Survey Enhancement of Modified DSR protocol For Removal and Detection of Selective Black Hole Attack in MANET

Rahul Vasant Chavan, M S Choudhari, R A Ghatage

Abstract— **A black hole attack in ad hoc network refers to an attack by malicious nodes, which forcibly acquires the route from a source to destination by falsely advertising shortest hop count to reach the destination node. In this paper, we present a Modified Dynamic Source Routing Protocol (MDSR) to detect and prevent selective black hole attack. Selective black hole attack is a special kind of black hole attack where malicious nodes drop the data packets selectively. We proposed an Intrusion Detection System (IDS) where the IDS nodes are set in promiscuous mode only when required, to detect the abnormal difference in the of data packets being forwarded by a node. When any anomaly is detected, the nearby IDS node broadcast the block message, informing all nodes on the network to cooperatively isolate the malicious node from the network. The proposed technique employs Glomosim to validate the effectiveness of proposed intrusion detection system.**

Index Terms—**About four key words or phrases in alphabetical order, separated by commas.**

I. Introduction

The black hole attack is one of the well-known security threats in wireless mobile ad-hoc networks. The intruders utilize the loophole to carry out their malicious behaviors because the route discovery process is necessary and inevitable. Many researchers have conducted different detection techniques to propose different types of detection schemes. In this paper, we survey the existing solutions and discuss the state-of-the-art routing methods. We not only classify these proposals into single black hole attack and collaborative black hole attack but also analyze the categories of these solutions and provide a comparison table. We expect to furnish more researchers with a detailed work in anticipation. . A black hole attack in ad hoc network refers to an attack by malicious nodes . In a wireless Mobile Ad hoc Network (MANET), there are no routers or access points; data transfer among nodes is achieved by means of multiple hops. Every mobile node acts both as a host and as a router to establish a route. When a source node intends to transfer data to a destination node, packets are transferred through the intermediate nodes, thus, searching for and quickly establishing a route from a source to a destination node is an Important issue for MANETs. The currently available routing protocols of MANET are mainly categorized into proactive and reactive routing protocols.

A.PROBLEM DEFINITION

In Black Hole Attack within fraction of second huge amount of packet sending will be done so at the time of sending packet in between sender to receiver how to provide security to all the data or node is the important problem in mobile ad-hoc network.

B.PROTOCOLS IN MANET

I. Proactive routing protocol
II. Reactive Routing Protocol

In a proactive routing protocol such as DSDV (Destination Sequence Distance Vector) [1] and OLSR (Optimized Link StateRouting Protocol) [1], every node retroactively searches for routes to other nodes, and periodically exchanges routing messages, in order to keep the formation in the routing table up-to-date and correct. Due to limitation in power and bandwidth of MANET nodes, frequent transmission of routing messages would lead to congestion of the network. In a reactive routing protocol such as AODV (Ad hoc On-Demand Distance Vector) [1] or DSR (Dynamic Source Routing) [2], a route is searched and established only when two nodes intend to transfer data. Because most of these routing protocols assume cooperation between nodes for packet forwarding, a malicious node can launch routing attacks that disrupts the normal routing operations or Denial-Of-Service (DOS) attacks such as black hole or gray hole attack that denies the service to the legitimate nodes on MANET.

C.OBJECTIVE AND PROPOSED WORK

In a wireless Mobile Ad hoc Network (MANET), there are no routers or access points; data transfer among nodes is achieved by means of multiple hops. Every mobile node acts both as a host and as a router to establish a route. When a

Manuscript received Oct, 2014.

Rahul V. Chavan*, Department of computer engineering, sinhgad institute of technology, pune, Pune, India, 9503475101.*
Manohar S Choudhari*, Department of computer engineering, Sinhgad Institute Of Technology, Pune, India, 94038317984.*
Rahul Anil Ghatage*, Department of computer engineering, imperial college of engineering & research, Pune, India, 9975251285.*

source node intends to transfer data to a destination node, packets are transferred through

The intermediate nodes, thus, searching for and quickly establishing a route from a source to a destination node is an important issue for MANETs.so the main objective of our paper is to provide security to the intermediate node.in our searvey enhancement we are going to focusing on both co-operative black hole attack and gray hole attack also.so the some information of this attack is given below.

B.PREVENTION OF CO-OPERATIVE BLACK HOLE ATTACK

I. AODV Routing Protocols

The Ad Hoc On-Demand Distance Vector (AODV) routing protocol is an adaptation of the DSDV protocol for dynamic link conditions [10(1)]. Every node in an Ad-hoc network maintains a routing table, which contains information about the route to a particular destination. Whenever a packet is to be sent by a node, it checks with its routing table to determine whether a route to the destination is already available. If so, it uses that route to send the packets to the destination. If a route is not available or the previously entered route is inactivated, then the node initiates a route discovery process.

A RREQ (Route REQuest) packet is broadcasted by the node. Every node that receives the RREQ packet checks if it is the destination for that packet and if so, it sends back an RREP (Route Reply) packet. If it is not the destination, then it checks with its routing table to determine if it has got a route to the destination. If not, it relays the RREQ packet by broadcasting it to its neighbors. If its routing table does contain an entry to the destination, then the next step is the comparison of the Destination Sequence number in its routing table to that present in the RREQ packet. This Destination Sequence number is the sequence number of the last sent packet from the destination to the source. If the destination sequence number present in the routing table is lesser than or equal to the one contained in the RREQ packet, then the node relays the request further to its neighbors. If the number in the routing table is higher than the number in the packet, it denotes that the route is a fresh Route and packets can be sent through this route. This intermediate node then sends a RREP packet to the node through which it received the RREQ packet. The RREP Packet gets relayed back to the source through the reverse route. The source node then updates its routing table and sends its packet through this route. During the operation, if any node identifies a link failure it sends a RERR (Route Error) packet to all other nodes that uses this link for their communication to other nodes. This paper provides routing security to the AODV routing protocol by eliminating the threat of Black Hole attacks.

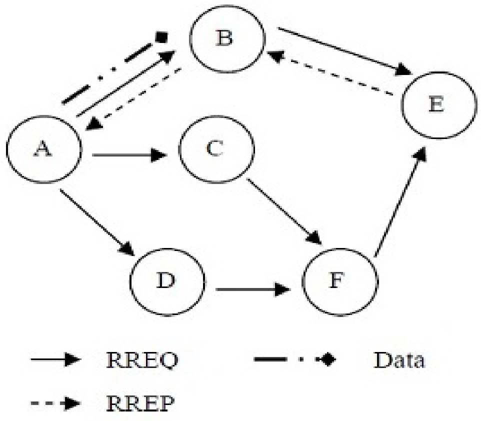
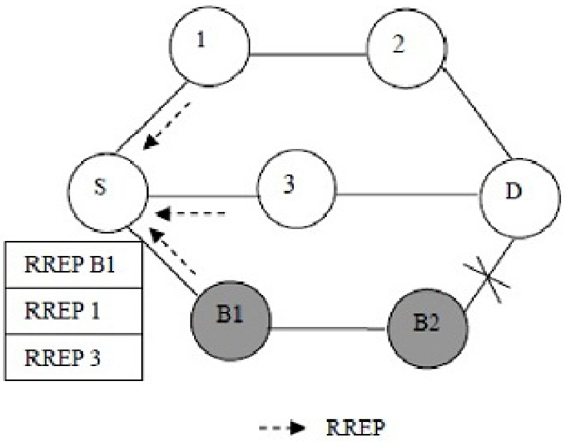


Figure 3.1: Propagation of RREQ RREP from A to E Ref. Paper NO [10(2)] This is illustrated in _gure 3 .Since AODV has no security mechanisms, malicious nodes can perform many attacks just by not behaving according to the AODV rules. A malicious node M can carry out many attacks against AODV.A Black Hole attack [1][5][20] is a kind of denial of service where a malicious node can attract all packets by falsely claiming a fresh route to the destination and then absorb them without forwarding them to the destination. Cooperative Black hole means the malicious nodes act in a group [15].Here node S is the source node and D is the destination node. Nodes 1 to 5 act as the intermediate nodes. Nodes 4 (B1) and 5 (B2) act as the cooperative Black holes. When the source node wishes to transmit a data packet to the destination, it request sends out the RREQ packet to the neighboring nodes. The malicious nodes being part of the network, also receive the RREQ. Since the Black hole nodes have the characteristic of responding request to any RREQ, it immediately sends out the RREP. The RREP from the Black hole B1 reaches the source node, well ahead of the other RREPs, as it can be seen from the figure 3. Now on receiving the RREP from B1, the source starts transmitting the data packets. On the receipt of data packets, B1 simply drops them, instead of forwarding to the The source node transmits the RREQ to all its neighbors. Then the source Waits for TIMER seconds to collect the replies, RREP. A reply is chosen based on the following criteria. In each of the received RREP, the fidelity level of the responding node, and each of its next hops level are checked. If two or more routes seem to have the same fidelity level, then select the one with the least hop count; else, select the one with the Highest level. The fidelity levels of the participating nodes are updated based on their faithful participation in the network. On receiving the data packets, the destination Node will send an acknowledgement to the source, whereby the intermediate node level will be incremented. If no acknowledgement is received, the intermediate nodes level will be decremented.

B. Working principle of PCBHA

I. Collecting response

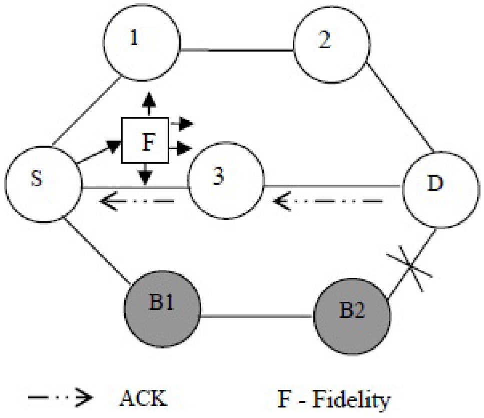
The incoming responses are collected in a table, namely, the Response table. The entries will have fields like, source address, destination address, hop count, next hop, lifetime, and destination sequence number, source and destinations header address. The responses will be collected till a timer expiry event. This is illustrated in figure



II CHOSING RESPONSES

A valid route is selected from among the received responses based on the following methodology. A fidelity table is maintained that will hold the fidelity levels of the participating nodes. The basic idea is to select the node with a high fidelity level. Initially the fidelity levels of the responded node and its next hop are looked

for. If the average of their levels is found to be above the specified threshold, then the node is considered to be reliable. On the receipt of multiple responses, the one with the highest fidelity level is chosen. In case, two or more nodes seemed to have the same fidelity levels, then the one with the minimum hop count is chosen. As shown in Figure 3d, the source S chooses the response RREP-3, as highlighted, after checking the _delity levels. It then transmits the data packets.



On receiving the acknowledgement, as seen in Figure 5, the fidelity levels of the respective nodes are incremented, and the fidelity packets are exchanged.

III.RELATED WORK

Black hole attacks have serious impact on reactive routing protocols such as AODV or DSR. It had drawn significant attention in recent research activities and many secure routing protocols have been proposed to mitigate single and cooperative black hole attacks[1(2)].Gray hole attack is a special kind of black hole attack (selective forwarding attack) in which a malicious nodes behavior is exceptionally unpredictable. The gray hole nodes can perform the attack in three different ways: (i) The malicious node may drop packets from certain nodes while forwards all other packets.(ii) A node may behave maliciously for a certain time, dropping packets selectively. (iii) Is the combination of both attacks, i.e. the malicious node may drop packets from Suspicious nodes for certain time only, later it behaves as a normal node. Due to these characteristics, detection of gray hole attacks is very hard. A gray hole attack can disturb route discovery process and degrade networks performance. Both black hole and gray hole attacks can be easily launched on reactive routing protocols like AODV and DSR .In a new routing security scheme based on the reputation evaluation in hierarchical ad-hoc networks is proposed. The reputation relation is built based on the behaviors and correlation of the node. It has the incentive mechanism to promote the cooperation of cluster members for forwarding data packets and to increase the activity probability of cluster members in the network. Karlof and Wagner theory proposed selective forwarding attacks and suggested that multi path forwarding can be used to counter these attacks in sensor networks. However, the algorithm fails to suggest a method to detect and isolate the attackers from the network. In the authors propose a scheme that randomly selects part of the intermediate nodes along a forwarding path as checkpoint nodes Which are responsible for generating acknowledgments for each packet received. If suspicious behavior is detected, it will generate an alarm packet and deliver it to source node.[1(2)].

IV Intrusion Detection System in MANET

In the Ref no[25], This paper presents an approach to prevent attacks in MANETs by deploying intrusion detection nodes. Some nodes performing Intrusion Detection Systems, IDS nodes for short, are used to mitigate attacks. Two kinds of attacks, wormhole attacks and black hole attacks are addressed in the paper. The modules used to mitigate wormhole and black hole attacks are called Anti-Worm and Anti-Black hole, respectively, in this paper. The IDS nodes are set in singling mode in order to estimate the suspicious value of a node within the communication range, according to the routing messages transmitted by the node. When the suspicious value of a node exceeds a threshold, an IDS nearby will broadcast a block message to inform all nodes on the network, asking them to cooperatively isolate the malicious node. This research tried to propose an IDS that can detect both wormhole and black hoe attacks through modifying the algorithms proposed in and. Because in the real world we could predict what kind of attack would occur, so as to deploy a detection system with unique function in advance.The proposed modifications, AntiWorm and AnTiBlackhole,now can share the same tables to against wormhole attacks and black hole attacks, respectively. That means regular nodes and IDS nodes can keep the necessary information for detecting both attacks. In the near future, we expect to merge the two modules into one multifunctional IDS system. Currently, when there are two (one pair) wormhole nodes, the average rate of total packets lost is increased to 49.63 percent with the deployment of 9 IDS nodes performing Anti-Worm, the packet loss rate can be decreased to 28.17 percent in average. As to the black hole attacks, considering one black hole node the total packet loss rate rises to about 90.42 percent[25(4)]. In a context adaptive IDS system has been proposed which is able to dynamically adapt to contextual factors at a given node such as residual energy, potential security threats and transction loading to accommodate and inspect new arriving packets.

There is a need for an IDS to implement an intelligent control mechanism in order to monitor and recognize security breach attempts efficiently over a period of the expected network lifetime. By leveraging the Network Node Intrusion Detection (NNID) strategy, we developed a context adaptive IDS controller that advises an IDS to carry out intrusion detection while being prepared for a possible cut through if it is likely that the residual energy is not sufficient. By being embedded with the context adaptive IDS controller, the proposed Context Adaptive Intrusion Detection System (CAIDS) is able to adapt to the current node context (such as residual energy, security threats and loading) for accommodating and inspecting new arriving packets. The performance is evaluated using a reward function that discovers an effective way to perform Intrusion detection and delivers security benefits while meeting the energy budget.

II. Conclusion

We have reviewed current studies of, a light weight solution methodology which is a simple acknowledgement scheme to detect gray hole nodes in MANET. It can be incorporated with any existing on demand ad hoc routing protocols. By the proposed algorithm, the destination node detects the presence of malicious nodes in the source route and with the help of intrusion detection system the malicious nodes are isolated from the network. Also our IDS nodes will turn into promiscuous listening only in the presence of suspected nodes resulting less energy loss, which makes our method suitable for the resource constrained characteristics of MANET.Regarding the comparative results of related work.

REFERENCES

[1] M. Mohanapriya,Ilango Krishnamurthi."Modi_ed DSR protocol for detection and removal of selective".Computers and Electrical Engineering 40 (2014) 530538.

[2] Karlof C, Wagner D. "Secure routing in wireless sensor networks: attacks and countermeasures". Elseviers Ad hoc Networks J September 2003;1(23):293315 [Special Issue on Sensor Network Applications and Protocols].

[3] Xiao B, Yu B, Gao C. CHEMAS: identify suspect nodes in selective forwarding attacks. J Parallel Distributed Comput 2007;67(11):1230.

[4] Wang Wei, Zeng Guosun, Yao Jing, Wanga Hanli, Tang Daizhong. "Towards reliable self-clustering mobile ad hoc networks". Comput Electr Eng 2012;38:55162.

[5] Ming-Yang Su. "Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems". Comput Commun 2010.

[6] Tamilselvan Latha, Sankaranarayanan V."Prevention of co-operative black holeattack in MANET".J Networks 2008;3(5):1320.

[7] Kurosawa Satoshi, Nakayama Hidehisa, Kato Nei, Jamalipour Abbas,Nemoto Yoshiaki. "Detecting blackhole attack on AODV-based mobile ad hoc networks by dynamic learning method". Int J Network Security 2007;5(3):33846.

[8] Cheng Bo-Chao, Tseng Ryh-Yuh. "A context adaptive intrusion detection sys- tem for MANET". Comput Commun 2011;34:3108.

[9] Hongmei Deng, Wei Li, and Dharma P. Agarwal, Routing Security in Wireless Ad Hoc Networks, University of Cincinnati, IEEE Communications magazine,Vol.40, no.10, October 2002.

[10] C.E. Perkins, S.R. Das, and E. Royer, Ad-Hoc on Demand Distance Vec- tor (AODV), March 2000, http://www.ietf.org/internet-drafts/draft-ietf-manet-aodv-05.txt

[11] Lidong zhou, Zygmunt J. Haas, Securing Ad Hoc Networks, IEEE network, special issue on network security, Vol.13, no.6, November/December 1999.

[12] Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya, John Dixon and Kendall Nygard, Prevention of Cooperative Black Hole Attack in Wireless AdHoc,www.cs.ndsu.nodak.edu/nygard/research /BlackHoleMANET.pdf 2003 .

[13] Bracha Hod, Cooperative and Reliable Packet-Forwarding On Top of AODV, www.cs.huji.ac.il/ dolev/pubs/reliable-aodv.pdf, 2005 .

[14] M.-Y. Su, Deployment of Intrusion Detection Nodes to Prevent Wormhole Attacks in Mobile Ad Hoc Networks, International Journal of Ad Hoc and Ubiquitous Computing, Vol. 7, No. 4, pp. 246-260, 2011.

[15] T. Clausen, P. Jacquet, Optimized Link State Routing Protocol (OLSR), IETF RFC 3626, October 2003.

[16] R.A. Raja Mahmood, A.I. Khan, A Survey on Detecting Black Hole Attack in AODV-based Mobile Ad Hoc Networks, in: Proc. of the International Symposium on High Capacity Optical Networks and Enabling Technologies (HONET), pp. 16, 2007.

[17] Kimaya Sanzgiri, Bridget Dahill, Brain Neil Levine, Clay Shields, Elizabeth Belding-Royer, A Secure Routing Protocol for Ad hoc Networks, in: Proc. of the IEEE International Conference on Network Protocols (ICNP02), November 2002.

[18] Djahel Sou_ne, Nait-Abdesselam Farid, Khokhar Ashfaq, An acknowledgment- based scheme to defend against cooperative black hole attacks in optimized link state routing protocol. In: Proc. of the IEEE international conference on communications (ICCs)2008. p. 27805.

[19] Yao Yu, Guo Lei, Wang Xingwei, Liu Cuixiang. Routing security scheme based on reputation evaluation in hierarchical ad hoc networks. Comput Netw 2010;54:14609.

[20] Karlof C, Wagner D. Secure routing in wireless sensor networks: attacks and countermeasures. Elseviers Ad hoc Networks J September 2003;1(23):293315 [Special Issue on Sensor Network Applications and Protocols].

[21] Xiaopeng Gao, Wei Chen. A novel gray hole attack detection scheme for mobile ad-hoc networks. In: IFIP international conference on network and parallel computing