RESEARCH ARTICLE OPEN ACCESS

Study of DSR and AODV under Sinkhole Attack and Its Proposed Prevention Technique

Winnie Main*, Narendra M. Shekokar**
*(Computer Engineering Department, D.J. Sanghvi College of Engineering, Mumbai University, India)
** (Computer Engineering Department, D.J. Sanghvi College of Engineering, Mumbai University, India)

ABSTRACT
Mobile Ad-hoc Networks (MANET) are wireless mobile nodes that communicate without any predefined infrastructure. This allows MANETs to be easily setup in geographical and terrestrial constraints. To achieve this kind of communication MANET routing protocols play an important role. Two routing protocols, DSR and AODV are studied in detail. This basic trait of a MANET makes its routing protocols very vulnerable to security attacks. One such attack is the 'Sinkhole' attack which lures packets towards the sinkhole node. A malicious Sinkhole node severely degrades the network once the attack is in progress. This paper describes two of the popular MANET routing protocols, DSR and AODV and the sinkhole attack on these protocols. Prior research carried out to prevent the sinkhole attack is analyzed. Multiple procedures are documented to prevent and mitigate the problem of Sinkhole in MANETs. The proposed solution relies on tackling the sequence number discontinuity to contain Sinkhole attacks. A prevention technique is proposed that relies on the fact that the sequence number discontinuity if tackled can go a long way in containing Sinkhole attacks.

***Keywords* -** AODV, DSR, MANET, Security, Sinkhole

I. INTRODUCTION

MANETs are a collection of wireless network nodes which lack any predefined infrastructure for communication and rely upon temporary network topologies. The MANETs provide an easy method of link setups in situations of geographical or terrestrial constraints. Applications in military warfare, emergency and disaster situations are some examples of a MANET [1]. As a result of this setup simplicity, MANETs are more vulnerable to the security at-tacks. Sinkhole attack is one of the severe attacks in MANETs. This attack makes trustable nodes vulnerable to malicious nodes which results in loss of secure information.

This paper discusses Sinkhole attack in the context of routing protocols, namely AODV and DSR. The literature survey and results support the theory of degradation in the network after an attack. Multiple procedures are present to prevent and mitigate the problem of Sinkhole in MANETs. The proposed solution relies on the fact that the sequence number discontinuity if tackled can go a long way in containing Sinkhole attacks. This solution is based on Digital Encryption, Sequence Number Discontinuity Check and Sequence Number Duplication check.

The remainder of this paper is organized as follows: Section II describes two of the popular MANET routing protocols, DSR and AODV and the sinkhole attack on these protocols. Section III analyzes the protocol under sinkhole attack. Section IV outlines related work carried out in the prevention and detection of sinkhole attacks. Section V proposes a novel prevention technique for sinkhole attack. Section VI concludes the paper.

II. DSR, AODV AND SINKHOLE

The Dynamic Source Routing protocol (DSR) [2] is an efficient and simple routing protocol designed specifically for MANETs. The on-demand nature of the protocol adds routing information to be included in the packet overhead. Each sender is able to select and control the routes used in routing its packets to the destination, through multiple routes.

The Ad hoc On-Demand Distance Vector (AODV) [4] algorithm enables dynamic, self-starting, multihop routing between participating mobile nodes in a MANET. AODV allows mobile nodes to obtain routes quickly for new destinations, and does not require nodes to maintain routes to destinations that are not in active communication. AODV allows nodes to take into effect any links gone down and allows the routing to be modified accordingly.

Sinkhole attack is one of the most severe attacks on mobile Ad-hoc networks [6]. A sinkhole node tries to lure nearly all the network traffic towards it. Sinkhole attack will be launched by making the compromised node look attractive and better intermediate node to reach the destination. This is done either by introducing new bogus routing packets on the network or by changing the content of the genuine packets. The Sinkhole node may drop the packets or launch some other severe attacks. It increases network overhead, decreases network's life time by boosting energy consumption and finally destroys the network.

The sinkhole node modifies the sequence number in the RREQ packet with a higher value. This is treated as a fresh route (updated route) to the destination node. The neighboring nodes upon receiving this bogus RREQ, assume that it is a better route and updates this route in their cache and broadcasts it to the destination node. The destination node will generate a RREP for this bogus RREQ and sends it to the source node. Thus a route is established and the packets are lured towards the sinkhole node. Instead of creating the bogus RREQ the sinkhole can also modify the RREQ by adding itself in the route. RREP is sent back to the source projecting that it has better route to the destination.

III. Protocol Analysis Under Sinkhole

The two routing protocols DSR and AODV are analyzed over 3 parameters of packet delivery ratio (PDR), Throughput and Packet drop. The effect under a sinkhole attack is also noted.

3.1 DSR

Packet Delivery Ratio (PDR) is the ratio of number of packets received at destination to the number of packets sent by source node [6]. A decrease in packet delivery ratio is observed when sinkhole is present. Packets which are not delivered to the destination may be forwarded by the sinkhole node to another node in the network or may be dropped. This can cause fluctuations in the delivery ratio as the sinkhole may selectively drop or forward packets.

Throughput is the total number of packets received by the destination node over a period of time [6]. It has been observed that throughput decreases with time. The reason is sinkhole has access to more packets on the network and sinkhole will not allow the packets to reach the destination and hence the throughput decreases.

Packet drop is the difference between the number of packets sent by the source node to that of the number of packets received by the destination node [6]. The behavior of sinkhole nodes is to drop or reroute any packets it receives. As a result, packet drop increases in the presence of sinkhole attacks.

3.2 AODV

The greater value of packet delivery ratio (PDR) means better performance of the protocol [5]. When the network is under a AODV Sinkhole attack, it is observed that the PDR value is low. This is in-line with the described Sinkhole attack behavior where the Sinkhole node drops or delay packets from source.

The Throughput of the network without any attack for AODV is seen to be continuously increasing. Again in-line with the expected behavior of a Sinkhole node, we see that the throughput is low when attacked by a Sinkhole node.

The lower the value of the packet loss means the better performance of the protocol [5]. This result is the reverse from the previous two, in the sense that Packet Loss is low when the network is not under attack. From the results [5], we can say that, the packet loss for original AODV decreases constantly at the same time packet loss for sinkhole AODV is high compare to original AODV.

Since sinkhole attack has major repercussions in the performance of the network, it needs to be addressed for both AODV and DSR.

IV. Related Work

There has been a lot of research on the problem of Sinkhole attack which affects MANETs. Many different identification, prevention and mitigation methods have been proposed. The below survey describes few papers researched along with the analysis of the different implemented techniques.

Nisarg Gandhewar et al [5], discusses the sinkhole problem, its consequences & presents a mechanism for detection & prevention of it on the context of AODV protocol. The detection and prevention technique is based on sequence numbers. The paper does not consider the problem of duplicate sequence numbers. Also, no action has been taken after sequence number is identified. There is also no mentioned technique mentioned to prevent the attack from happening.

Sonal R. Jathe et al [7], inspects the different kinds of security attacks in MANETs, addresses the sinkhole problem and describes different parameters for attack detection technique based on sequence number discontinuity. The paper talks about how the Sinkhole attack can be detected by identifying requests with a very high sequence number. There is no clear prevention technique mentioned.

Benjamin J. Culpepper et al [3] analyzes the sinkhole attack on DSR. An intrusion detection system is proposed for detecting sinkhole attacks. The sequence number check method is the underlying logic which is implemented here. However, the problem of duplicate sequence numbers as well as encryption has not been validated.

V. Proposed Prevention Technique

After studying the underlying problem of Sinkhole attack in MANET, the security around the sequence numbers is further analyzed. The quality of messages received from neigh-boring nodes with out-of-order, missing or duplicate sequence numbers is kept under watch. This term is measured by the overall average difference between the current and the last sequence number from each node [3]. A penalty is then introduced for every suspicious packet.

Each RREQ packet can be uniquely identified by a 3-tuple: <source, destination, sequence number>. In a fully cooperating network, the sequence numbers contained in packets that originate from a node are strictly increasing [3]. This is not true in a network with a malicious node that is attacking the network. In this case, the attacker node emits packets with an unusually high sequence number to ensure that the bogus route will replace any previously learned routes in the nodes under attack. For this reason, it makes sense for a node to monitor the sequence numbers contained in all packets it receives, taking care to note when the sequence emitted by packets purporting to originate from a single node is not strictly increasing. This property is called sequence number discontinuity [3].

For attacks from superior malicious nodes, an issue of receiving packets with duplicate sequence number can also be encountered. This scenario will pan out when a malicious node sets its sequence number slightly higher than the current sequence number being used. Legitimate will continue sending packets with increasing sequence numbers and a situation will arise of receiving duplicate sequence numbers as well.

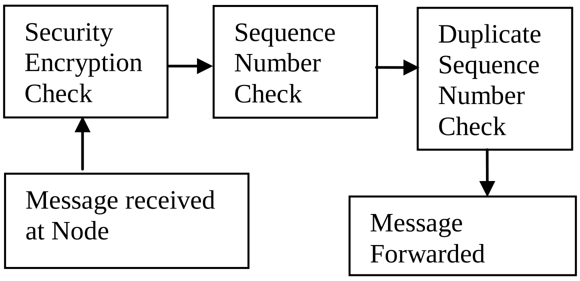

Fig -1: Proposed Prevention Technique

- Step1: Security encryption check

A secret key is shared with each genuine node. Each packet is encrypted and decrypted with this key.

- Step2: Sequence number check

A threshold_diff parameter is set based on network size. Next, a prob_mal_node parameter is also set. The difference between the current sequence number and the previously received sequence number for the same tuple is calculated. If the difference is less than the threshold_diff, the packet is forwarded. Else if the difference is greater than the threshold_diff, the value of the prob_mal_node is incremented and the packet is dropped. Else if the value of prob_mal_node is less than its threshold, the packet is forwarded.

- Step 3: Duplicate sequence number test

A dup_threshold parameter is set based on network size. Another dup_prob_mal_node parameter is also set. Increment the value of dup_prob_mal_node. Now if the value of dup_prob_mal_node exceeds its dup_threshold, mark node as malicious node and drop the packet. Else is the value of prob_mal_node is less than its threshold, forward the packet.

- Step 4: Message Flow

Each packet is received at node A. Start a first_time timer after receiving the first RREQ packet and note down the tuple. If the packet is encrypted then proceed for Security Encryption Check Using the previously shared secret key, decrypt the packet. If the packet cannot be decrypted, drop the packet. If the packet can be decrypted, proceed to extract packet contents. If the packet is received with a new sequence number, perform Sequence Number Check. Else if the sequence number has been previously received from the same tuple and if the first_time timer has not yet expired, drop the packet. If the first_time timer has expired, perform Duplicate Sequence Number Test. Else drop the packet.

The above proposed 3-fold prevention technique will effectively curtail the sinkhole problem. The performance of both the protocols and the network can then be improved.

VI. Conclusion

The ease of setting up a MANET also makes it open to attacks. A malicious Sinkhole node severely degrades the network once the attack is in progress. The routing protocols of DSR and AODV are analyzed and their performance under the sinkhole attack is noted.

Multiple procedures are available to prevent and mitigate the problem of Sinkhole in MANETs. The proposed solution relies on tackling the sequence number discontinuity to contain Sinkhole attacks. A basic level encryption is first step. The sequence number check then follows. Care has also been taken to check duplicate sequence numbers as stealthier nodes may be intelligent enough to send packets with not so large sequence numbers. The proposed algorithm also takes into account the fact that certain network characteristics may incorrectly mark nodes as malicious. The element of ‘probable malicious node’ helps to overcome the incorrectness. Further research on Sinkhole attacks in MANETs may result in newer routing protocols being introduced which will be more resistant to these attacks.

References

[1] Hongmei Deng, Wei Li, and Dharma P. Agrawal, Routing Security in Wireless Ad

Hoc Networks, *IEEE Communications Magazine*, October 2002, pages 70-75.

[2] D. Johnson, Y. Hu and D. Maltz, The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4, IETF RFC 4728, February 2007; *www.rfc-editor.org/rfc/rfc4728.txt*

[3] Benjamin J. Culpepper, H. Chris Tseng, Sinkhole Intrusion Indicators in DSR MANETs, *Proceedings of the First International Conference on Broadband Networks (BROADNETS 04)*, IEEE Computer Society, 2004

[4] C. Perkins, E. Belding-Royer and S. Das, Ad hoc On-Demand Distance Vector (AODV) Routing, IETF RFC 3561, July 2003; *www.rfc-editor.org/rfc/rfc3561.txt*

[5] Nisarg Gandhewar, Rahila Patel, Detection & Prevention of Sinkhole Attack on AODV Protocol in Mobile Adhoc Network, *2012 Fourth International Conference on Computational Intelligence and Communication Networks*, IEEE Computer Society, 2012

[6] Mohammed Ashfaq Hussain, Dr. A. Francis Saviour Devaraj, Upshot of Sinkhole Attack in DSR Routing Protocol Based MANET, *International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com, Vol. 3, Issue 2,* March -April 2013, pp.1737-1741

[7] Sonal R. Jathe, D.M. Dakhane, Detection of Sinkhole Attack against DSR Protocol MANET, International Journal of Advanced Research in *Computer Science and Software Engineering, Volume 2, Issue 4,* April 2012

[8] Bing Wu, Jianmin Chen, Jie Wu and Mihaela Cardei, A Survey on Attacks and Counter measures in Mobile Ad Hoc Networks, in Yang Xiao, Xuemin Sherman Shen, Ding-Zhu Du (Ed.), Wireless Mobile Network Security, Ch. 12 (USA: Springer, 2007) 103-135.

[9] Gagandeep, Aashima, Study on Sinkhole Attacks in Wireless Adhoc Networks, *International Journal on Computer Science and Engineering (IJCSE), Vol. 4 No. 06* June 2012.