Handling Malicious Flooding Attacks through Enhancement of Packet Processing Technique in Mobile Ad Hoc Networks

NAVEEN YADAV, KRISHAN KUMAR, PRAVESH SHARMA

(DRONACHARYA COLLEGE OF ENGINEERING)

ABSTRACT **Mobile ad hoc networks are expected to be widely used in the near future. However, they are susceptible to various security threats because of their inherent characteristics. Malicious flooding attacks are one of the fatal attacks on mobile ad hoc networks. These attacks can severely clog an entire network, as a result of clogging the victim node. If collaborative multiple attacks are conducted, it becomes more difficult to prevent. To defend against these attacks, we propose a novel defense mechanism in mobile ad hoc networks. The proposed scheme enhances the amount of legitimate packet processing at each node. The simulation results show that the proposed scheme also improves the end-to-end packet delivery ratio.**

Keywords—Collaborative Attack, Malicious Flooding Attack, Wireless Ad Hoc Network

I. INTRODUCTION

As many users like to use mobile equipment such as cell phones, smart phones, laptops etc. mobile ad hoc networks are expected to be widely used in the near future.

Today’s mobile nodes have a broad range of applications. With the introduction of smart phones into the market, there is an immense need for privatization and security. Today’s mobile nodes do not have many restrictions in terms of processor speed etc. One main problem existing in mobile nodes in use these days is their battery life due to the immense energy that they depend upon. But, this is not the problem we will be discussing in the following paper. In the present research we assume that this energy is available in sufficient quantities for the mobile nodes to be able to function and process data.

As the technology involving mobile nodes is developing at a fast pace, we expect that mobile ad hoc networks, which use mobile nodes as communication entities, will be widely used in the future.

In mobile ad hoc networks, mobile nodes communicate with other nodes helped by neighboring nodes rather than base stations in a multi-hop fashion [1]. Hence, mobile ad hoc networks do not require any additional costs, such as costs for installing base stations, and are formed on-the-fly.

However, all signals go through bandwidth-constrained wireless links [1]. Moreover, mobile nodes used in mobile ad hoc networks are compact and portable, so they have limited resources

such as memory space, battery power, etc. [2-3]. Besides, as the nodes in the network are mostly handheld equipment, they move out of or join networks dynamically.

There are many possible attacks such as black hole attacks [4], wormhole attacks [5], malicious flooding attacks [6], and so on. The malicious flooding attack is one of the fatal attacks on existing on-demand routing protocols. Malicious flooding attacks can be performed either by forwarding many Route Request (RREQ) packets or data packets. Hence, they can be categorized into RREQ flooding attacks and data flooding attacks.

In on-demand routing protocols like Ad hoc On Demand Vector (AODV) [7], a mobile node sends a RREQ packet to initiate route discovery. Either the destination node, or an intermediate node, which has a fresh enough route to the destination node, sends a Route Reply (RREP) packet back to the source node. On receiving the RREP packet, the source node constructs a path and then transmits data packets through this path. If the path is disconnected during data transfer, a Route Error (RERR) packet is sent to the source node to notify the path failure and then, the path is reinitiated. Hence, the RREQ packet is an essential packet in mobile ad hoc networks since it is used for establishing a data transmission path. The malicious flooding attacker(s) floods many RREQ packets to or through the victim node as if they were trying to establish a path.

Meanwhile, after constructing the path, the attacker(s) flood many data packets to or via the victim node in order to paralyze the node. Moreover, the packet size of such data packets is much larger than that of a RREQ packet, so they easily clog the victim node [8]. Further, the attacker(s) exhaust the battery power of the victim node and then isolate it from the network. Therefore, the malicious flooding attack leads to a Denial-of-Service (DoS) attack [9], on the victim node in that the attack can neutralize the availability of the victim node [6]. Hence, the performance of processing legitimate packets at the victim node is significantly degraded.

Furthermore, the malicious flooding attack is hazardous to mobile ad hoc networks, not only because it clogs the victim node, but also because it clogs the entire network [6]. The malicious flooding attack is much harder to prevent when it is performed by colluded multiple attackers. Hence, it is necessary to devise a defense mechanism against malicious flooding attacks performed by collaborative attackers.

Therefore, we propose a novel defense mechanism against malicious flooding attacks, performed by collaborative attackers. The contributions of the paper are as follows: we improve the amount of legitimate packet processing at each node in order to improve the end-to-end packet delivery ratio. We also present various categories of possible malicious flooding attacks. We defend against malicious flooding attacks, collaboratively conducted by flooding nodes using RREQ packets, data packets, or both. Then, we evaluate the proposed defense mechanism.

The rest of the paper is organized as follows: Section 2 shows the amount of legitimate packets to be processed at each node. Section 3 categorizes the malicious flooding attacks, into four specific cases. Section 4 presents previously done related works for defending against malicious flooding attacks. Section 5 explains the procedure of the proposed scheme. Section 6 presents the evaluation results. Finally, the paper is concluded in Section 7.

2. PROBLEM STATEMENT

The packet delivery ratio between source nodes and destination nodes can be enhanced by processing more legitimate packets at each mobile node. Hence, we focus on measuring the amount of legitimate packet processing at each mobile node.

Without loss of generality, we consider a transmission from any node i to a neighboring node j, where i ≠ j and j∈ {1… N}, where N is the number of nodes in the network.

The node j can receive a packet from multiple neighboring nodes, so i ℵ {1,…, n}, where nℵ{1,…, N}. The number of packets transferred to the node j from its neighboring nodes (Rcvj) is as:

$$Rcv_j {}^{=} \sum_{i=1}^{n} (Rcv_{ij}). \qquad (1)$$

Here, Rcvij is the number of packets that the node j received from a neighboring node i.

Note that each node forwards RREQ and RREP packets in order to perform route discovery and RERR packets to notify path failure to the source node. Data packets are forwarded to the neighboring nodes. Hence, we can present Rcvj by the following equation, where α, β, γ, and δ are the number of data packets, RREQ packets, RREP packets, and RERR packets, respectively:

$$Rcv_j = \alpha+\beta+\gamma+\delta. \qquad (2)$$

However, the malicious flooding attack is conducted by flooding too many RREQ or data packets to the network which paralyzes not only the victim node but also the entire network. So, we investigate the quality of legitimate packet processing among the received packets at the node j. The legitimate packet processing at node j is calculated by the ratio of legitimate packets over received packets at the node j. This is defined as gain of legitimate packet processing in our scheme and can be presented as:

$$\Phi_j = \frac{Le_j}{Rcv_j}. \qquad (3)$$

Here, we denote Lej as the legitimate packets processed at the node j. We assume for simplicity that the amount of the received legitimate packets is the same in all neighboring nodes.

Using Equation (3), we can measure how the defense mechanism defends against the attack at each node.

Meanwhile, we can present Lej and Rcvj by the following equations because the node j receives packets from the multiple neighboring nodes i.

$$Le_j = \sum_{i=1}^{n} (Le_{ij}), \qquad (4)$$

where Leij is the number of legitimate packets at the node j from the node i, respectively.

If we denote αM, βM, γM, and δM as the number of received data, RREQ, RREP, and RERR packets respectively, which are used in the attack, we can rewrite (2) using the following equations:

$$\begin{aligned} Rcv_j = {} & (\alpha-\alpha^M)+\{[(\alpha-\alpha^M)+\alpha^M]-(\alpha-\alpha^M)\} \\ & +(\beta-\beta^M)+\{[(\beta-\beta^M)+\beta^M]-(\beta-\beta^M)\} \\ & +(\gamma-\gamma^M)+\{[(\gamma-\gamma^M)+\gamma^M]-(\gamma-\gamma^M)\} \\ & +(\delta-\delta^M)+\{[(\delta-\delta^M)+\delta^M]-(\delta-\delta^M)\} \end{aligned} \qquad (5)$$

Since (x - y) + y can be simplified to x, then we have,

$$\begin{aligned} Rcv_j = {} & \{(\alpha-\alpha^M)+\alpha^M\} \\ & +\{(\beta-\beta^M)+\beta^M\} \\ & +\{(\gamma-\gamma^M)+\gamma^M\} \\ & +\{(\delta-\delta^M)+\delta^M\} \end{aligned} \qquad (6)$$

Then, we can present Lej as:

$$\begin{aligned} Le_j = {} & (\alpha-\alpha^M)+(\beta-\beta^M)+(\gamma-\gamma^M) \\ & +(\delta-\delta^M) \end{aligned} \qquad (7)$$

Then, we apply (6) and (7) to (1) and (4), respectively. Hence, we can measure the ratio between processed legitimate packets and received packets by applying both (1) and (4) to (3).

The end-to-end packet delivery ratio of the legitimate packets (PDRL) is measured by the ratio between the received legitimate packets at the destination node (RL) and the transmitted legitimate packets at the source node (TL) in the time from ta to tz.

$$t\,z\,R \quad {}_L \quad \int_{t_a} \frac{}{T_L})dt$$

$$\underline{\Omega_\forall - \{R_\forall(1-R_L) + \mathrm{B} + \Gamma + \Delta\}}$$

$$PDR = (\,{}^{L}{}_{t\,z} \qquad (8)$$

$$= {}_{t}\int{}_{a}(\quad T^L \quad)dt$$

Here, Ω∀ is all received packets at the destination node in the measured time. R∀ is the received data packets at the destination node. We denote Β, Γ, and Δ as the number of received RREQ, RREP, and RERR packets at the destination node, respectively.

Then, we can improve PDRL by improving RL. RL can in turn be improved by improving the number of processed legitimate packets at each node using the following equation:

$$R_L = \Psi \times \sum_{j=1}^{N} (Le_j)\,, \qquad (9)$$

where Ψ is the proportional constant.

3. CATEGORIZATION OF MALICIOUS FLOODING ATTACKS

The attacker(s) may flood the victim node with garbage packets for clogging purposes. Attacker(s) may achieve this by either flooding nodes with redundant or random Route Request (RREQ) packets, data packets or both. The malicious flooding attack, either by a single attacker or by collaborative multiple attackers, can be categorized into the following possible cases:

Case 1: An attacker, pretending to be a source node, chooses to flood by generating excessive RREQ packets. Here, the attacker chooses to keep the same source address in all the RREQ packets as shown in Figure 1.

Malicious node Victim node or

(pretending as source) another malicious node

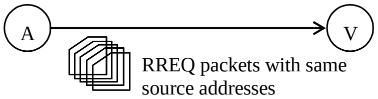


Fig. 1. Case 1: An attacker floods RREQ packets with redundant source address

Case 2: An attacker, again pretending to be the source node, chooses to flood by generating excessive RREQ packets with different source addresses, masquerading himself as shown in

Figure 2.

Malicious node Victim node or

(pretending as source) another malicious node

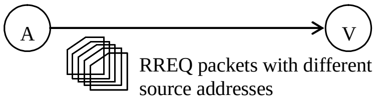


Fig. 2. Case 2: An attacker floods RREQ packets with different source addresses

Case 3: An attacker chooses to flood by generating excessive data packets instead of RREQ packets. The case is explained further in Figure 3.

Malicious node Victim node or

(pretending as source) another malicious node

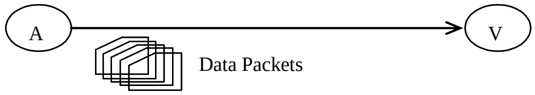


Fig. 3. Case 3: An attacker floods many data packet

Case 4-1: An attacker can conduct a collaborative attack along with another attacker. In this case, one of them attacks the victim node (or another malicious node) with RREQ packets with redundant source addresses, while his counterpart attacks the victim node (or another malicious node) with data packets as shown in Figure 4.

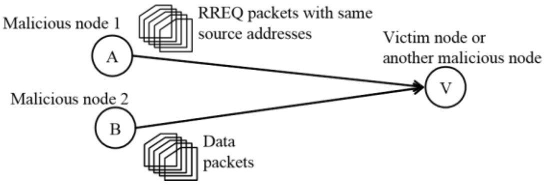


Fig. 4. Sub-case 4-1: A collaborative attack is conducted by combining case 1 and 3

Case 4-2: This is again a case of conducting collaborative attacks. In this case, one of them attacks the victim node (or another malicious node) with RREQ packets having different source addresses, while his counterpart attacks the victim node (or another malicious node) with data packets as shown in Figure 5.

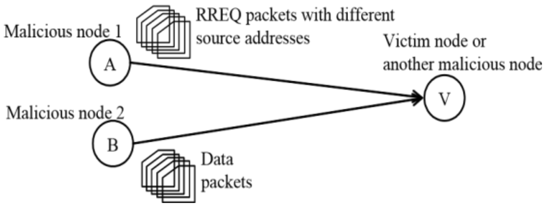


Fig. 5. Sub-case 4-2: A collaborative attack is conducted by combining case 2 and 3

The above mentioned attacks are conducted in order to clog and paralyze the victim node and eventually the complete network.

4. RELATED WORKS

Many researchers have studied scheduling algorithms in mobile ad hoc networks to serve received packets at a mobile node [10]. However, they do not guarantee the gain of legitimate packet processing when a node is victimized under malicious flooding attacks. Most of the scheduling algorithms give high priority to control packets over data packets and serve the data packets in a first-in-first-out order [10]. However, the RREQ flooding attackers flood tremendous amount of RREQ packets. Therefore, the previously researched schemes have not been able to effectively defend themselves against malicious flooding attacks.

The Flooding Attack Prevention (FAP) scheme [6] has addressed the malicious flooding attack and proposed a defense system, being the first to do so. They propose the neighbor suppression mechanism for the RREQ flooding attack and the path cut off mechanism for the data flooding attack. In the neighbor suppression mechanism, they determine the priority of neighboring nodes by inverse proportion to its frequency of originating RREQ packets. The threshold is determined by the maximum number of originating RREQ packets in a certain time period. If a neighboring node forwards more RREQ packets than the threshold, the receiving node simply denies them. However, the neighbor suppression mechanism does not check whether it receives the corresponding RREP packet or not. Hence, prevention from unreachable destination [11] is not possible. It is also vulnerable to the RREQ flooding attack conducted by the generation of many different source addresses. To prevent from the data flooding attack, the path cut off mechanism cuts the path off when the number of received data packets from one neighboring node exceeds the threshold. Hence, the path over which legitimate packets are transferred is also disconnected due to the suspected neighboring node.

Meanwhile, the Avoiding Mistaken Transmission Table (AMTT) scheme [12] suggests a defense system against the malicious flooding attack by utilizing an avoiding mistaken transmission table. The AMTT scheme requires huge memory space and considerable processing time for saving the packets at each node.

The Detect and Isolate Malicious Host (DIMH) [13] uses the topology information and the public key cryptosystem to detect colluding malicious nodes. However, it is very hard to utilize the key management and exchange in mobile ad hoc networks.

Hence, a defense mechanism against malicious flooding attacks by a single attacker or collaborative attackers is needed to be proposed.

5. PROPOSED SCHEME

Our scheme assumes AODV [7] for routing. The goal of our scheme is to provide a defense mechanism against collaborative flooding attacks. Our scheme is used whenever there is a need to defend against malicious flooding attacks.

We denote the size of a receiving buffer of a mobile node as Rbuffer. The corresponding sizes of control packets' buffer and the data packets' buffer, which make up the total receiving buffer, are denoted by Rbuffer(control) and Rbuffer(data), respectively. The size of above buffers is measured as the total number of corresponding packets existing in the buffer at a given time. The local density, ζ, of a node is defined as the number of neighboring nodes lying under its transmission range. With respect to local density, Rbuffer(control) and Rbuffer(data) can be defined as in (10) and (11).

$$R_{buffer}\,(control)=\zeta\times R_{buffer}\,, \qquad (10)$$

$$R_{buffer}\,(data)=(1-\zeta)\times R_{buffer}\,, \qquad (11)$$

where $0<\zeta\leq 1$.

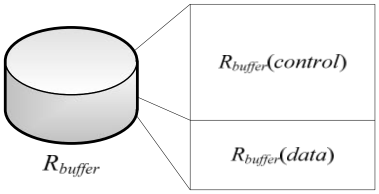
As can be seen from (10), if a node's local density is determined to be high (closer to 1), then the size of its Rbuffer(control) will increase.

The division of Rbuffer into Rbuffer(control) and Rbuffer(data), respectively is shown in Figure 6 and summarized in (12).

$$Rbuffer = \zeta\times Rbuffer\ (control)$$

$$+(1-\zeta)\times R_{buffer}\,(data) \tag{12}$$

Fig. 6. Division of Rbuffer



Our scheme is applied to any mobile node, in the network, whose Rcvj is larger than its Rbuffer. The algorithm of our scheme is as follows:

Step 1. If there exist any RERR packets in Rcvj, process the RERR packet and proceed to Step 2;

Step 2. If there exist any RREQ packets in Rcvj, check if the number of RREQ packets, β, is larger than Rbuffer(control). If the number of received RREQ packets is larger than Rbuffer(control), go to Step 3. Otherwise, go to Step 4;

Step 3. If any corresponding RREP packets are received, process rounded value of β/2 RREQ packets in receiving order. Then, go to Step 5. Otherwise, process the first received RREQ packet and go to Step 5;

Step 4. If any corresponding RREP packets are received, then process the RREQ packets without making any assumptions of an attack. Otherwise, randomly select rounded value of β/2 RREQ packets for processing. Go to Step 5;

Step 5. If there exist any data packets in Rcvj, check if the number of data packets are more than Rbuffer(data). If the number of received data packet is larger than Rbuffer(data), go to Step 6. Otherwise, go to Step 7;

Step 6. Prioritize the processing sequence according to Rcvj passing through the mobile node, in ascending order. Then, process rounded value of Rbuffer(data)/2 data packets in the order received. Go to Step 8;

Step 7. If data packets in Rcvj are smaller than Rbuffer(data), process rounded value of α/2 data packets in receiving order;

Step 8. Loop back to Step 1 and continue until connection is terminated.

The flow of procedure of our scheme is shown in Figure 7.

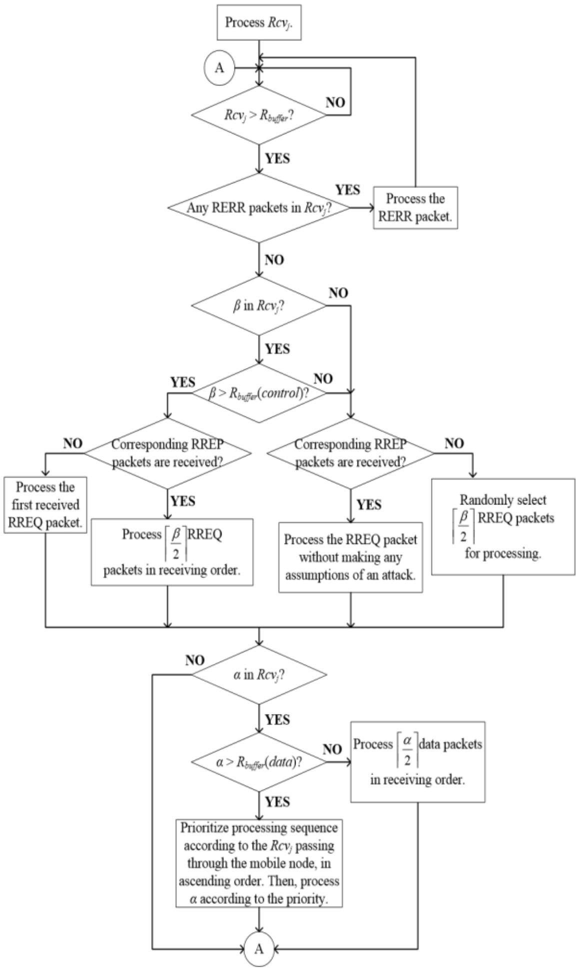

Process Rcv_j.
A
$Rcv_j > R_{buffer}$?
NO
YES
Any RERR packets in Rcv_j?
YES
Process the RERR packet.
NO
β in Rcv_j?
NO
YES
YES
$\beta > R_{buffer}(control)$?
NO
NO
Corresponding RREP packets are received?
Corresponding RREP packets are received?
NO
Process the first received RREQ packet.
YES
Process $\left\lceil \frac{\beta}{2} \right\rceil$ RREQ packets in receiving order.
YES
Process the RREQ packet without making any assumptions of an attack.
Randomly select $\left\lceil \frac{\beta}{2} \right\rceil$ RREQ packets for processing.
NO
α in Rcv_j?
YES
$\alpha > R_{buffer}(data)$?
NO
Process $\left\lceil \frac{\alpha}{2} \right\rceil$ data packets in receiving order.
YES
Prioritize processing sequence according to the Rcv_j passing through the mobile node, in ascending order. Then, process α according to the priority.
A

Fig. 7. Flowchart of Our Scheme

We evaluate the performance of the proposed scheme and compare it with the well-known FAP scheme [6] using ns-2 simulations [14].

7. CONCLUSION

In this paper, we propose a novel defense mechanism against collaborative flooding attacks. In order to do so, we have classified the various attack categories of possible malicious flooding attacks. The attacks can be conducted by collaboratively flooding RREQ packets, data packets, or both. We have also showed that the quality of legitimate packet processing at each node has improved when our scheme was used. Our scheme has also enhanced the end-to-end packet delivery ratio. We evaluated the performance of the proposed scheme and compared it with the FAP scheme. The simulation results show that our scheme is more robust than the FAP scheme. As our future work we will be considering the effect on packet delivery ratio with the increase in number of malicious nodes instead of the increase in amount of attack traffic. We also plan to conduct simulations in regard to application characteristics, in respect to percentage of legitimate packet delivery ratio, resulting in retransmission of data.

REFERENCES

[1] D. B. Johnson, D. A. Maltz, and J. Broch, DSR: The Dynamic Source Routing Protocol for Multi- Hop Wireless Ad Hoc Networks, Ad Hoc Networking, Chapter 5, Addison-Wesley, 2001, pp.139-172.

[2] Y.-C. Hu and A. Perrig, A Survey of Secure Wireless Ad Hoc Routing, *IEEE Security & Privacy*, Vol.2, No.3, 2004, pp.28-39.

[3] J. Li, D. Cordes, and J. Zhang, Power-Aware Routing Protocols in Ad Hoc wireless Networks, *IEEE Wireless Communications*, Vol.12, No.6, 2005, pp.69-81.

[4] M. Al-Shurman, S.-M. Yoo, and S. Park, Black Hole Attack in Mobile Ad Hoc Networks, the 42nd annual southeast regional conference, ACM Southeast Regional Conference, 2004, pp.96-97.

[5] Y.-C. Hu, A. Perrig, and D. B. Johnson, Wormhole attacks in wireless networks, *IEEE Journal on Selected Areas in Communications*, Vol.24, No.2, 2006, pp.370-380.

[6] P. Yi, Z. Dai, Y. Zhong, and S. Zhang, *Resisting Flooding Attacks in Ad Hoc Networks*, International Conference on Information Technology: Coding and Computing (ITCC 2005), Vol.2, 2005, pp.657662.

[7] C. E. Perkins and E. M. Royer, Ad hoc On-Demand Distance Vector Routing, the *2nd IEEE Workshop on Mobile Computing Systems and Applications (WMCSA '99*), 1999, pp.90-100.

[8] A. Khan, T. Suzuki, M. Kobayashi, W. Takita, and K. Yamazaki, Packet Size Based Routing for Stable Data Delivery in Mobile Ad-Hoc Networks, *IEICE Transactions on Communication*s, Vol.E91-B, No.7, 2008, pp.2244-2254.

[9] B. A. Forouzan, *Cryptography and Network Security*, McGraw-Hill, 2008.

[10] B.-G. Chun and M. Baker, Evaluation of Packet Scheduling Algorithms in Mobile Ad Hoc Networks, *ACM Mobile Computing and Communications Review (MC2R*), Vol.6, No.3, 2002, pp.36-49.

[11] R. Kumar, M. Misra, and A. K. Sarje, A Routing Protocol for Delay-Sensitive Applications in Mobile Ad Hoc Networks, *International Symposium on Ad Hoc and Ubiquitous Computing (ISAUHC '06),* 2006, pp.13-18.

[12] S. Li, Q. Liu, H. Chen, and M. Tan, "*A New Method to Resist Flooding Attacks in Ad Hoc Networks, International Conference on Wireless Communications", Networking and Mobile Computing 2006 (WiCOM 2006)*, 2006, pp.1-4.

[13] Z. Y. Xia and J. Wang, DIMH: "*A novel model to detect and isolate malicious hosts for mobile ad hoc network", Elsevier Computer Standards & Interfaces*, Vol.28, 2006, pp.660-669.

[14] The VINT Project, The network simulator- ns-2, available at http://www.isi.edu/nsnam/ns/.