee, and H. Lee, TTM: An Efficient Mechanism to Detect Wormhole Attacks in Wireless AdHoc Networks, In Proceeding of 4th IEEE CCNC, pp. 593-598, Las Vegas, USA, Jan. 2007.

[47] C. Sun, K. Doo-young, L. Do-hyeon& J. Jae-il, "WAP: Wormhole Attack Prevention Algorithm in Mobile Ad Hoc Networks," In Proceeding of the IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC), pp. 343-348, 2008.

[48] P Subhash and S Ramachandram, "Preventing Wormholes in Multi-hop Wireless Mesh Networks", Third International Conference on Advanced Computing & Communication Technologies, pp. 293-300, 2013.

[49] S. Capkun, L. Buttyan and J.P., Hubaux, "SECTOR: Secure Tracking of Node Encounters in Multi-hop Wireless Networks", In Proceedings of 1st ACM Workshop on Security of Ad hoc and Sensor Networks (ACM SANS), pp. 21-32, New York, USA, 2003.

[50] L. Hu and D. Evans, "Using Directional Antennas to Prevent Wormhole Attacks," In Network and Distributed System Security Symposium (NDSS), San Diego California, USA, 5-6 February, 2004.

[51] S. Gupta and S. Dharmaraja, "WHOP: Wormhole Attack Detection Protocol using Hound Packet", In International Conference of Innovations in Information Technology, PP. 226 – 231, 2011.

[52] Jian-Ming Chang, Po-Chun Tsou, Han-Chieh Chao, and Jiann-Liang Chen, "CBDS: A Cooperative Bait Detection Scheme to Prevent Malicious Node for MANET Based on Hybrid Defense Architecture," Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronics Systems Technology (Wireless VITAE), 2011 2nd International Conference, pp. 1 - 5, March 2011.

[53] Isaac Woungang, Sanjay Kumar Dhurandher, RajenderDheerajPeddi, and IssaTraore, "Mitigating Collaborative Black hole Attacks on DSRBased Mobile Ad Hoc Networks," Springer-Verlag Berlin Heidelberg, pp. 308-323, October 2013.

[54] Rutvij H. Jhaveri, Sankita J. Patel and Devesh C. Jinwala, "A Novel Approach for GrayHole and BlackHole Attacks in Mobile Ad-hoc Networks," Second International Conference on Advanced Computing & Communication Technologies, pp. 556 - 560 , January 2012.

[55] Saurabh Gupta, SubratKar, and S Dharmaraja, "BAAP: Blackhole Attack Avoidance Protocol for Wireless Network," International Conference on Computer & Communication Technology (ICCCT), November 2011.S