International Journal of Current Trends in Engineering & Technology
ISSN: 2395-3152
Volume: 01, Issue: 07 (NOVEMBER-DECEMBER, 2015)

"Survey On Nearest Neighbor Based Security Scheme Against Black Hole Attack In MANET"

Swati Saxena
Computer Science & Engineering
NIIST Bhopal
swtsaxena14@gmail.com

Prof. Sini Shibu
Computer Science & Engineering
NIIST Bhopal
Sini.Shibu09@gmail.com

ABSTRACT: - Security is one of the major issue in Mobile Ad hoc Network (MANET). Due to unique characteristics of MANETS, it creates a number of consequential challenges to its security design. To overcome the challenges, there is a need to build a dominant security solution that achieves both extensive protection and desirable network performance. This work analyzes the effect of cooperative attack which is probable attacks in ad hoc networks. In this attack, a malevolent node or malicious node impersonates a target node by sending a spoofed route reply packet to a source node which initiates a route discovery. Mobile ad hoc networks may be unprotected against attacks by the malicious nodes. One of these attacks is the Black Hole Attack against network integrity absorbing all data packets in the network. Since the data packets do not reach the destination by that due to this attack, data loss will occur. The damage will be serious if malicious node in a network working as an attacker node absorbs all data packets delivered through them. In this paper we proposed a simple IDS Algorithm against black hole attack and measure the network performance after applying IDS. We simulated black hole attacks in network simulator 2 (ns-2) and measured the packet loss in the presence of black hole and in presence of Intrusion Detection System against Black hole attack.. Our solution improved the 80% network performance in the presence of a black hole attack.

Keywords:- Black hole attack, IDS, Routing, AODV, Security

I. `INTRODUCTION

Wireless ad-hoc networks are composed of autonomous nodes that are self- managed with none infrastructure. During this means, ad-hoc networks have a dynamic topology such nodes will simply be part of or leave the network at any time. They have several potential applications, especially, in military associate degreed rescue areas like connecting troopers on the field or establishing a replacement network in situ of a network that folded once a disaster like an earthquake. Ad-hoc networks square measure appropriate for areas wherever it's impracticable to line up a hard and fast infrastructure. Since the nodes communicate with each other one associate degree other while not an infrastructure, they supply the property by forwarding packets over themselves. To support this property, nodes use some routing protocols like AODV (Ad-hoc On-Demand Distance Vector), DSR (Dynamic Source Routing) and DSDV (Destination-Sequenced Distance-Vector). Besides acting as a bunch, every node conjointly acts as a router to get a path and forward packets to the right node within the network. As wireless ad-hoc networks lack AN infrastructure, they're exposed to lots of attacks. One among these attacks is that the part attack. Within the part attack, that result in dropping of messages. Offensive node 1st agrees to forward packets thus} fails to try and do so. At first the node behaves properly and replays. true RREP messages to nodes that initiate RREQ message. This way, it takes over the causation packets. Afterwards, the node simply drops the packets to launch a (DoS) denial of service attack. Part attack might occur owing to a malicious node that is deliberately misbehaving, furthermore as a broken node interface. In any case, nodes within the network can perpetually try and notice a route for the destination, which makes the node consume its battery additionally to losing packets. In our study, we tend to simulate the part attack in wireless ad-hoc networks and evaluated its injury within the network. We tend to create our simulations exploitation NS-2 (Network machine version 2) simulation program that consists of the gathering of all network protocols to simulate several of the prevailing network topologies. Even if NS-2 contains wireless ad-hoc routing protocols, it doesn't have any modules to simulate malicious protocols. Thus, to simulate part attacks, we tend to 1st extra a replacement part protocol into the NS-2. We tend to start our study by writing a replacement AODV protocol exploitation C++, to simulate the part attack. Having enforced a replacement routing protocol that simulates the part we tend to performed tests on totally different topologies to check the network performance with and while not Black holes within the network. we tend to projected AN IDS resolution to eliminate the part effects within the AODV network. We tend to enforce the answer into the NS-2 and evaluated the results as we tend to did in part implementation.

II LITERATURE SURVEY

In this paper [1], we use a reactive routing protocol known as Ad hoc On-demand Distance Vector (AODV) routing for analysis of the effect of the black hole attack when the destination sequence number is changed via simulation. Then, we select features in order to define the normal state from the characteristic of black hole attack. Finally, we present a new training method for high accuracy detection by updating the training data in every given time intervals and adaptively defining the normal state according to the changing network environment. In this paper [2], wormhole attack detection is proposed based on RTT between successive nodes and congestion detection mechanism. If the RTT between two successive nodes is higher than the threshold value, a wormhole attack is suspected. If a wormhole is suspected, node_s transitory buffer is probed to determine whether the long delay between the nodes is due to wormhole or not, as delays can be caused due to congestion or by queuing delays. The proposed method prevents both the hidden

and the exposed attack. Advantage of our proposed solution is that it does not require any specialized hardware or synchronized clocks. In this paper [3], a number of systems factors that affect a network's DoS resilience and obtain the following findings. 1) JF (Jelly Fish) have a network partitioning effect that severely degrades or altogether prevents long-range communication. Consequently, an increased number of JF reduce the system's fairness index but may *increase* network capacity, as capacity can be increased by starving long-range flows and serving only one-hop flows. 2) The mean and distribution of path length have a significant effect on attack scalability as higher path length flows are highly vulnerable. In this paper [4] Audit-based Misbehavior Detection (AMD) can construct paths consisting of highly trusted nodes, subject to a desired path length constraint. When paths contain misbehaving nodes, these nodes are efficiently located by a behavioral audit process. AMD detects selective dropping behaviors by allowing the source to perform matching against any desired selective dropping patterns. This is particularly important when end to end traffic is encrypted. In the latter scenario, only the source and destination have access to the contents of the packets and can detect selective dropping. In this paper [5], source node verifies the authenticity of node that initiates RREP by finding more than one route to the destination. The source node waits for RREP packet to arrive from more than two nodes. In ad hoc networks, the redundant paths in most of the time have some shared hops or nodes. When source node receives RREPs, if routes to destination shared hops, source node can recognize the safe route to destination. But, this method can cause the routing delay. Since a node has to wait for RREP packet to arrive from more than two nodes. Therefore, a method that can prevent the attack without increasing the routing overhead and the routing delay is required. In this paper [6] has proposed an algorithm to prevent black hole attacks in ad hoc networks. According to the algorithm, any node on receiving a RREP packet, crosschecks 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 solution cannot prevent cooperative black hole attacks. Apart of that there are many techniques which are used for the security of AODV. In this paper [7], they proposed a method uses Intrusion Detection using Anomaly Detection (IDAD) to defend against black hole attacks established by both single and multiple black hole nodes. It proved the specific result increases network performance by reducing formation of control (routing) packets including effectively defend black hole attacks opposed to mobile ad-hoc networks. In this paper [8], they proposed a method uses promiscuous mode to find malicious node and transmit the data of malicious node to every some other nodes in the network. The efficiency of suggested mechanism as throughput of the network does not decay in existence of the black holes. In this paper [9], they proposed two possible solutions to study black hole attack. The first solution is to study several route to the destination. The second is to apply the packet sequence number contained in any packet header. In study to AODV routing scheme, the second solution is superior and of the route to the destination rely upon on the pause time at a lowest cost of the delay in the networks. In this paper [10], they have proposed a solution the requesting node wait and check the replies from all neighboring node to find a safe route. It is provide better performance than the conventional AODV in the existence of Black holes with smallest additional delay and overhead. In this paper [11], they apply a reactive routing protocol called as Ad hoc On-demand Distance Vector (AODV) routing for examine of the outcome of the black hole attack when the destination sequence number is altered via simulation. Then, they determine characteristic in order to define the normal state from the character of black hole attack. They proposed training scheme for huge accuracy detection by modifying the training data in every given time intervals and adaptively specifying the normal state according to the changing network environment.

III. PROBLEM IDENTIFICATION

3.1 Black Hole Attack In Aodv Protocol

Initially, we must always take into consideration Ad-hoc On-Demand Distance Vector (AODV) Routing Protocol so we tend to shall make a case for part Attack and interference. Our aim to guard the Mobile ad-hoc network through part Attack, Intrusion Detection System aimed to securing the AODV protocol victimization our Intrusion Detection system. They conclude that AODV performs well the least bit quality rates and movement speeds. However, we tend to argue that their definition of quality doesn't actually represent the dynamic topology of MANETs. During this thesis, the work of has been extended and therefore the projected protocol is termed IDSAODV (Intrusion Detection System AODV). In our work, we tend to build use of AODV primarily based intrusion detection. Our Intrusion Detection and Response Protocol for MANETs are incontestable to perform higher than that AODV protocol and presence of part Attack, in terms of false positives and share of packets delivered. Since the sooner work don't report true positive i.e. the detection rate, we tend to couldn't compare our results against that parameter with projected technique. The implementation of the IDSAODV protocol according during this thesis has shown to figure in real world eventualities. IDSAODV performs real time detection of attacks in MANETs running AODV routing protocol. Experimental results validate the flexibility of our protocol to with success observe each native and distributed attacks against the AODV routing protocol. The algorithmic program conjointly imposes an awfully tiny overhead on the nodes, which is a crucial issue for the resource affected nodes.

3.1.1 AODV Protocol

AODV may be a terribly easy, efficient, and effective routing protocol for Mobile Ad-hoc Networks that don't have fastened topology. This algorithmic rule was impelled by the restricted information measure that's obtainable within the media that are used for wireless communications. It borrows most of the advantageous ideas from DSR and DSDV algorithms. The on demand route discovery and route maintenance from DSR and hop-by-hop routing, usage of node sequence numbers

from DSDV create the algorithmic rule cope up with topology and routing data. Getting the routes strictly on-demand makes AODV a really helpful and desired algorithmic rule for MANETs. Maximum utilization of the bandwidth: this will be thought of the foremost action of the rule. Because the protocol doesn't need periodic world advertisements, the demand on the obtainable information measure is a smaller amount. And a monotonically exaggerated sequence variety counter is maintained by every node so as to replace any stale cached routes. All the intermediate nodes in a full of life path change their routing tables additionally certify of most utilization of the information measure. Since, these routing tables are used repeatedly if that intermediate node receives any RREQ from another supply for same destination. Also, any RREPs that area unit received by the nodes area unit compared with the RREP that was propagated last victimization the destination sequence numbers and area unit discarded if they're not higher than the already propagated RREPs. *Simple*: it's easy with every node behaving as a router, maintaining an easy routing table, and also the supply node initiating path discovery request, creating the network self-starting. Most effective routing info: once propagating associate RREP, if a node finds receives associate RREP with smaller hop-count, it updates its routing information with this higher path and propagates it. *Most current routing info*: The route info is obtained on demand. Also, once propagating associate RREP, if a node finds receives associate RREP with bigger destination sequence variety, it updates its routing information with this latest path and propagates it. *Loop-free routes*: The rule maintains loop free routes by exploitation the easy logic of nodes discarding non higher packets for same broadcast-id. Coping up with dynamic topology and broken links: once the nodes within the network move from their places and also the topology is modified or the links within the active path are broken, the intermediate node that discovers this link breakage propagates associate RERR packet. And also the supply node re-initializes the trail discovery if it still wishes the route. This ensures fast response to broken links. *Highly Scalable:* The rule is extremely ascendable due to the minimum area complexness and broadcasts avoided once it compared with DSDV.

3.1.2 Ad Hoc AODV Routing Protocol

It is employed for locating a path to the destination in AN ad-hoc network. to search out the trail to the destination all mobile nodes add cooperation exploitation the routing management messages. Thanks to these management messages, AODV Routing Protocol offers fast adaptation to dynamic network conditions, low process and memory overhead, low network information measure utilization with little size management messages. The foremost distinctive feature of AODV compared to the opposite routing protocols is that it uses a destination sequence range for every route entry. The destination sequence range is generated by the destination once a association is requested from it. Exploitation the destination sequence range ensures loop freedom. AODV makes certain the route to the destination doesn't contain a loop and is that the shortest path. Route Requests (RREQs), Route Replay (RREPs), Route Errors (RERRs) are management messages used for establishing a path to the destination, sent exploitation UDP/IP protocols. Once the supply node desires to form a reference to the destination node, it broadcasts AN RREQ message. This RREQ message is propagated from the supply, received by neighbors (intermediate nodes) of the supply node. The intermediate nodes broadcast the RREQ message to their neighbors. This method goes on till the packet is received by destination node or AN intermediate node that includes a contemporary enough route entry for the destination. Next Figure shows however the RREQ message is propagated in AN ad-hoc network. Fresh enough implies that the intermediate node features a valid route to destination shaped an amount of your time past, below the brink. Whereas the RREQ packet travels through the network, each intermediate node will increase the hop count by one. If associate RREQ message with a similar RREQ ID is received, the node taciturnly discards the new received RREQs, dominant the ID field of the RREQ message. Once the destination node or intermediate node that has recent enough route to the destination receive the RREQ message they produce associate RREP message and update their routing tables with accumulated hop count and also the sequence variety of the destination node. After the RREP message is uncased to the supply node. The distinction between the broadcasting associate RREQ and unicasting RREP is seen from Figures nine and ten. whereas the RREQ and also the RREP messages are forwarded by intermediate nodes, intermediate nodes update their routing tables and save this route entry for three seconds, that is that the ACTIVE_ROUTE_TIMEOUT constant worth of AODV protocol. The default constant values of the AODV protocol are listed in appendix of RFC – 3561. Therefore the node is aware of over that neighbor to succeed in at the destination.

3.1.3. Sequence Numbers

Sequence number function time stamps and permit nodes to match however recent their info on the opposite node is. But once a node sends any style of routing management message, RREQ, RREP, RERR etc., it will increase its own sequence range. Higher sequence range is a lot of correct info and whichever node sends the very best sequence range, its info is taken into account and route is established over this node by the opposite nodes. The sequence range could be a 32-bit unsigned whole number price (i.e., 4294967295). If the sequence range of the node reaches the doable highest sequence range, 4294967295, then it'll be reset to zero (0). If the results of subtraction of the presently hold on sequence range in an exceedingly node and therefore the sequence range of incoming AODV route management message is a smaller amount than zero, the hold on sequence range is modified with the sequence range of the incoming management message.

3.1.4. Black Hole Attack

Black Hole Attack is briefly explained in the previous Chapter. In this Chapter we shall explain it in more detail as we have already explained the AODV protocol. In an ad-hoc network that uses the AODV protocol, a Black Hole node absorbs the network traffic and drops all packets.

To explain the Black Hole Attack we added a malicious node that exhibits Black Hole behavior in the scenario of the figures of the previous section. In this situation shown in Figure twelve, we tend to assume that Node three is that the malicious node. once Node one broadcasts the RREQ message for Node four, Node three intermediate node between Node one and Node four therefore abolition just in case of route requesting time region Node three immediate send false RREP, wherever sender node receive route reply packet, sender node sends actual knowledge packet through region Node three, region Node three Receives knowledge packets, if knowledge packets square measure UDP then this packets Capture by the region Node and if communications protocol kind packet then Block this sort Packets By Malicious Node. Therefore our Network has infected. In a region Attack, when a minute, the causing node understands that there's a link error as a result of the receiving node doesn't send communications protocol ACK packets. If it sends out new communications protocol knowledge packets and discovers a brand new route for the destination, the malicious node still manages to deceive the causing node. If the causing node sends out UDP knowledge packets the matter isn't detected as a result of the UDP knowledge connections don't await the ACK packets. In our situations we tend to use UDP knowledge packets and that we can make a case for our situations.

IV. PROPOSED SOLUTION

4.1. Solution for black hole attack and ids its effects

In the previous sections, we have a tendency to make a case for however region Attack is enforced in NS2 and that the results square measure obtained from the simulations. After we examine the trace file of the simulations that embody one region node, we have a tendency to saw that when a minute second RREP message came to supply node from the $64000 destination node.

4.1.1. Expected Proposed Solution in NS-2

To evaluate effects of the projected answer, we tend to initial required to implement it in NS- Therefore, we tend to clone the ―aodv‖ protocol, ever-changing it to ―idsaodv‖ as we tend to did ―blackhole‖ before. To implement the part we tend to modified the receive RREP perform (recvRequest) of the blackholeaodv.cc file however to implement the answer we tend to had to vary the receive RREP perform (recvReply) and make RREP caching mechanism to count the second RREP message. The RREP caching mechanism ―rrep_insert‖ perform is for adding RREP messages, ―rrep_lookup‖ perform is for trying any RREP message up if it's exist, ―rrep_remove‖ perform is for removing any record for RREP message that arrived from outlined node and ―rrep_purge‖ perform is to delete sporadically from the list if it's terminated. We tend to selected this expire time ―BCAST_ID_SAVE‖ as vi (means three seconds). In the ―recvReply‖ perform, we tend to initial management if the RREP message arrived for itself and if it did, perform appearance the RREP message up if it's already arrived. If it failed to, it inserts the RREP message for its destination address and returns from the form. If the RREP message is cached before for an equivalent destination address, traditional RREP perform is meted out. Afterwards, if the RREP message isn't meant for itself the node forwards the message to its applicable neighbor.

V. CONCLUSION

We will simulate attack in the ad-hoc networks and find its affects. We study on AODV routing protocol. But the other various routing protocols can be simulate. In this study, we try to resolve cooperative effect in the network. But the detection of the black hole attack is possible through proposed IDS security scheme. Our solution looks the path in the AODV level. As malicious node is the main security threat that effect the performance of the AODV routing protocol.

REFERENCES

[1]. Liu, Ting, Yang Liu, Yashan Mao, Yao Sun, Xiaohong Guan, Weibo Gong, and Sheng Xiao. "A dynamic secret-based encryption scheme for smart grid wireless communication", IEEE Transactions on Smart Grid, Vol. 5, Issue 3, August 2013.

[2]. T. Franklin, “Wireless Local Area Networks”, Technical Report http://www.jisc.ac.uk /uploaded_documents/ WirelessL ANTechRep.pdf. 25 July 2010.

[3]. www.cs.cmu.se/education/examina/Rapporter/ClaesGahlin.pdf.

[4]. 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.

[5]. P. Yau and C. J. Mitchell, “Security Vulnerabilities in Adhoc Network”. SCOTT CORSON AND JOSEPH MACKER, “Mobile Ad Hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations”. Internet-Draft, draft-ietf-manet-issues-01.txt, March 2008.

[6]. Hao Yang, Haiyun Luo. Fan Ye, Songwu Lu, and Lixia Zhang. “Security in mobile ad hoc networks: Challenges and solutions”. IEEE Wireless Communications, February 2010.

[7]. Charles E. Perkins and Elizabeth M. Royer. “Ad-Hoc on- Demand Distance Vector Routing”. In Proceedings of the Second IEEE Workshop on Mobile Computing Systems and Applications (WMCSA‟99), pages 90- 100, February 1999.

[8]. C. Perkins, E. B. Royer, S. Das, “Ad hoc On-Demand Distance Vector (AODV) Routing - Internet Draft”, RFC 3561, IETF Network Working Group, July 2003.

[9]. Y.-C. Hu, D.B. Johnson, and A. Perrig, “SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad hoc Networks,” Proc. 4th IEEE Workshop on Mobile Computing Systems and Applications, Callicoon, NY, June2002,

[10]. Y.-C. Hu, A. Perrig, and D.B. Johnson, “Ariadne: A Secure On-Demand Routing Protocol for Ad hoc Networks,” Proc.8th ACM Int‟l. Conf. Mobile Computing and Networking (Mobicom‟02), Atlanta, Georgia, September 2002, pp. 12-23.

[11]. Kimaya Sanzgiti, Bridget Dahill, Brian Neil Levine, Clay shields, Elizabeth M, Belding-Royer, “A secure Routing Protocol for Ad hoc networks In

Proceedings of the 10thIEEE International Conference on Network Protocols (ICNP‟ 02), 2002.

[12]. S. Yi, P. Naldurg, and R. Kravets, “Security-Aware Ad hoc Routing for Wireless Networks,” Proc. 2nd ACM Symposium Mobile Ad hoc Networking and Computing (Mobihoc‟01), Long Beach, CA, October 2001, pp. 299-302.

[13]. Y. Zhang and W. Lee, "Intrusion detection in wireless ad – hoc networks," 6th annual international Mobile computing and networking Conference Proceedings, 2000.

[14]. T. Anantvalee and J. Wu. “A Survey on Intrusion Detection in Mobile Ad Hoc Networks”, Book Series Wireless Network Security, Springer, pp. 170 – 196, 2007.

[15]. S. Lee, B. Han, and M. Shin, “Robust routing in wireless ad hoc networks,” in ICPP Workshops, pp. 73, 2002.

[16]. M. A. Shurman, S. M. Yoo, and S. Park, “Black hole attack in wireless ad hoc networks,” in ACM 42nd Southeast Conference (ACMSE‟04), pp. 96-97, Apr. 2004.