IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 5, May 2020

Software Engineering Approach for Detecting Black-Hole Attacks in MANETs

Prajeeth Kumar M.J[1], Manjula. R [2]

U.G. Student, SCOPE, Vellore Institute of Technology, Vellore, Tamilnadu, India[1]

Associate Professor, SCOPE, Vellore Institute of Technology, Vellore, Tamilnadu, India[2]

Abstract: Mobile Ad Hoc Network (MANET) is a cluster of portable wireless nodes that energetically organize an interim system. MANETs typically configured without any single control unit; devices operating in a MANET depend on external groups to route information towards their targets. There may be risks of various forms of malware attacks in these networks that can trigger the whole system to break. The black hole attack is one of the noteworthy outbreaks in the most prevalent on-demand routing protocols ad hoc network. In this paper, a novel approach proposed to find the black hole attacks in MANETs and to protect against the threat. The method proposed is based on promiscuous listening and is used to identify nodes that misbehave. For a particular node, the number of data packets lost and the number of data packets successfully transmitted can be identified by the node constitutes a criterion for labeling the node as either disobeying or well-behaving. Based on the threshold value, disobeying and well behaving nodes are identified. Once finding a disobeying node, the finding node tries to stop the node from being misbehaved and routes the packets through a separate direction to reach a secure route. The metrics such as packet size, overhead, average End to end delay evaluated by simulation. The result shows that in the presence of black holes with minimum delay and better packet delivery ratio. The proposed black hole AODV outperforms than the traditional AODV.

Keywords: On-Demand distance vector, Proactive, Replication, Routing Information table.

I. INTRODUCTION

Software Development Life Cycle's 7 phases comprise planning, requirements, design, development, testing, deployment, and maintenance. We also built IDS based on software development life cycle for monitoring, data collection, detection, response, testing. The IDS model is used to identify network black hole attacks, and to isolate them from the network.

A mobile ad hoc network is an uninterruptedly self-configuring, infrastructure less network of mobile devices coupled without wires. Each device in MANET is allowed to travel freely in any route, and will consequently change its links to other devices recurrently. The ad hoc mobile network is the furthermost insecure of cellular networks, owing to the complex topology and little infrastructure support.

Routing is the centerpiece of network arrangement. It switches and succeeds message movement within the network. Routers retain swapping communications about link status, cost, and metrics to set up links and manage modified network topology. The essential purpose of a wireless network routing protocol is to create a right and a valid route among a couple of nodes so that messages communicated on time. The routing protocol effectively sets an upper limit for protection in any network of packets. Unless the routing misdirected, it will paralyze the whole network.

Three types of ad hoc routing protocols exist to date: constructive (DSDV, WRP), reactive (DSR, AODV), and hybrid (ZRP). Most protocols rely on finding the shortest route between two nodes; in other words, the length of the routes is the only metric used in such contracts. In certain instances, though, stability may be the most critical parameter.

Mobile Ad Hoc Network (MANET) attacks loosely divided into two main groups, namely, passive and aggressive ones. The successful attacks entail acts carried out by enemies, such as the duplication, alteration, and deletion of exchanged records. Blackhole intrusion, wormhole attack, rushing attack, spoofing, routing table overload, sleep deprivation, and location leakage are several examples of aggressive attacks that quickly conducted against an ad hoc network. Since the black hole attack creates significant consequences on the efficiency of the system, it should be correctly detected and solution given for the secure routing.

DOI 10.17148/IJARCCE.2020.9515

These attacks by black hole adversely affect the routing protocol for the Ad-hoc On-Demand Distance Vector (AODV). So, this paper goal to identify a black hole attack in the AODV-based network routing protocol and, consequently, rectify the attack.

II. RELATED WORKS

This section lists the survey of some current attempts to resolve the problem of routing misbehavior in ad hoc networks.

According to the 2007 survey carried out by Satoshi Kurosawa1, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, and Yoshiaki Nemoto[1], they suggested a Hierarchical Learning Approach in which the average gap between the Dst Seq message in RREQ and the one in the list determined. Every node registers the terminus IP address and the target sequence in its groups when sending or forwarding an RREQ message. When receiving an route reply packet , the station checks the list to see if there is an IP address of the same terminus. If it does exist, the target sequence difference premeditated, and this process performed on behalf of each route reply message received.

They suggested a method to pause and test the answers from all the surrounding nodes to catch a harmless route. V Sankaranarayanan and Latha Tamilselvan[2]. suggested solution that the requesting node must pause until further answers with next-hop particulars from the added neighboring nodes, without sending the data packs to the replying node simultaneously.

M. A. Shurman, and S. M. Yoo. Park[3], here, the source node tests the node validity triggering RREP by seeking over and above one route to the target. The sending node waits the route reply packet from more than two nodes to reach. The complementary routes in ad hoc networks often contain several mutual hops or nodes.

S. Ramaswamy, H. Fu, M. Sreekantaradhya, J. Dixon, K. Nygard[4], the suggested approach includes a data routing table where one for 'real' and zero for 'fake.' Whenever route reply packet received during the route discovery process, cross-checking performed to determine whether the answer originates from a reliable in-between node.

Following on from H. Deng, W. Li, D. P. Agrawal,[5], the process allows the in-between node to send next-hop details to an route reply packet.

As soon as a sending node accepts the route reply packet from an in-between node, it directs a additional request to the next hop to crisscross that it has a route to the in-between node that transfers the route reply packet rear and a route to the target.

Following on from S. Lee, Han B. and Han M. Shin, [6] approach allow the in-between node to direct route validation request to the succeeding target hop node. Next hop node then disobeying CREQ and examines up its accumulation for a target route.

III. PROPOSED WORK

Intrusion detection system has been designed based on the software development life cycle. Each node in MANETs monitors its neighbouring node and collects the data. An IDS is a section of computer and network infrastructure which is intended at spotting attacks against computer systems and network, or information system. The main constituents of IDS are information gathering, finding and reply.

In the above architecture, the analyzing component is built without any attacks to evaluate the network output utilizing the AODV routing protocol. It achieved by using the AODV routing protocol to establish a wireless MANET by transmitting the data packets using route request and route reply messages and eventually evaluating the whole network output.

The next section of architecture discusses how a black hole attack node generated and identified using the same AODV routing protocol. If the malicious node reacts with a bogus route response pretending to have a one-hop route to the target, then it is named a black hole attack node. The black hole discards such packets as data packets arrive. A forged route has created if the malicious response extents the requesting node before the targeted node replies. If the malicious system may inject itself between the transmitting nodes, it can do something about the packets that move through them. It may select to droplet the packets to accomplish a dos attack or custom its place on the route as the first step in a man-in-the-middle attack as an alternative. The efficiency parameters measured by simulation are packet size, overhead routing power, and average end-to-end latency.

DOI 10.17148/IJARCCE.2020.9515

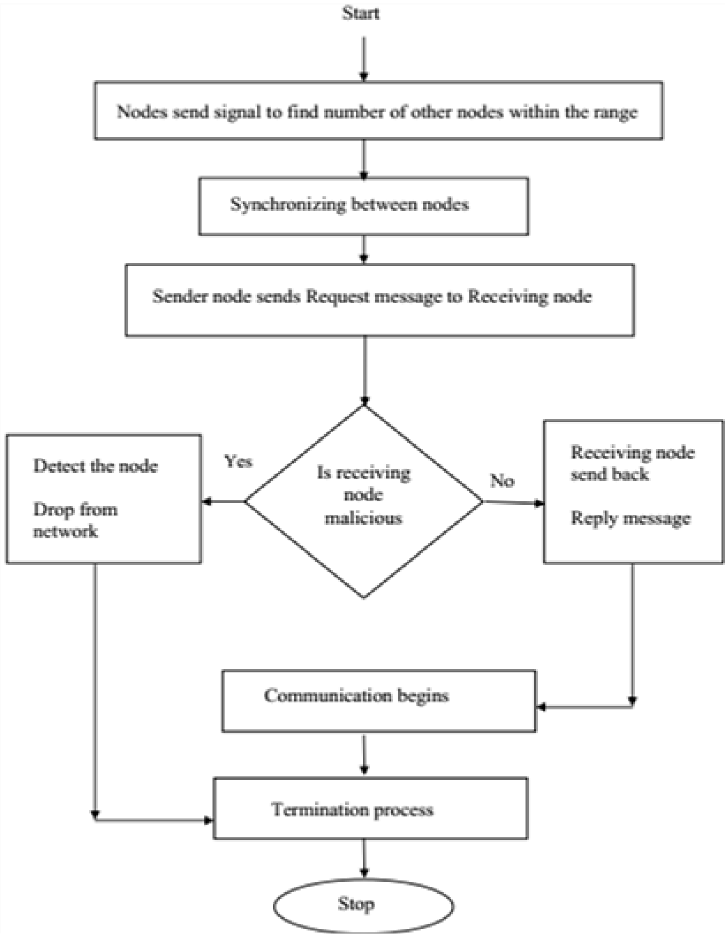
Start
Nodes send signal to find number of other nodes within the range
Synchronizing between nodes
Sender node sends Request message to Receiving node
Is receiving node malicious
Yes
No
Detect the node
Drop from network
Receiving node send back
Reply message
Communication begins
Termination process
Stop

Fig.1 Flow diagram of secured wireless networks

The final module describes the reaction to the black hole node, which formed. Here is the mechanism proposed, based on promiscuous eavesdropping to identify disobeying nodes. The detection is done by comparing the number of dropped to the number of positively accelerated data packets and then finally checking against the threshold value. Once finding a disobeying node, the finding node attempts to stop the node from being misbehaved and routes the packets through a separate direction to reach a secure route. Ultimately, the network efficiency parameters such as packet density, overhead routing control, and end-to-end average latency evaluated for both the network, i.e., the non-attack network and the black hole attack network.

IV. RESULTS AND DISCUSSION

The simulation has done using NS-2 to analyse the network's performance by varying the motion of the nodes from 10 m/s to 60 m/s.

A. *Simulation Parameters*

Table-I: Simulation Parameters for network without attack

Simulator	NS-2(ver.2.30)
Simulation time	200(s)
Number of mobile nodes	9
Topology	500m x 500m
Transmission Range	250meter
Routing Protocol	AODV
Maximum Bandwidth	2Mbps
Traffic	CBR
Maximum Speed	10-60(meter/second)
Pause Time	10(seconds)

DOI 10.17148/IJARCCE.2020.9515

In this paper, three significant success indicators evaluated below:

- The packets distribution ratio is the number of data packets acquired divided by the number of data packets created.
- The end-to-end delay calculated as the period when the target obtains a data packet, minus the period the source produces the data packet.
- The amount of AODV messages sent during the simulation is known as the overhead. For AODV messages directed over several hops, message transmission (every hop) counted as one transmission.

B. *Performance Metrics*

For the wireless network, efficiency measurements calculated with and without a black hole attack.

i) Packet delivery ratio

Simulation is performed with nine nodes to determine the packet distribution ratio, with the source node sending packet number to the target node. It shows from figure.2 that 100 percent of the packet distribution ratio is when there is no usual network versatility. When the black hole attacks the network, the packet delivery has fallen to about 80 percent when mobility is zero.

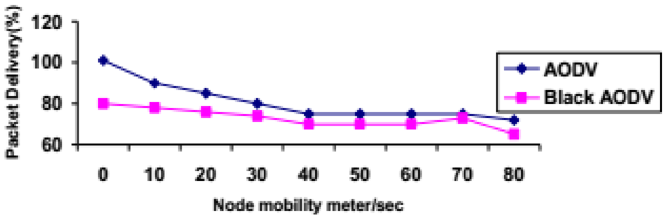

Fig. 2 Packet Delivery Ratio

ii) *Average end-to-end delay*

End to End latency measured from the time packet a source submitted to the target until the moment it was obtained. Here the time packet got from 10 m / s to 60 m / s for the mobility. From figure to figure. 3. We can see that the typical end-to-end latency is steady (with a slight dip) around the usual network mobility spectrum. When the black hole hits the network, the latency increases relative to a conventional system, because the cause is black hole node behavior. Whenever the black hole server sends the request, it is the first to respond to the data packets.

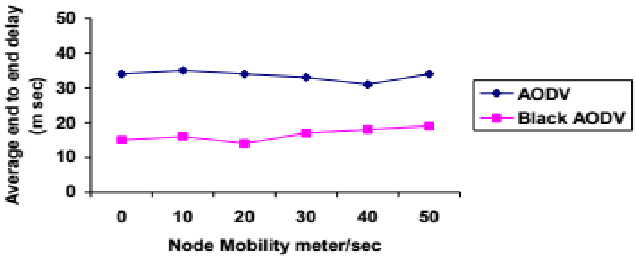

Fig. 3 Average end-to-end delay

iii) Routing overhead

The overhead routing calculated by finding the total amount of AODV messages transferred in a specified simulation time (ex. 1 sec to 5 sec). The transition number indicates the name of flows initiated during a given period. From figure 4 it can be shown that the overhead routing decreases as transaction numbers rise.

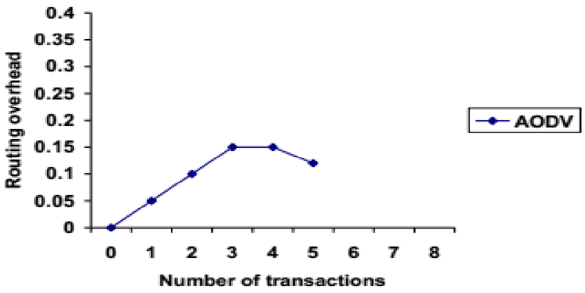

Fig. 4 Routing overhead

DOI 10.17148/IJARCCE.2020.9515

V. CONCLUSION

This paper analyzes a black hole attack that can be easily deployed in contrast to a MANET and proposes a possible elucidation for it in the AODV protocol. To identify the blackhole intrusion in mobile ad hoc networks and to protect against the threat, a promiscuous listening strategy based on the identification of disobeying nodes introduced. Upon detecting a disobeying node, the detecting node tries to avoid the disobeying node and route the packets along another route to find a safe route. Black AODV outperforms than AODV for finding blackhole attacks.

REFERENCES

[1]. 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, Vol.5, No.3, PP.338–346, Nov. 2007.

[2]. Dr. V Sankaranarayanan and Latha Tamilselvan "Prevention of Blackhole Attack in MANET," The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications, IEEE.(AusWireless 2007).

[3]. 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.

[4]. S. Ramaswamy, H. Fu, M. Sreekantaradhya, J. Dixon, K. Nygard, "Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks" Proceedings of the International Conference on Wireless Networks, June 2003.

[5]. H. Deng, W. Li, and D. P. Agrawal, "Routing security in ad hoc networks," IEEE Communications Magazine, vol. 40, no. 10, pp. 70-75, Oct. 2002.

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

[7]. Animesh Patcha and Amitabh Mishra "Collaborative Security Architecture for Black Hole Attack Prevention in Mobile Ad Hoc Networks", IEEE, 2006.

[8]. S. Marti, T.J. Giuli, K. Lai, M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," 6th MobiCom, Boston, Massachusetts, August 2000

[9]. Satish Salem Ramaswami and Shambhu Upadhyaya, " Smart Handling of Colluding Black HoleAttacks in MANETs and Wireless Sensor Networks using Multiroute Routing" Workshop on Information Assurance Proceedings , IEEE, 2006.

[10]. Bo Sun Yong Guan Jian Chen Udo W. Pooch, "Detecting Black-hole Attack in Mobile Ad Hoc Networks" EPMCC, IEEE, 2003.

[11]. Alem, Y. F., & Xuan, Z. C. (2010, May). Preventing black hole attack in mobile ad-hoc networks using Anomaly Detection. In Future Computer and Communication (ICFCC), 2010 2nd International Conference on (Vol. 3, pp. V3-672). IEEE.

[12]. Alheeti, K. M. A., Gruebler, A., & McDonald-Maier, K. D. (2015, January). An intrusion detection system against malicious attacks on the communication network of driverless cars. In Consumer Communications and Networking Conference (CCNC), 2015 12th Annual IEEE (pp. 916-921)

[13]. Alikar GA, Biradar RC. A survey on hybrid routing mechanisms in mobile ad hoc networks. J Netw Comput Appl. 2017;77:48–63

DOI 10.17148/IJARCCE.2020.9515