Discovering a Secure Path in MANET by Avoiding Black/Gray Holes

Sarita Choudhary, Kriti Sachdeva

Abstract- Mobile ad hoc networks (MANET) are widely used in places where there is little or no infrastructure. A number of people with mobile devices may connect together to form a large group. Later on they may split into smaller groups. This dynamically changing network topology of MANETs makes it vulnerable for a wide range of attack. In this paper we propose a complete protocol for detection & removal of networking Black/Gray Holes by using OPNET network simulator 14.5; it is the latest version of simulation software. Basically, OPNET allows you to build a network with a range of simulated "real-life" equipment, so different configuration options can be tested. And considering two different networks with 15nodes and 35 nodes in network and evaluating a security attack against MANET as a network, different statistics or performance metrics Packet loss, Packet delivery ratio and Average end to end delay has been used.

Keywords-Mobile Ad-hoc Networks, Black Holes, Gray Holes, Routing, AODV, Routing Table.

I. INTRODUCTION

A mobile ad-hoc network (MANET) is a collection of wireless mobile nodes which have the ability to communicate with each other without having fixed network infrastructure or any central base station. Since mobile nodes are not controlled by any other controlling entity, they have unrestricted mobility and connectivity to others. Routing and network management are done cooperatively by each other nodes. Due to its dynamic nature MANET has larger security issues than conventional networks.

AODV is a source initiated on-demand routing protocol. Every mobile node maintains a routing table that maintains the next hop node information for a route to the destination node.

When a source node wishes to route a packet to a destination node, it uses the specified route if a fresh enough route to the destination node is available in its routing table. If not, it starts a route discovery process by broadcasting the Route Request (RREQ) message to its neighbors, which is further propagated until it reaches an intermediate node with a fresh enough route to the destination node specified in the RREQ, or the destination node itself.

Each intermediate node receiving the RREQ, makes an entry in its routing table for the node that forwarded the RREQ message, and the source node.

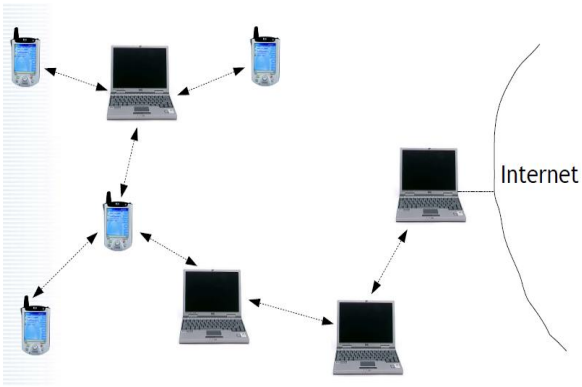

Figure 1 MANET

The destination node or the intermediate node with a fresh enough route to the destination node, unicast the Route Response (RREP) message to the neighboring node from which it received the RREQ. An intermediate node makes an entry for the neighboring node from which it received the RREP, then forwards the RREP in the reverse direction. On receiving the RREP, the source node updates its routing table with an entry for the destination node, and the node from which it received the RREP. The source node starts routing the data packet to the destination node through the neighboring node that first responded with an RREP.

A black hole is a malicious node that falsely replies for any Route Request (RREQ) without having active route to specified destination and drops all the receiving packets. If these malicious nodes work together as a group then the damage will be very serious. This type of attack is called cooperative black hole attack. A gray hole attack is a variation of the black hole attack, where the malicious node is not initially malicious, it turns malicious sometime later.

We present a mechanism to detect and remove the above two types of malicious nodes. Our proposed technique works as follows. Initially a backbone network of trusted nodes is established over the ad hoc network. The source node periodically requests one of the backbone nodes for a restricted (unused) IP address. Whenever the node wants to make a transmission, it not only sends a RREQ in search of destination node but also in search of the restricted IP simultaneously. As the Black/Gray holes send RREP for any RREQ, it replies with RREP for the Restricted IP (RIP) also. If any of the route responds positively with a RREP to any of the restricted IP then the source node initiates the detection procedure for these malicious nodes.

In section2, we discuss the related work on detection/ prevention of black hole attacks. In section3, we discuss the network model and assumption. In section4, we present the methodology and algorithms. Finally the conclusion &discussion of future work is discussed in section5.

Manuscript received on August, 2012.

Assistant Professor Sarita Choudhary Department of Computer Science and Engg., Doon Valley College Of Engg and Technology, Karnal, Haryana, India.

Scholar Kriti Sachdeva Department of Computer Science and Engg, Doon Valley College of Engg. and Technology, Karnal, Haryana, India.

II. LITERATURE REVIEW

Deng et. al.[2] has proposed an algorithm to prevent black hole attacks in ad hoc networks. According to their algorithm, any node on receiving a RREP packet, cross checks with the next hop on the route to the destination from an alternate path. If the next hop either does not have a link to the node that sent the RREP or does not have a route to the destination then the node that sent the RREP is considered as malicious. This technique does not work when the malicious nodes cooperate with each other.

S.Ramaswamy et. al. [3] presented an algorithm to prevent the co-operative black hole attacks in ad hoc network. This algorithm is based on a trust relationship between the nodes, and hence it cannot tackle gray hole attacks .Besides due to intensive cross checking, the algorithm takes more time to complete, even when the network is not under attack.

S.Banerjee et. al. [4] has also proposed an algorithm for detection & removal of Black/Gray Holes. According to their algorithm instead of sending the total data traffic at once, they divide it into small sized blocks, in the hope that the malicious nodes can be detected& removed in between transmission. Flow of traffic is monitored by the neighbors of each node. Source node uses the acknowledgement sent by the destination to check for data loss & in turn evaluates the possibility of a black hole. However in this mechanism false positives may occur and the algorithm may report that a node is misbehaving, when in fact it is not.

Finally P.Agarwal et. al. [5] have proposed a technique of establishing a backbone network of strong nodes. With the assistance of the backbone network of strong nodes, source and destination nodes carry out an end to end checking to determine if all the data packets reached the destination. If checking results in a failure, then the backbone network initiates a protocol for detecting the malicious nodes.

We have used this concept of backbone nodes & designed an algorithm that is much simpler.

We have also made use of the concept of state full approach of IP addresses allocation in ad-hoc networks as discussed by S.Indrasinghe et.al. [6] and Mansoor Mohsin et. al. [7]

III. NETWORK MODEL & ASSUMPTION

We approach this problem by selecting some nodes which are trustworthy and powerful in terms of battery power and range. These nodes which are referred to as Back Bone Nodes (BBN) will form a Back Bone network and has special functions unlike normal nodes. For the co-ordination between the Back Bone Nodes (BBN) and the Normal Nodes, it is assumed that the network is divided into several grids. It is assumed that the nodes, when initially enters the network is capable of finding their respective grid locations. It is also assumed that the numbers of normal nodes are more than the number of black/gray nodes at any point of time.

3.1 Core Maintenance of the Allocation Table:-

In this approach only the backbone network in MANET is permitted to select the IP addresses for unconfigured hosts. The mechanism is based on allocating a conflict free address to all newly arrived nodes by using multiple disjoint address spaces [6].Each BBN in MANET is responsible for allocating a range of addresses disjoint from the ranges of all other BBN. In other words each BBN generates numbers that are unique for that host. Every hosts in the MANET must have the possibility to reach one of the Backbone Nodes (BBN) all the time.

IV. METHODOLOGY & ALGORITHM

The main idea behind this method is to list out the set of malicious nodes locally at each node whenever they act as a source node. As mentioned in the Assumption our protocol uses the concept of Core Maintenance of the Allocation Table ie, whenever a new node joins the network, it sends a broadcast message as a request for IP address.

The backbone node on receiving this message randomly selects one of the free IP addresses. The new node on receiving the allotted IP address sends an acknowledgement to the BBN. Now since the allocation is only under the control of the Back Bone Nodes(BBN) the dynamic pool of unused/restricted IPs of the network at any point of time is known only to the BBN.

4.1 Algorithm

Actions by Source Node (SN)

Step 1: Source Node (SN) sends a Request to RestrictedIP (RRIP) to the Backbone Node (BBN).

Step 2: On receiving the Restricted IP(RIP), from the BBN it sends the RREQ for the Destination as well as for the RIP simultaneously.

Step 3: Waits for RREP.

Actions by Intermediate Node/Destination Node

Step 1: On receiving the RREQ it first makes an entry in its Routing table for the node that forwarded the RREQ.

Step 2: If it is the Destination node or if it has a fresh enough route to the Destination node, it replies to the RREQ with an RREP.

Step 3: If it is neither the destination nor does it have a fresh enough route to the Destination, then it forwards the RREQ to its neighbours.

Step 4: On receiving an RREP, it again makes a note of the node that sent the RREQ in its routing table & then forwards the RREP in the reverse direction.

Step 5: On receiving a request to enter into the promiscuous mode, it starts listening in the network for all the packets destined to that particular IP address & monitors its neighbours, for the movement of the dummy data packet.

Step6: In case, it finds out that the dummy data packet loss is exceptionally more than the normal data packet at any particular node, it informs back the IP of this IN.

4.1.1 Gray/Black Hole Removal process

Actions by Source node on receiving the RREP

Step 1: If the RREP is received only to the Destination & not to the Restricted IP (RIP), the node carries out the normal functioning by transmitting the data through the route.

Step 2: If the RREP is received for the RIP, it initiates the process of black hole detection, by sending a request to enter into promiscuous mode, to the nodes in an alternate path (i.e. neighbours of next hop for RIP).

Step 3: The feedback sent by the alternate paths are analyzed to detect the black hole & this information is propagated throughout the Network, leading to the revocation of the Black Holes certificates.

V. IMPLEMENTATION AND ANALYSIS

5.1 Implementation

Simulation using OPNET Modeler was used to investigate the performance impact of a collaborative blackhole attack on a mobile ad hoc network. Network throughput, packet delivery ratio and end-to-end delay are the performance metrics used in our result analysis. Based on the analyses of performance metrics made, we realized the consequences of a collaborative blackhole attack on MANET.

In our proposed work we consider three metrics to evaluate the performance mentioned below –

a) Performance Metrics

In evaluating a MANET routing protocol as well as evaluating a security attack against MANET as a network, different statistics or performance metrics are used. In this subsection, we discuss the essential metrics required to evaluate and determine the possibility of multiple node attacks on a MANET. The performance metrics:

5.1.1 Network throughput

5.1.2 End to end delay

5.1.3 Packet delivery ratio

5.1.1 Network throughput

A network throughput is the average rate at which message is successfully delivered between a receiver (destination node) and its sender (source node). It is also referred to as the ratio of the amount of data received from its sender to the time the last packet reaches its destination. Throughput can be measured as bits per second (bps), packets per second or packet per time slot and OPNET Modeler expresses it using bits per second. For a network, it is required that the throughput is at high-level. Some factors that affect MANET's throughput are mentioned in: these are unreliable communication, changes in topology, limited energy and bandwidth.

5.1.2 End-to-end delay

Packet end-to-end delay is the time delay it takes a network source to deliver a packet to its destination. Thus, the end-to-end delay of packets is the total amount of delays encountered in the whole network at every hop going to its destination. In MANETs, this kind of delay is usually caused by certain connection tearing or/and the signal strength among nodes been low. The reliability of a routing protocol can be determined by its end-to-end delay on a network, thus a steadfast MANET routing gives less packet end-to-end delay.

5.1.3 Packet delivery ratio

This refers to the ratio of the total number of data packets that reach the receiver (destination node) to the total number of data packets sent by the source node. This is another performance metric that is used to determine the efficiency and accuracy of MANET's routing protocol because it is used to calculate the rate of loosing packets. Similar to the network throughput, packet delivery ratio (PDR) is expected to be high.

b) Scenarios

Different scenarios can be created in a simulation in OPNET. We created different scenarios during the simulation model in order to provide another phase of designed project space that we used for different experiments and results analyses. Another reason for having different scenarios is to enable us to determine the consequences of mobile network under regular operation, under collaborative attack and in terms of varying network size. Here, we present the various results obtained in our two main scenarios and explain each scenario.

1) Scenario 1: 15-Node MANET Network

First scenario is simulation of a small network of 15 mobile nodes. In this scenario, we carried out two different simulations. The first simulation in this scenario is building a regular MANET in terms of noting the outcome and behaviour of nodes of the mobile ad-hoc network without any form of attack launched on them. This would enable us to take note and measure the effects of the network when there is an attack (in second simulation). We carried out different simulations that were run many times to ascertain the results and we were able to present relevant and comparable results.

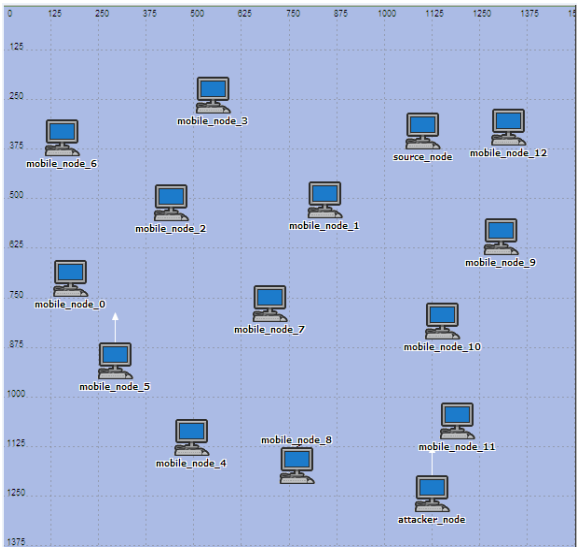

Figure-1 Scenario-1 workspace with 15-nodes

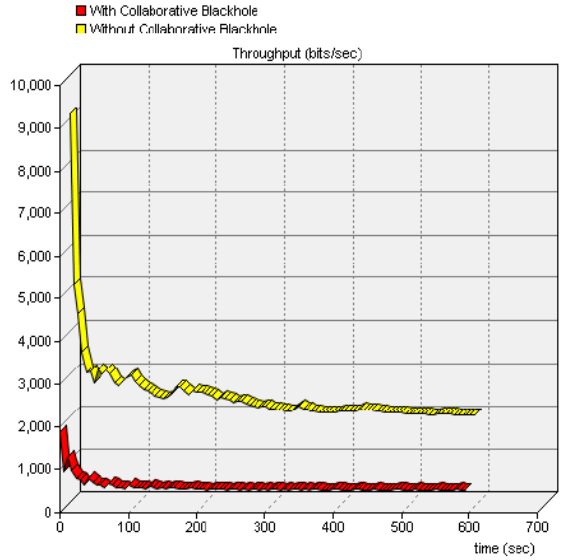

Figure a) Throughput of 15-node MANET Network

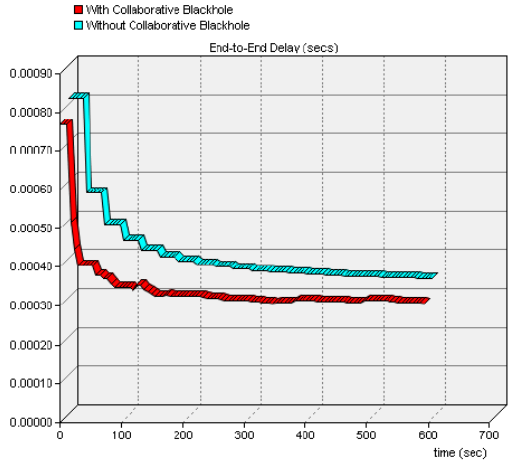

Figure b) Packet Delivery Ratio of 15-node MANET Network

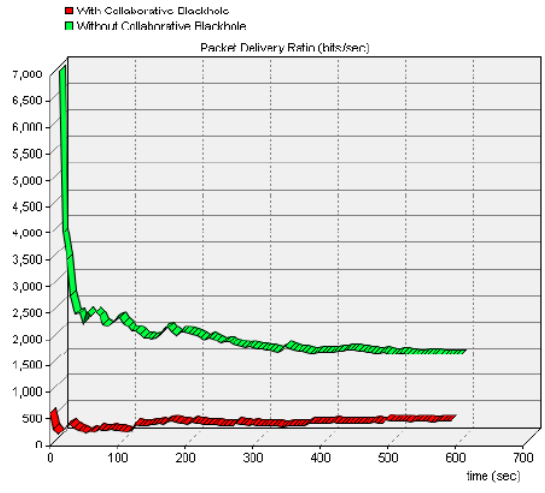

Figure c) End-to-End Delay of 15-node MANET Network

2) Scenario 2: 35-Node MANET Network

In the second scenario; a simulation of a larger network in term of size compared to the first scenario. The network environment is still the same 1 x 1 kilometre square pace of a campus network but the network size is bigger; having 35 mobile nodes compared to the earlier two simulations with 15 mobile nodes. Here, we present two simulations in which the first is a network of MANET under regular operation while the latter is a MANET network under direct collaborative attack and both include 35 nodes. The model layout in this scenario is similar to that depicted in figure-2 except that it contains mobile nodes 0 to 34.

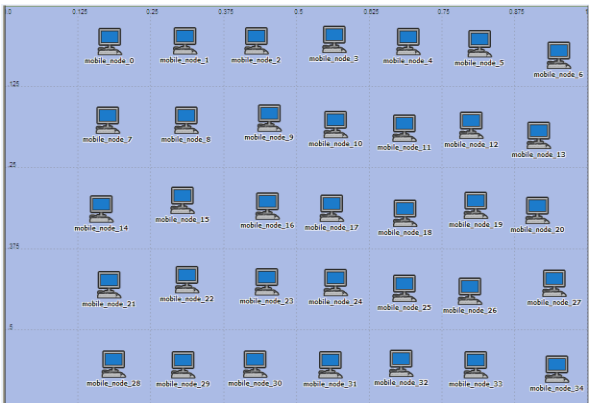

Figure-2 Scenario-2 workspace with 35-nodes

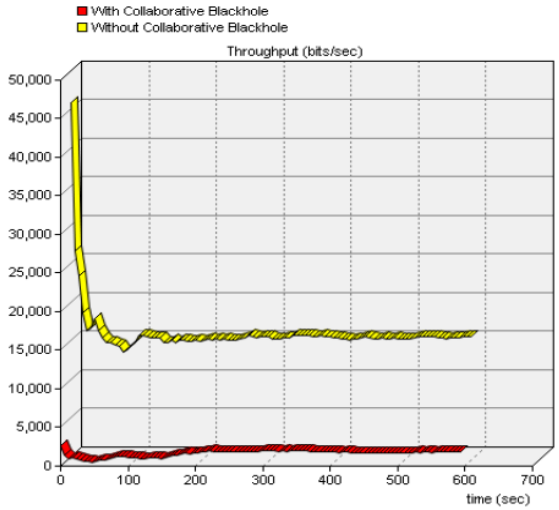

Figure a) Throughput of 35-node MANET Network

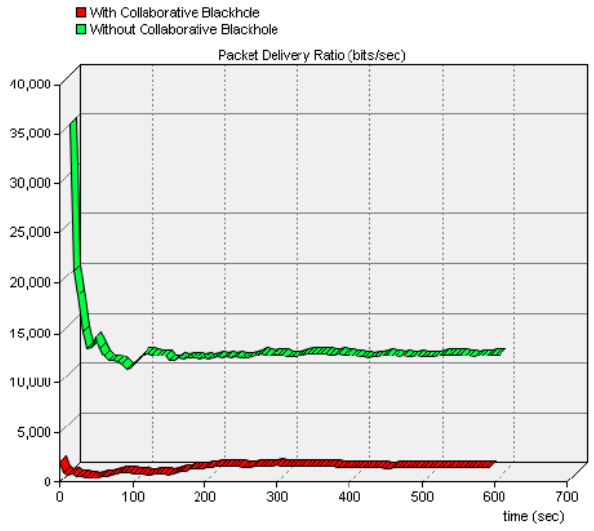

Figure b) Packet Delivery Ratio of 35-node MANET Network

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

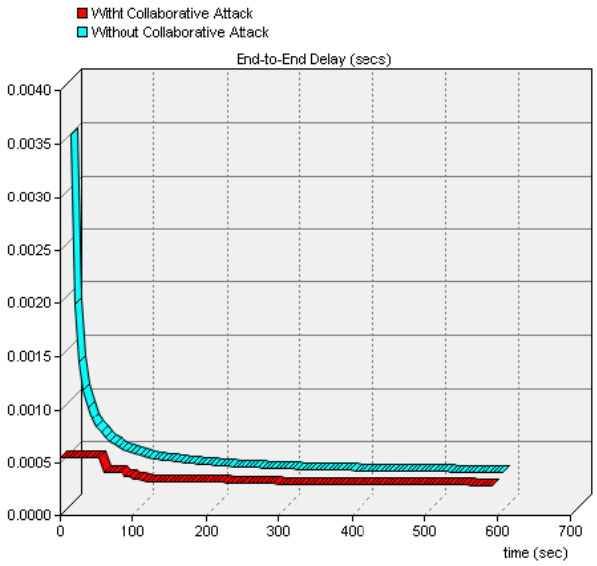

Figure c) End-to-End Delay of 35-node MANET Network

5.2 ANALYSIS

5.2.1 Scenario 1 vs. Scenario 2

In comparing scenarios 1 and 2 with all the results presented and also when comparing the data in tables 1 & 2; we observe that our measurement based on some metrics; throughput, packet delivery ratio and end-to-end delay, scenario 2 has higher network performance both when the MANET was with and without collaborative black hole attack. This is expected because of the obvious reason that scenario 2 has higher number of mobile nodes compared to scenario 1. On the other hand, comparing the margins of each performance parameter of the different scenarios, we observe that the rate of degradation and collaborative effects of the malicious nodes make the data margin of scenario 2 to be wider. This is as a result of the collaborative black hole attack, which affects more nodes compared to the number of nodes affected in scenario 1. In order to find differences in the simulation results and to be able to compare results, our simulation was performed in two scenarios based on different network sizes. Each scenario has first experiment for regular operation of MANET and second experiment for MANET operation under a collaborative black hole attack. Our experiments show encouraging results obtained from the two scenarios of the simulation. The regular MANET outperforms the MANET under attack in terms of throughput and packet delivery ratio. These results show the effect of the collaborative black hole attack on MANET because the packet delivery ratio and throughput of a good network is usually high. On the other hand, in terms of the end-to-end delay performance metric, the result obtained when the MANET was under collaborative black hole attack shows there was a slight decrease in the delay because the malicious nodes provide a quick route reply to the source node claiming to be benign nodes and having the shortest route to the desired destination node. In conclusion, we detect that the larger the MANET network size is in terms of the number of nodes, the more nodes that would be compromised and thus malicious; the more powerful the effect of the collaborative attack would be in terms of degradation of performance.

Table-1: Scenario 1: Data of 15-Node MANET Network

Scenario 1: Data of 15-Node			
Metrics	Value	Sim1:Regular operation	Sim2:Colaborative Blackhole operation
Throughput bits/sec	Initial	9072.00	1861.33
	Final	2008.16	506.03
	Minimum	2001.14	502.74
	Maximum	9072.00	1861.331
Packet Delivery Ratio	Initial	6912.00	597.33
	Final	1530.03	440.48
	Minimum	1524.48	199.11
	Maximum	6912.00	597.33
End-To-End Delay	Initial	0.0008120	0.0007659
	Final	0.0003465	0.0003055
	Minimum	0.0003465	0.0003052
	Maximum	0.0008120	0.0007659

Table-2: Scenario 2: Data of 35-Node MANET Network

Scenario 2: Data of 35-Node			
Metrics	Value	Sim3:Regul	Sim4:Colaborati
Throughput bits/sec	Initial	45808.00	2576.00
	Final	15485.12	1781.00
	Minimu	13512.00	444.30
	Maximu	45808.00	2576.00
Packet Delivery Ratio	Initial	34901.00	1962.67
	Final	11798.18	1479.90
	Minimu	10294.86	343.56
	Maximu	34901.33	1962.67
End-To-End Delay	Initial	0.0034772	0.0005455
	Final	0.0003078	0.0002874
	Minimu	0.0003079	0.0002874
	Maximu	0.0034772	0.0005455

VI. CONCLUSION AND FUTURE WORK

The simulation results are analyzed to draw the final conclusion about two different network scenarios with 15 and 35 nodes. These results show the effect of the collaborative black hole attack on MANET because the packet delivery ratio and throughput of a good network is usually high. On the other hand, in terms of the end-to-end delay performance metric, the result obtained when the MANET was under collaborative black hole attack shows there was a slight decrease in the delay because the malicious nodes (Black/Gray holes) provide a quick route reply to the source node claiming to be benign nodes and having the shortest route to the desired destination node. Comparing the margins of each performance parameter throughput, Packet Delivery Ratio, end-to-end delay of the different scenarios, we observe that the rate of degradation and collaborative effects of the malicious nodes make the data margin of scenario 2 to be wider. This is as a result of the collaborative black hole attack, which affects more nodes compared to the number of nodes affected in scenario1.

REFERENCES

1. "Security Issues in Mobile Ad Hoc Networks- A Survey" Wenjia Li and Anupam Joshi, Department of Computer Science and Electrical Engineering, University of Maryland, Baltimore County.
2. Hongmei Deng, Wei Li, and Dharma P. Agrawal, "Routing Security in Wireless Ad Hoc Network", IEEE Communications Magzine, vol. 40, pp. 70-75, 2002.
3. Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya, John Dixon, and Kendall Nygard, "Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks". In Proceedings of 2003 International Conference on Wireless Networks (ICWN'03), Las Vegas, Nevada, USA, pp. 570-575.
4. Sukla Banerjee "Detection/Removal of Cooperative Black and Gray Hole Attack in Mobile Ad-Hoc Networks" Proceedings of the World Congress on Engineering and Computer Science 2008 WCECS 2008, October 22 - 24, 2008, San Francisco, USA
5. Piyush Agrawal, R. K. Ghosh, Sajal K. Das, Cooperative Black and Gray Hole Attacks in Mobile Ad Hoc Networks In Proceedings of the 2nd international conference on Ubiquitous information management and communication, Pages 310-314, Suwon, Korea, 2008.
6. Sudath Indrasinghe, Rubem Pereira, John Haggerty,"Conflict Free Address Allocation Mechanism for Mobile Ad Hoc Networks", 21st International Conference on Advanced Information Networking and Applications Workshops (AINAW'07)
7. Mansoor Mohsin and Ravi Prakash,"IP Address Assignment in a mobile ad hoc network", The University of Texas at Dallas Richardson, TX Kaixin Xu, Xiaoyan Hong, Mario Gerla Computer Science Department at UCLA, Los Angeles, CA 90095 project under contract N00014-01-C-0016
8. Poongothai T. and Jayarajan K., "A non-cooperative game approach for intrusion detection in Mobile Adhoc networks", International Conference of Computing, Communication and Networking (ICCC), 18-20 Dec 2008, St. Thomas, VI, pp 1-4
9. Bo Sun,Yong Guan,Jian Chen,Udo , "Detecting Black-hole Attack in Mobile Ad Hoc Network" , The institute of Electrical Engineers, Printed and published by IEEE, 2003.
10. Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, and Yoshiaki Nemoto, "Detecting Black hole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method", International Journal of Network Security, Vol.5, issue 3, Nov 2007, pp 338–346.
11. Chang Wu Yu, Tung-Kuang Wu, Rei Heng Cheng, and Shun Chao Chang,"A Distributed and Cooperative Black Hole Node Detection and Elimination Mechanism for Ad Hoc Network" , Springer-Verlag Berlin Heidelberg, 2007.
12. Payal N. Raj and Prashant B. Swadas, "DPRAODV: A dynamic learning system against black hole attack in AODV based MANET", International Journal of Computer Science Issues (IJCSI), Volume 2, Number 3, 2009, pp 54-59
13. S. Ramaswamy, H. Fu, M. Sreekantaradhya, J. Dixon, and K. Nygard, "Prevention of cooperative black hole attack in wireless ad hoc networks," International Conference (ICWN'03), Las Vegas, Nevada, USA, 2003, pp 570-575
14. Mohammad Al-Shurman, Seong-Moo Yoon and Seungjin Park, "Black Hole Attack in Mobile Ad Hoc Networks", ACM Southeast Regional Conference , Proceedings of the 42nd annual Southeast regional conference, 2004, pp 96-97
15. Chang Wu Yu, Tung-Kuang, Wu, Rei Heng, Cheng and Shun Chao Chang, "A Distributed and Cooperative Black Hole Node Detection and Elimination Mechanism for Ad Hoc Networks", PAKDD 2007 International Workshop, May 2007, Nanjing, China, pp 538–549
16. Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, and Yoshiaki Nemoto, "Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method", International Journal of Network Security, Volume 5, Number 3, 2007, pp 338–346
17. Hongmei Deng, Wei Li, and Dharma P. Agrawal, "Routing Security in Wireless Ad Hoc Network", IEEE Communications Magazine, Volume 40, Number 10, 2002, pp 70-75
18. Latha Tamilselvan and V Sankaranarayanan, "Prevention of Black hole Attack in MANET", Journal of networks, Volume 3, Number 5, 2008, pp 13-20
19. Bo Sun Yong, Guan Jian Chen and Udo W. Pooch, "Detecting Black-hole Attack in Mobile Ad Hoc Networks", The Institution of Electrical Engineers (IEE) ,Volume 5, Number 6, 2003, pp 490-495
20. Marc Greis, "Tutorial for the Network Simulator",
21. http:// www.isi.edu/nsnam/ns/tutorial/index.html.
22. http://en.wikipedia.org/wiki/Personal_area_network, 25 July 2005.
23. T. Franklin, "Wireless Local Area Networks", Technical Report http://www.jisc.ac.uk/uploaded_documents/WirelessLANTechRep.pdf. 25 July 2005.
24. J. Reynold, "Going Wi-Fi", Chapter 6, The Wi-Fi Standards Spelled out, Pg. 77.
25. http://certifications.wi-fi.org/wbcs_certified_products.php 25 July 2005.
26. P. Misra,. "Routing Protocols for Ad Hoc Mobile Wireless Networks",http://www.cse.wustl.edu/~jain/cis788-99/adhoc_routing/index.html, 14 May 2006.
27. P. Yau and C. J. Mitchell, "Security Vulnerabilities in Adhoc Network".
28. G. Vigna, S. Gwalani and K. Srinivasan, "An Intrusion Detection Tool for AODV-Based Ad hoc Wireless Networks", Proc. of the 20th Annual Computer Security Applications Conference (ACSAC'04).
29. P. Ning and K. Sun, "How to Misuse AODV: A Case Study of Insider Attacks Against Mobile Ad-Hoc Routing Protocols", Proc.of the 2003 IEEE Workshop on Information Assurance United States Military Academy, West Point, NY., June 2003. Computer Science, 2008

AUTHOR PROFILE

SARITA CHOUDHARY received her B.Tech and M.Tech degree in Computer Science & Engineering Department from Vaish College of Engineering Rohtak (affiliated to M.D.U,Rohtak) and is working as a Assistant Professor in Computer Science & Engineering Department of Doon Valley Institute of Engineering & Technology (DIET) College, Karnal, Haryana.

KRITI SACHDEVA received her B.Tech degree in Computer Engineering from Haryana Engineering College (affiliated to Kurukshetra University). And is pursuing M.Tech in Computer Science & Engineering Department from Doon Valley Institute of Engineering & Technology (DIET) College, Karnal, Haryana.