Effective Filtering Scheme against RREQ Flooding Attack in Mobile Ad Hoc Networks

Jian-Hua Song[1, 2], Fan Hong[1], Yu Zhang[1]

[1]College of Computer Science and Technology, Huazhong University of Science and Technology, Wuhan 430074, Hubei, China
sjhhust@163.com

[2]School of Mathematics and Computer Science, Hubei University, Wuhan 430062, Hubei, China
sjhhubu@163.com

Abstract

In Mobile Ad hoc Networks (MANET), various types of Denial of Service Attacks (DoS) are possible because of the inherent limitations of its routing protocols. The attack of initiating / forwarding fake Route Requests (RREQs) can lead to hogging of network resources and hence denial of service to genuine nodes. This type of attack is hard to detect since malicious nodes mimic normal nodes in all aspects except that they do route discoveries much more frequently than the other nodes. A distrusted filtering mechanism is proposed to mitigate such situations and reduce the loss of throughput. The proposed mechanism could prevent this specific kind of DoS attack and does not use any additional network bandwidth.

1. Introduction

A mobile ad hoc network (MANET) is a collection of wireless devices moving in seemingly random directions and communicating with one another without the aid of an established infrastructure. Communicating nodes in a Mobile Ad hoc Network usually seek the help of other intermediate nodes to establish communication channels. Thus, the communication may be via multiple intermediate nodes from source to destination. Because of node mobility, network topology and hence the routes change frequently. Malicious nodes may become part of actively used routes and disrupt network operation. In such an environment, malicious intermediate nodes can be a threat to the security of conversation between mobile nodes. Examples of attacks include passive eavesdropping over the wireless channel, denial of service attacks by malicious nodes and attacks from *compromised* nodes.

In this paper, we focus on a special type of DoS attack due to RREQ flooding attack. In this type of attack, those malicious nodes behave like the normal nodes in all aspects except that they initiate frequent RREQ control packet floods. This type of attack is hard to detect since any normal node with frequently broken routes could legitimately initiate frequent route discoveries. One or more malicious nodes flooding the MANET with RREQ control packets related to bogus route discoveries can cause a sharp drop in network throughout.

The rest of the paper is organized as follows. In section 2, we describe the DoS attack caused by RREQ

Foundation item: This work is supported by the National Natural Science Foundation of China (60403027) and the Natural Science Foundation Of Hubei Province of China (2005ABA243).

Proceedings of the Seventh International Conference on
Parallel and Distributed Computing,Applications and Technologies (PDCAT'06)
0-7695-2736-1/06 $20.00 © 2006 IEEE

flooding. In section 3 we describe some related work. A filtering mechanism is proposed in section 4 and evaluated in Section 5. Section 6 concludes the paper.

2. DoS attack due to RREQ flooding

The Route Request (RREQ) Flooding Attack is a kind of denial-of-service attack, which aims to flood the network with a large number of RREQs to the destinations in the network. In this attack, the malicious node will generate a large number of RREQs, possibly in the region of hundreds or thousands of RREQs, into the network until the network is saturated with RREQs and unable to transmit data packets.

Many different reactive (on-demand) dynamic routing protocols proposed for MANETs can suffer from this kind of attack. In an on-demand dynamic routing protocol, it usually uses a "route discovery" process to dynamically obtain a route when a node attempts to send a data packet to a destination for which it does not already know the route. The route discovery works by flooding the network with route request (RREQ) control packets. A node that receives a RREQ rebroadcasts it, unless it has already seen it from another neighbor or it has a route to the destination indicated in the RREQ. If the received RREQ is a duplicate, it will be dropped. If a node has the route because it is the destination or it has learned it in another route discovery, then it replies to the RREQ with a route reply (RREP) packet that is routed back to the original sender of the RREQ. A drawback of blind flooding based route discovery process is the high control overhead. Each RREQ initiated by a node results in n broadcasts in the MANET, where n is the number of nodes in the MANET. As we know, in an ad hoc wireless network where wired infrastructures are not feasible, energy and bandwidth conversation are the two key elements presenting research challenges. Limited bandwidth makes a network easily congested by control signals of the routing protocol. As the mobility and load of the network increases, the RREQ control packets used for route discoveries may consume more bandwidth than the data packets. Malicious nodes could exploit this potential weakness of routing protocols. Attackers can initiate much more REEQ control packets than the normal nodes to consume network resource. Since control packets are given higher priority over data packets in transmitting, then at high loads, the wireless channel usage can be completely dominated by the control packets used for route discoveries. In this situation, valid communication can't be kept and normal network nodes cannot be served, then it leads to a kind of denial-of-service attack.

In some on-demand protocols, for example AODV, a malicious node can override the restriction put by *RREQ_RATELIMIT* (limit of initiating / forwarding RREQs) by increasing it or disabling it. A node can do so because of its self-control over its parameters. The default value for the *RREQ_RATELIMIT* is 10 as proposed by RFC 3561. A compromised node may choose to set the value of parameter *RREQ_RATELIMIT* to a very high number. This allows it to flood the network with fake RREQs and leads to a kind of DoS attack. In this type of DoS attack a non-malicious node cannot fairly serve other nodes due to the network-load imposed by the fake RREQs. This will not only lead to the exhaustion of the network resources like memory (routing table entries), but also lead to the wastage of bandwidth and the wastage of nodes' processing time.

3. Related work

Significant work has been done to secure routing protocols against attacks on routing traffic. Most of them apply cryptographic techniques (asymmetric or symmetric) to authenticating routing traffic and can prevent external intruders from joining the network or malicious insiders from spoofing or modifying routing messages [1]. But these enhancements still cannot handle this type of attack caused by RREQ flooding

since the malicious node is not forging any information.

The AODV RFC specifies that a node should not originate more than RREQ_RATELIMIT RREQs per second. This can prevent attacks from the application layer but does not prevent the attacker from modifying the routing protocol to set RREQ_RATELIMIT to a very large value. Furthermore, the static limit on RREQs generated by a node can hurt the performance of the network. If the limit is too low, it will restrict the route discovery capability of genuine nodes. Genuine RREQ attempts to reachable destinations can be hindered since they may be dropped when RREQ_RATELIMIT is always reached due to excessive forged RREQs. And a high static limit is not effective.

In Ariadne[2], route discovery chains are used to rate-limit the number of route discoveries. Each route discovery needs a key from the route discovery chain and the release of keys can be regulated. This limits the impact of RREQ flooding attack on the network but a fixed number of forged RREQs can still be injected into the entire network. Furthermore, genuine RREQ attempts from a compromised node to reachable destinations may never be sent if the number of forged RREQs generated by it is large.

In [3], an adaptive statistical packet dropping mechanism is proposed to defend against malicious control packet floods like RREQ flooding attack. Each node maintains a count of RREQs received for each RREQ sender during a preset time period. The RREQs from a sender whose smoothed average rate is above the rate limit will be dropped without forwarding. The mechanism has some drawbacks. Dropping RREQ will lead to the reduction of throughput of the network. And also some normal nodes with higher rate will be treated as malicious nodes.

In [4], a priority system is used to determine the transmission priority of RREQs. When the malicious node broadcast excessive RREQs, the priorities of its RREQs are reduced. But this method does not distinguish between genuine and forged RREQs from the malicious or victim nodes.

In [5], a route request flooding defense mechanism is proposed to mitigate the effect of denial of service attacks by flooding with RREQs to unreachable destinations. The scheme consists of three components: RREQ binary exponential backoff, Route Discovery Cycle (RDC) binary exponential backoff and Fast Recovery. The main shortcoming is that it can't isolate the malicious nodes.

4. Proposed Scheme

In this section, we propose a simple, distributed, and adaptive technique to automatically control the spread of RREQ packets and reduce the effects of broadcast attacks using RREQ. We assume that there exists a security mechanism, such as public key cryptography and digital signatures or MAC (Message Authentication Code) that enables a node to authenticate routing messages from any node in the network. Therefore, a malicious node cannot spoof the originator and destination IP addresses in a RREQ packet although the destination IP address may not be reachable in the network.

The proposed technique uses a filter to detect misbehaving nodes and reduces their impact on network performance. The aim of the filter is to limit the rate of RREQ packets. Each node maintains two threshold values. The threshold values are the criterion for each node's decision of how to react to a RREQ message.

The *RATE_LIMIT* parameter denotes the number of RREQs that can be accepted and processed as normal per unit time by a node. Each node monitors the route requests it receives and maintains a count of RREQs received for each RREQ originator during a preset time period. Whenever a RREQ packet is received, a check is performed. If the rate of this RREQ originator is below the *RATE_LIMIT*, the RREQ packet

is processed as normal.

The *BLACKLIST_LIMIT* parameter is used to specify a value that aids in determining whether a node is acting malicious or not. If the number of RREQs originated by a node per unit time exceeds the value of *BLACKLIST_LIMIT*, one can safely assume that the corresponding node is trying to flood the network with possibly fake RREQs. On identifying a sender node as malicious, it will be blacklisted. This will prevent further flooding of the fake RREQs in the network. The blacklisted node is ignored for a period of time given by *BLACKLIST_TIMEOUT* after which it is unblocked. The proposed scheme has the ability to block a node till *BLACKLIST_TIMEOUT* period on an incremental basis. By blacklisting a malicious node, all neighbors of the malicious node restrict the RREQ flooding. Also the malicious node is isolated due to this distributed defense and so cannot hog its neighbor's resources. The neighboring nodes of the malicious node are therefore free to entertain the RREQs from other genuine nodes. In this way genuine nodes are saved from experiencing the DoS attack.

If the rate of RREQs originated by a node is between the *RATE_LIMIT* and the *BLACKLIST_LIMIT*, the RREQ packet is added to a "delay queue" waiting to be processed. Every time a *DELAY_TIMEOUT* expires, if there is anything in the delay queue (RREQ packet waiting to be processed), then the first packet is removed to be processed. To do so, malicious node that has a high attack rate will thus be severely delayed. Meanwhile, the proposed rate control mechanism will have no impact on other nodes and also have minimal impact on the normal nodes that send abnormally high RREQs.

The filter process is shown in figure 1.

The filtering forwarding scheme slows down the spread of excessive RREQs originated by a node per unit time and successfully prevents DoS attacks. The proposed scheme incurs no extra overhead, as it makes minimal modifications to the existing data structures and functions related to blacklisting a node in the existing version of pure AODV. Also the proposed scheme is more efficient in terms of resource reservations and its computational complexity. In addition to limiting the clogging up of resources in the network, the proposed scheme also isolates the malicious node.

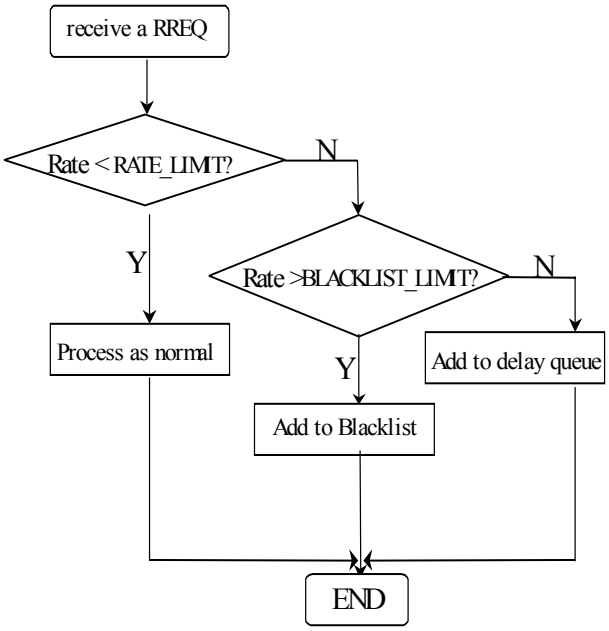

Figure 1. Processing of the received RREQ

5. Simulation Results

NS-2 simulator is used for the implementation of the proposed scheme. The AODV routing protocol is used for all simulations. 50 Nodes were randomly generated in an area of $500m \times 500m$. Traffic sources used are Constant-Bit-Rate (CBR) with a rate of 2pkts/sec and 512 bytes/pkt. The minimum speed for the simulations is 0 m/s while the maximum speed is 20 m/s. The selected pause time is 0 seconds. The malicious node floods the network with bogus route discoveries at a rate of 0 to 20 RREQs/s. A random node is selected to be the destination for which this malicious node initiates bogus route discoveries. The malicious node drops any route information received in

response to its route discoveries and continues to initiate route discoveries at the specified rate. In AODV protocol, a node should not originate more than 10 RREQ messages per second. Here we set the *RATE_LIMIT* threshold to 5 and set the *BLACKLIST_LIMIT* up to 10. The malicious node starts flooding the network with fake RREQ's at simulated time of 50s till time 100s.

The performance evaluation of the proposed detection scheme involves study of two different aspects: performance of original AODV protocol in presence of compromised nodes and performance of proposed scheme in presence of compromised nodes. The metrics are the important determinants of network performance, which have been used to compare the performance of the proposed scheme in the network with the performance of the original protocol. We use Packet Delivery Ratio and End-to-End Delay as the metrics. The results are in figure 2and figure 3. On the x-axis we plot the number of RREQ per second.

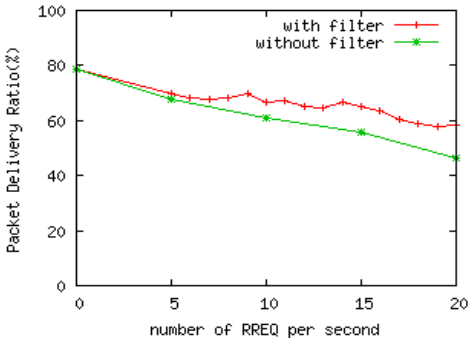

Figure 2. Packet Delivery Ratio

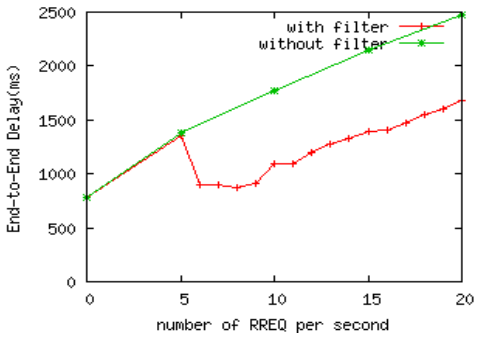

Figure 3. End-to-End Delay

From the figures above, it is found that the proposed filter scheme can work well in the network with high mobility. The improvement in the proposed scheme is due to the fact that there exists optimum utilization of the network resources and there is no overload, leading to comparatively lesser packet drops. When some normal nodes send abnormally high RREQs due to high mobility, it is better to delay the request than to drop them directly since these nodes should not be denied of service. The route established in this scheme is expected to be the optimum route, which consists of fewer intermediate nodes. Thus, no DoS attack is experienced in the developed scheme.

6. Conclusions

In this paper, we introduce a simple rate based control packet forwarding mechanism to mitigate malicious control packet floods. The DoS attack caused due to RREQ flooding in ad hoc network can be successfully detected in the proposed scheme. The malicious nodes identified are blacklisted and none of the genuine nodes in the network are wrongly accused of misbehaving. In the proposed scheme, there is an enhancement in the performance of the network in presence of compromised nodes. Further, the protocol can be made secure against other types of possible DoS attacks that threaten it.

References

[1] M. G. Zapata and N. Asokan, "Securing Ad hoc Routing Protocols", *Proceedings of the ACM Workshop on Wireless Security (WiSe 2002),* September 2002, pp. 1-10

[2] Yih-Chun Hu, Adrian Perrig, and David B. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks", *Proceedings of the Eighth Annual International Conference on Mobile Computing and Networking (MobiCom 2002)*, ACM, Atlanta, GA, September 2002, pp. 12-23

[3] S. Desilva and R.V. Boppana, "Mitigating

Malicious Control Packet Floods in Ad Hoc Networks" , *Proceedings of 2005 IEEE Wireless Communications and Networking Conference (WCNC05)*, March 2005, pp. 2112-2117

[4] P. Yi, Z. Dai, Y. Zhong and S. Zhang, "Resisting Flooding Attacks in Ad Hoc Networks", *Proceedings of International Conference on Information Technology: Coding and Computing (ITCC'05)*, April 2005, pp.657-662

[5] Zhi Ang EU and Winston Khoon Guan SEAH, "Mitigating Route Request Flooding Attacks in Mobile Ad Hoc Networks", *Proceedings of International Conference on Information* networking (ICOIN-2006), Sendai, Japan, 2006

[6] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks", Mobile Computing and Networking, 2000, pp.255-265

[7] Jonathan M. McCune, Elaine Shi, Adrian Perrig, Michael K. Reiter, "Detection of denial-of-message attacks on sensor network broadcasts", *Proceedings of IEEE Symposium on Security and Privacy*, May 2005, pp.64-78

[8] W. Yu, Y. Sun, and K. J. R. Liu, "HADOF: Defense against routing disruptions in mobile ad hoc networks," in *IEEE INFOCOM*, Miami, FL, March 2005