Enhanced and More Secure AODV Routing Protocol To Avoid Black Hole Attack In MANET

Vijay Chhari
Dept. Of Computer Science &Engineering
NITM Gwalior, M.P,India
vijay_chhari@yahoo.com

Rajesh Singh
Dept. Of Computer Science &Engineering
NITM Gwalior , M.P,India
raj25682@gmail.com

S.S. Dhakad
Dept. Of Computer Science &Engineering
NITM Gwalior, M.P,India
ssdhakad38@gmail.com

Abstract **-** Nowadays wireless networks are much popular due to increasing user requirement in wireless connectivity irrespective of their location and topology. There is a greater risk of attacks in MANET because of low security given by the user. Black hole attack is a major security threat where the packet is redirected to such a node that actually does not exist in the network and the data packet gets directed somewhere else in place of the intended destination. It is similar to the black hole in the universe in which things disappear and seem to be engulfed. In black hole attack mischievous nodes uses its routing protocol to promote itself for having the shortest and optimum path to the destination or to the packet it wants to forward. MANETs should have a vulnerable way for transmitting packet or information over given network which is very challenging and crucial issue. In this paper, a review on different existing techniques for detection of black hole attacks with their defects is presented along with black hole implementation on AODV routing protocol.

Keywords- Mobile adhoc network component; DOS; black hole attack ; AODV; collaborative black hole attack**.**

I. Introduction

Ad-Hoc network is called Independent Basic Service Set (IBSS) Stations. IBSS communicate with each other directly and do not have any access point. Because of the mobility of nodes in ad-hoc networks, they are commonly called MANET (Mobile Ad-hoc network). Mobile Ad-Hoc network [1] is a group of mobile nodes which are free to move haphazardly while being able to communicate with each other without the help of an existing network infrastructure. MANETs are suitable for use in situations where any wired or wireless infrastructure is inaccessible, overloaded, damaged or destroyed such as emergency or rescue missions, disaster relief efforts and tactical battlefields, as well as civilian MANET situations, such as conferences and classrooms or in the research area like sensor networks. MANETs eliminate this dependence on a fixed network infrastructure where each station acts as an intermediate switch. Security in MANETs is a complex issue. This complexity is due to various factors like insecure wireless communication links absence of a fixed infrastructure, node mobility, dynamic topology and resource constraints. In mobile ad hoc networks, nodes also perform the role of routers that discover and maintain routes to other nodes in the network. The primary concern of routing protocols of MANETs is to establish an efficient and optimal route between the communicating entities. Any attack can mess up overall communication and the whole network will be destroyed. Nodes are more vulnerable to security attacks in mobile ad-hoc networks

DOI-10.18486/ijcsnt.2014.3.1.08
ISSN-2053-6283

than in traditional networks with a fixed infrastructure. There are different kinds of attacks by malicious nodes that can harm a network and make it unreliable for communication. One such kind of attack is black hole attack. A black hole attack is one in which a malicious node advertises itself as having the shortest path to a destination in a network. This can cause Denial of Service (DoS) [2] by dropping the received packets. The paper is organized as follows. Section 1 discusses the introduction to MANETs. Section 2 presents Security issues for MANETs. Section 3 presents Black Hole Attack Background and different techniques of black hole attack diction and prevention is discussed in section 4. Section 5 presents the conclusion and future work.

II. Security Issues

Security in Mobile Ad-Hoc Networks is an important concern for the network functioning. MANET often experience different security attacks because of its following features: Dynamically changing network topology, lack of central monitoring, cooperative algorithms and absence of a certification authority and etc [3, 4]. These features are explained below:

1. **Dynamically changing network topology**: Nodes are free and they can move arbitrarily. So the network topology changes unpredictably and frequently, which results in change in routes, frequent partitioning of network and loss of packets.

2. **Lack of centralized monitoring**: MANETs does not have any established infrastructure and centralized administration. MANET works without any preexisting infrastructure. Lack of centralized management system makes MANET more susceptible to attacks. Finding attacks and noting the changes in traffic in highly dynamic environment makes it less problematic in large scale Ad-Hoc network so that system becomes less prone to attacks.

3. **Cooperative algorithms**: In MANET the routing algorithms need to have trust between their neighboring nodes.

4. **Bandwidth constraint**: Wireless links have lower capacity as compared to the infrastructures networks.

5. **Limited physical security**: Mobility of nodes results in higher security risks, which increases the possibility of spoofing, eavesdropping and masquerading and DoS attacks.

6. **Energy constrained operation:** The only energy means for the mobile nodes in Ad-Hoc network is the battery power. And they also have a limited storage capacity and power.

III. Black Hole Attack

In black hole attack [5][6], a malefic node uses its routing protocol to attract the data packets towards itself and claim for having the shortest path to the destination node or to the packet it wants to reach. This node promotes its presence of legitimate routes irrespective of checking its routing table and other routing constraints thereby attacker node will always have the availability in replying to the route request and thus accept the data packet and retain it and hence fulfill its intension [7].

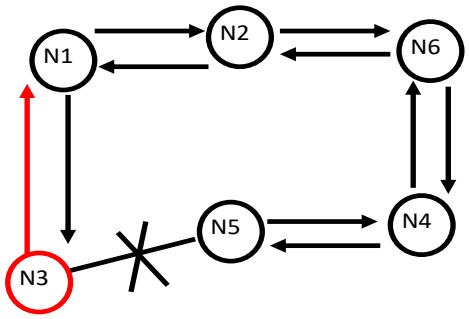


Fig. 1

Those protocols which are based on flooding claim that reply by the black hole node will be multifold times faster as compared to the reply given by the actual node before transmission; hence a wrong route which is not destined to destination is created. When this route is established, it depends on the black hole whether to forward or send the packet to some wrong address.

The route assignment of how the node adjusts in the data routes is different as per the scenario. Figure 1 shows how Black Hole problem arises, here node “N1” want to send data packets to node “N4” and initiate the route discovery process. So if node “N3” is a misbehaving then it will state that it has optimum route to the destination when it receives RREQ packets. It will then provide the response fastly to node “N1” before any other node. In this way node “N1” will assume that this is the right route and thus route discovery process is complete. Node “N1” will disregard all other replies and will start sending data packets to node “N3”. This results in the data packet to be wrongly consumed or lost forever in the network. **Black hole Attacks are classified into two categories:- 3.1.1 Single Black Hole Attack [9, 10]** In Single Black Hole Attack only one node acts as malicious node within a

DOI-10.18486/ijcsnt.2014.3.1.08
ISSN-2053-6283

zone. It is also known as Black Hole Attack with single malicious node. **3.1.2 Collaborative Black Hole Attack [11, 12]** In Collaborative Black Hole Attack multiple nodes in a group act as malicious node. It is also known as Black Hole Attack with multiple malicious nodes

IV. Literature Survey

1 Neighborhood-based and Routing Recovery Scheme

[1] Sun B et al. use AODV as their routing protocol and simulation is done in ns2 simulator. The detection scheme used neighborhood-based method to detect the black hole attack and then present a routing recovery protocol to build the true path to the destination. Based on the neighbor set information, a method is designed to deal with the black hole attack, which consists of two parts: detection and response. In detection procedure, two major steps are:

Step 1- Collect neighbor set information.

Step 2- Determine whether there exists a black hole attack. In

Response procedure, Source node sends a modify-RouteEntry (MRE) control packet to the Destination node to form a correct path by modifying the routing entries of the intermediate nodes (IM) from source to destination.

Advantages: This scheme effectively and efficiently detects black hole attack without introducing much routing control overhead to the network. Simulation data shows that the packet throughput can be improved by at least 15% and the false positive probability is usually less than 1.7%.

Disadvantages: The demerit of this scheme is that it becomes useless when the attacker agrees to forge the fake reply packets. This technique published in year 2003 and the simulation is done in NS-2 simulator.

V.2 Redundant Route Method and Unique Sequence Number Scheme

[2] Shurman et al. propose two techniques to prevent the black hole attack in MANETs. The first technique is to find at least two routes from the source to the destination node. The working is as follow. Firstly the source node sends a ping packet (a RREQ packet) to the destination. The receiver node with the route to the destination will reply to this RREQ packet and then the acknowledge examination is started at source node. Then the sender node will buffer the RREP packet sent by different nodes until there are at least three received RREP packets and after identifying a safe route it transmit the buffered packets. It represents that there are at least two routing paths existing at the same time. After that, the source node identifies the safe route by counting the number of hops or nodes and thus prevents black hole attacks. In the second technique, unique sequence number is used. The sequence value is aggregated; hence it's ever higher than the current sequence number. In this technique, two values are recorded in two additional tables. These two values are last-packet-sequence-numbers which is used identify the last packet sent to every node and the second one is for the last packet received. Whenever a packet are transmitted or received, these two table values are updated automatically. Using these two table values, the sender can analyze whether there is malicious nodes in network or not. Simulation result shows that these techniques have less numbers of RREQ and RREP when compared to existing AODV.

Advantage: second technique is considered to be good compared to first technique because of the sequence number which is included to every packet contained in the original routing protocol.

Disadvantage: these both techniques fail to detect cooperative black hole attacks. Technique published in year 2004 and simulator used is ns2.

V.3 Time-based Threshold Detection Scheme

[3] Tamilselvan L et al. proposed a solution based on an Enhancement of the original AODV routing protocol. The major concept is setting timer for collecting the other request from other nodes after receiving the first request. It stores the packet's sequence number and the received time in a table named collect route reply table (CRRT). The route validity is checked based on the arrival time of the first request and the threshold value.

Advantage: the simulation shows that a higher packet delivery ratio is obtained with only minimal delay and overhead. But end-to-end delay might be raised visibly when the malicious node is away from the source node. Simulation is done in glomosim.

V.4. Random Two-hop ACK and Bayesian Detection Scheme

[4] Djenouri D et al. proposed a solution in year 2007 to monitor, detect and remove the black hole attack in manets. In the monitor phase, an efficient technique of random two-hop ack is used. Regarding the judgment issue, a bayesian approach for node accusation is used thatenables node redemption before judgment. The aim of this approach is to consider and avoid false accusation attacks vulnerability, as well as decreasing false positives that might be caused by channel conditions and nodes mobility. This solution deals with all kinds of packet droppers, including as well selfish as malicious nodes launching a black hole attack. It also deals with any byzantine attack involving packet dropping in any of its steps. This solution detects the attacker when it drops packets. Simulation is done with glomosim simulator.

Advantages: the simulation results show that the random two-hop ack is as efficient as the ordinary two-hop ack in high true and low false detection, while hugely reducing the overhead. The solution utilizes cooperatively witnessbased verification nevertheless, it's does not to

avoid collaborate black hole attack for the judgment phase is only running on local side.
Disadvantages: it might be failed if there are multiple malicious nodes.

V.5. DRI Table and Cross Checking Scheme [5,6] Hesiri Weera singhe et al. proposed an algorithm to identify Collaborative black hole attack. In this the AODV routing protocol is slightly modified by adding an additional table i.e. Data routing information (DRI) table and cross checking using further request (freq) and further reply (FREP). If the source node (SN) does not have the route entry to the destination, it will broadcast a RREQ (route request) message to discover a secure route to the destination node same as in the AODV. Any node received this RREQ either replies for the request or again broadcasts it to the network depending on the availability of fresh route to the destination. If the destination replies, all intermediate nodes update or insert routing entry for that destination since we always trust destination. Source node also trusts on destination node and will start to send data along the path that reply comes back. Also source node will update the dri table with all intermediate nodes between source and the destination. the simulation is done in qualnet simulator. The algorithm is compared with the original AODV in terms of throughput, packet loss rate, end-to-end delay and control packet overhead.
Advantages: simulation results show that the original AODV is affected by cooperative black holes and it presents good performance in terms of throughput and minimum packet loss percentage compared to other solutions.

V.6. Distributed Cooperative Mechanism (DCM)
[7] Wu Chang et al. propose a distributed and cooperated "black hole" node detection mechanism which composes four sub-steps: (1) local data collection (2) Local detection (3) Cooperative detection (4) Global reaction. In local data collection, each node collects information through overhearing packets to evaluate if there is any suspicious node in its neighborhood. If finding one, the detecting node would initiate the local detection procedure to analyze whether the suspicious one is a malicious black hole node. Subsequently, the cooperative detection procedure is initiated by the initial detection node, which proceeds by first broadcasting and notifying all the onehop neighbors of the possible suspicious node to cooperatively participate in the decision process confirming that the node in question is indeed a malicious one. As soon as a confirmed black hole node is identified, the global reaction is activated immediately to establish a proper notification system to send warnings to the whole network. Simulation is done in NS-2 simulator.
Advantage: in this DCM is compared with original AODV routing protocol. The packet delivery ratio is improved by 64.14% to 92.93% when compared with AODV.
Disadvantage: defect of this technique is a higher control overhead when compared to original AODV.

V.7. Resource-Efficient AccounTability (REAct) Scheme based on Random Audits [8] Kozma W et al. propose a REAct scheme. This scheme provides publicly confirmable evidence of node misbehavior. REAct constitutes of three phases: (i) Audit phase, (ii) Search phase and (iii) Identification phase. The audit phase verifies the packet forwarding from audited node to the destination node. The audit phase constitutes three steps: (a) sending of an audit request. (b) Building up behavioral proof and (c) then processing of this build up behavioral proof. The search phase identifies the misbehaving links i.e., the link in which packets are dropped.
Advantage: The simulation result shows that REAct significantly reduces the communication over-head associated with the misbehavior identification process compared to reputation-based and acknowledgment-based schemes. This reduction in resource expenditure comes at the expense of a logarithmic increase in the identification delay, due to the reactive nature of the scheme. Finally, use of binary search method exposes audit node's information to the attacker and as a result attacker can try to cheat source by dynamically changing its behavior.

V.8. Detection, Prevention and Reactive AODV (DPRAODV) Scheme [9] In DPRAODV an additional check is done to find whether the RREP_seq_no value is higher than the threshold value as compared to normalAODV. If the RREP_seq_no value is higher than the threshold value, the node is considered to be malicious and that node is added to the black list. As the node detects a malicious node, it sends an ALARM packet to its neighbors. This ALARM packet has black listed node as a parameter. Later, if any other node receives the RREP packet it checks the black list. If that node is black listed, it simply ignores it and does not receive reply from that node again.
Advantage: The simulation result shows that the packet delivery ratio is improved as compared to AODV.
Disadvantage: Disadvantage of DPRAODV is that the routing overhead and end-to-end delay is little bit increased. And it fails with cooperative black hole attacks.

V.9. Hash based Scheme
[10] Wang W et al. propose a technique for detection of collaborative packet drop attacks on MANETs. This mechanism is for audit based detection of collaborative packet drop attacks. Firstly the vulnerability of the REAct system is studied and then illustrated that Collaborative adversary can compromise the attacker identification procedure by sharing Bloom filters of packets among them. To defend against such attacks, Wang proposed mechanism to generate node behavioral proofs. Every intermediate node needs to conduct only a hash calculation on the received packet. A collaborative attacker cannot generate its node behavioral proofs if an innocent node before it does not receive the data packets correctly.

DOI-10.18486/ijcsnt.2014.3.1.08
ISSN-2053-6283

Advantage: this approach will allow the system to successfully locate the routing segment in which packet drop attacks are conducted. No simulation is done for this technique.

V.10. Nital mistry et al.'s method

[11] mistry n et al. Proposed a solution for analyzing and improving the security of AODV routing protocol against blackhole attack. The approach basically modifies the working of source node only, using additional function pre_receivereply. A table cmg_rrep_tab, a variable mali_node and a new timer mos_wait_time are also added to the default AODV. In the proposed solution, after receiving the first rrep the source node waits for mos_wait_time and meanwhile it stores all the rreps in the cmg_rrep_tab table until mos_wait_time. In this technique the value of mos_wait_time is considered to be half the value of rrep_wait_time. Now, the source node will analyze the stored rreps and will discard the rrep which have high destination sequence number. The node which has sent these rrep with high destination sequence number are considered to be malicious node. This technique alsorecords the identity of suspected malicious nodes as mail_node, so that in future it can discard messages coming from that node. The simulation is done in ns2 simulator. The pdr is increased by 81.812% in presence of black hole attack compared to AODV and there is 13.28% rise in end-to end delay.

V.11. Bait DSR (BDSR) based on Hybrid Routing Scheme

[12] Tsou P-C et al. design a novel solution named Bait DSR (BDSR) scheme to avoid the collaborative black hole attacks. The proposed solution is composed of both proactive and reactive method to make a hybrid routing protocol. The base routing protocol used is the DSR on demand routing. Initially the source node sends bait RREQ packet. The destination address for this bait RREQ does not exists. The same method as used in DSR is used here to avoid the traffic jam problem generated by bait RREQ. The initially sent bait RREQ can attract the forged RREP and can easily remove malicious node to avoid black hole attack. In this solution the RREPs additional field records the identity of theses malicious nodes. Now the source node can easily detect the location of malicious node and will discard all the RREPs coming from that location. BDSR has an increased packet delivery ratio when compared to existing DSR and WD approach. And the communication overhead is higher than DSR routing protocol but, lower than WD approach.

V. Proposed Algorithm

DSN – Destination Sequence Number, NID – Node ID,

Hop_count.

Step 1: (Initialization Process)

Retrieve the current time

Add the present time along with waiting time

Step2: Modified route discovery process of AODV when a destination receives a RREQ packed it replies for all the RREQ packets received even for same sequence number using back path.

Step 3: (Storing Process)

Make a database to accumulate all the Route Replies and NID network id in RR-Table.

Follow above steps /procedure until the time exceeds a threshold value.

Step 4: (Identify top 1 to 5 shortest path on the bases of hop count) .

Short the table on the bases of Hop_count.

If table contain more than five entries than retrieve first five otherwise take all .

Step 5: (At the time of sending data)

if data available to send is big than divide it in parts and send through available paths

else

send data using first path(shortest) in table .

Step 6: If a path breaks send the data using other available paths .

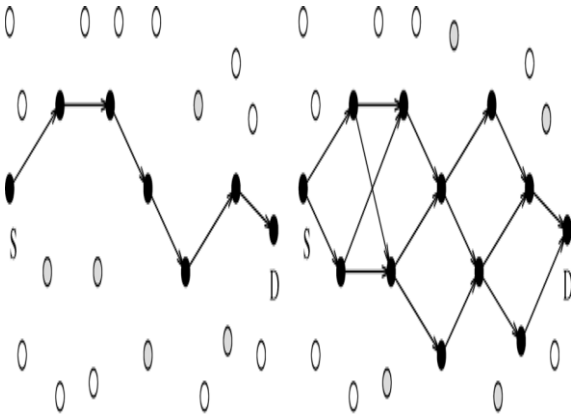


Fig 2: Under light and heavy traffic load conditions

DOI-10.18486/ijcsnt.2014.3.1.08
ISSN-2053-6283

VI. Simulation Result

In our simulation result we calculate packet delivery ratio and throughput in our simulation we take 7 14 and 21 nodes. For compare result.
Pdr IN ATTACK CONDITION when nodes have no moment

Number of node	Packet delivery ratio
7	**0**
14	0.6659
21	0.331

Proposed work packet delivery ratio when node have no movement

Number of node	Packet delivery ratio
7	0.0861
14	0.2473
21	0.4692

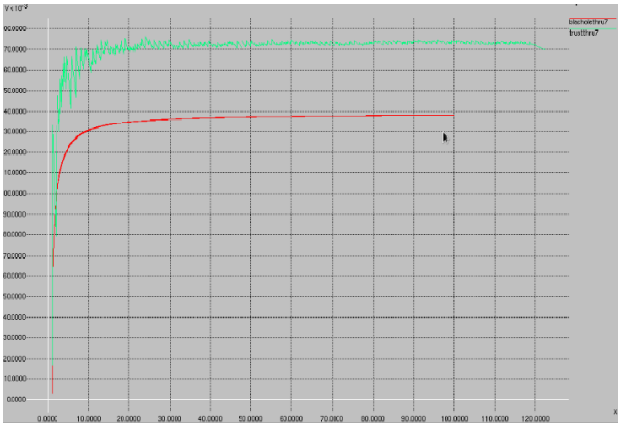
Comparision of PDR when node have no movement.

Node	Attack condition	Simple aodv	Praposedwork
7	**0.2002**	**1.000**	**0.0861**
14	**0.1844**	**0.9545**	**0.2473**
21	**0.1684**	**0.9200**	**0.4692**

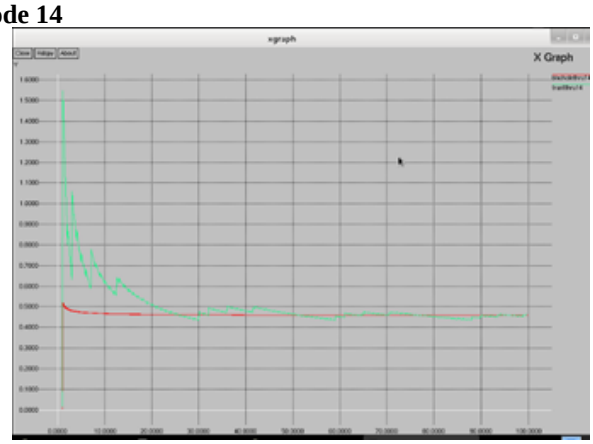
Comparision of PDR when node have movement

Node	Attack condition	Simple aodv	Proposed work
7	**0.4508**	**0.6850**	**0.5491**
14	**0**	**0.9688**	**0.4692**
21	**0.1691**	**0.9836**	**0.7107**

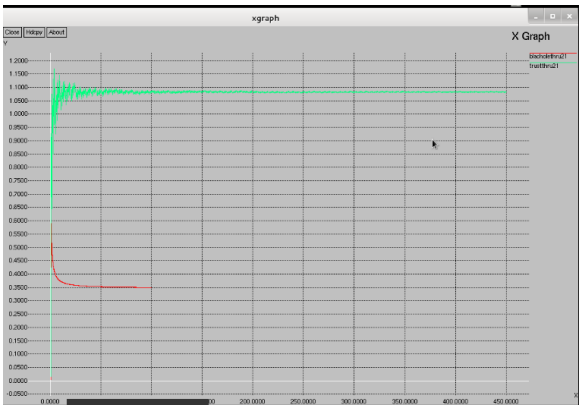
Throughput graph :- (node number 7 and have no movement base paper)



node 14

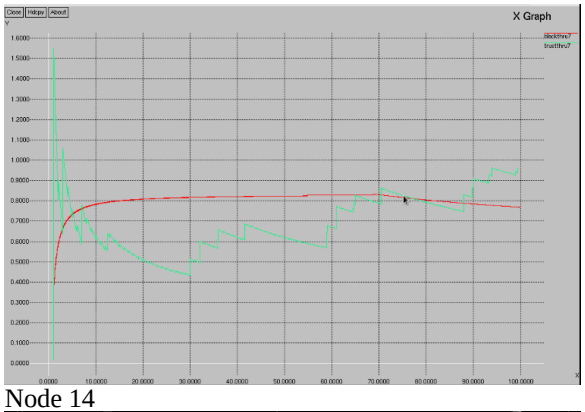


Node 21

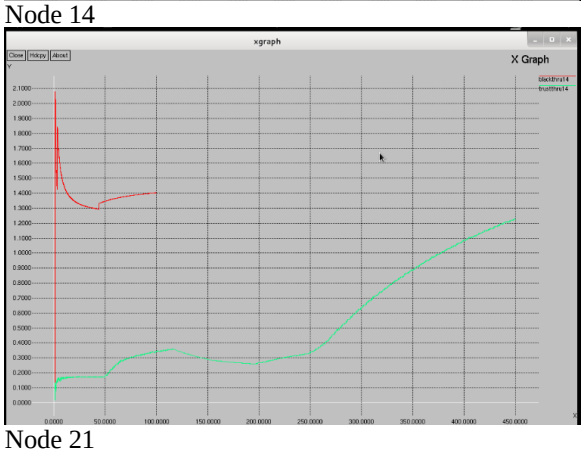


When Node have movement node 7

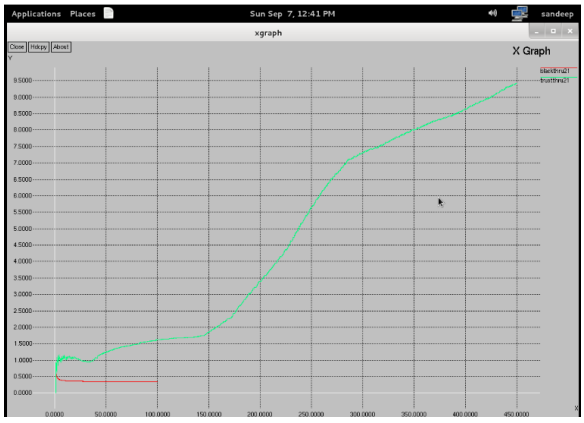
DOI-10.18486/ijcsnt.2014.3.1.08
ISSN-2053-6283



Node 14



Node 21



VII. Conclusion

Black Hole attack is one of the serious security problems in MANETs. It is an attack where a malicious node impersonates a destination node by sending forged RREP to a source node that initiates route discovery, and consequently deprives data traffic from the source node. In this paper a survey on different existing techniques for detection of black hole attacks in MANETs with their defects is presented. The detection techniques which make use of proactive routing protocol have improved packet delivery ratio and optimum detection probability, but have greater overheads. Multipath routing protocols have been implemented for mobile adhoc networks from many years. Multipath routing can yield load balancing and minimize the occurrence of route discovery mechanism effectively as compared to single path counterparts. Researchers have made rapid progress in ad hoc networks. Many multi path extensions of AODV have been suggested.

References

[1] Y.-C. Hu, D. B. Johnson, and A. Perrig, "Sead: Secure efficient distance vector routing for mobile wireless ad-hoc networks," in WMCSA '02: Proceedings of the Fourth IEEE Workshop on Mobile Computing Systems and Applications. Washington, DC, USA: IEEE Computer Society, 2002, . 3–13.

[2] X. Wang, T. liang Lin, and J. Wong, Feature Selection in Intrusion Detection System over Mobile Ad-hoc Network. Technical Report,Computer Science, Iowa State University, 2005.

[3] J. Grønkvist, A. Hansson, and M. Skøld, Evaluation of a Specification-Based Intrusion Detection System for AODV.di.ionio.gr/medhocnet07/wpcontent/uploads/papers/90.pdf, 2007.

[4] S. Kurosawa, H. Nakayama, and N. Kato, "Detecting blackhole attackon AODV based mobile ad-hoc networks by dynamic learning method,"International Journal of Network Security, pp. 338–346, 2007.

[5] K. Makki, N. Pissinou, and H. Huang, "Solutions to the black holeproblem in mobile ad-hoc network," 5th World Wireless Congress, pp.508–512, 2004.

[6] S. Lu, L. Li, K.Y. Lam, L. Jia, "SAODV: A MANET Routing Protocol that can Withstand Black Hole Attack.," International Conference on Computational Intelligence and Security, 2009.

[7] Opnet Technologies, Inc. "Opnet Simulator," Internet: www.opnet.com, date lastviewed: 2010-05-05

[8] M. Al-Shurman, S-M. Yoo, and S. Park, "Black Hole Attack in Mobile Ad-HocNetworks," ACM Southeast Regional Conf. 2004.

[9] Sun B, Guan Y, Chen J, Pooch UW, " Detecting Black-hole Attack in Mobile Ad Hoc Networks". 5th European Personal Mobile Communications Conference, Glasgow, United Kingdom, 22-25 April 2003.

[10] Al-Shurman M, Yoo S-M, Park S , " Black Hole Attack in Mobile Ad Hoc Networks". 42nd Annual ACM Southeast Regional Conference (ACM-SE'42), Huntsville, Alabama, 2-3 April 2004.

[11] Djenouri D, Badache N, "Struggling Against Selfishness and Black Hole Attacks in MANETs", Wireless Communications & Mobile Computing Vol. 8, Issue 6, pp 689-704, August 2008.

[12] Chang Wu Yu, Wu T-K, Cheng RH, Shun chao chang, "A Distributed and Cooperative Black Hole Node Detection and Elimination Mechanism for Ad Hoc

Network", Emerging Technologies in knowledge Discovery and Data Mining, Vol. 4819, Issue 3, pp 538-549,2007.
[13] Raj PN, Swadas PB, "DPRAODV: A Dynamic Learning System against Blackhole Attack in AODV based MANET", International Journal of Computer Science Issue, Vol. 2, pp 54–59, 2009.
[14] istry N, Jinwala DC, IAENG, Zaveri M, "Improving AODV Protocol Against Blackhole Attacks", International Multi Conference of Engineers and Computer Scientists IMECS Hong Kong, Vol. 2, pp 1-6, 17-19 March, 2010.
[15] Tsou P-C, Chang J-M, Lin Y-H, Chao H-C, Chen J-L, "Developing a BDSR Scheme to Avoid Black Hole Attack Based on Proactive and Reactive Architecture in MANETs". Paper presented at the 13th International Conference on Advanced Communication Technology, Phoenix Park, Korea, 13-16 Feb. 2011.

Vijay Chhari is a student of final year of M.Tech in Computer Science from Nagaji Institute of Technology and Management, Gwalior, MP, India. He received his B.E. degree in Computer Science from Institute of information Technology and Management, Gwalior. His area of research is Mobile Ad hoc networking and Wireless networks.

Rajesh Singh obtained **M.Tech** degree in **Computer Science and Engineering** from DAVV College Indore in 2010. Working as Asst. Prof. in the department of **Computer Science and Engineering** NITM Gwalior MP India. His area of interest is network security, cloud computing, computer networking.

S. S. Dhakad obtained **M.Tech** degree in Embedded System from ITM college Gwalior MP India in 2009.
Working as Asst. Prof. in the department of **Computer Science and Engineering** NITM Gwalior MP India His area of interest are embedded system, computer networking.