Routing Misbehavior in Ad Hoc Network

Moitreyee Dasgupta
Guru Tegh Bahadur Inst. Of Tech,
G-8 Area, Rajouri Garden
New Delhi 110064, India

[1]S. Choudhury, [2]N. Chaki
University of Calcutta
92 A. P. C. Road, Kolkata, India

ABSTRACT
Rushing attack may cause more vulnerability in MANET as it can be used as a pre-requisite for launching some other types of Denial-of-Service attacks. Significant research efforts have been made towards increasing the survivability of MANET either by developing secure routing algorithms or by improving the robustness of MAC layer protocol in the presence of selfish or compromised nodes. Malicious nodes that disobey the standard, degrades the performance of well-behaved nodes significantly. However, little work has been done on quantifying the impact of these misbehaviors on the performance of ad hoc routing protocols. In this paper, we focus on the impact of rushing attack implemented by malicious nodes (MNs) on AODV routing protocol as an extension of our previous work. The Simulation study shows that the claim of our previous work stands true that AODV protocol fails completely in presence of rushing attack.

Keywords
Security, Attacks ad hoc routing, Rushing Attack, DoS attacks, MANET etc.

1. INTRODUCTION

In a Mobile Ad hoc Network, nodes work in co-operative basis based on their mutual trust. Every node works as a processor as well as packet forwarder in such an environment where no pre-existing infrastructure is available. Because of the node mobility, topology changes dynamically in MANET. Due to its basic ad-hoc nature, MANET is vulnerable to various kinds of security attacks that have already been extensively studied in [2] [5].

The ultimate goal of the security solutions for MANETs is to provide a framework covering authentication, confidentiality, integrity, anonymity to ensure availability of applications & services to mobile users. To achieve this goal of handling security issues, various aspects of MANET needs to be taken care of. This includes detecting and preventing viruses, worms, malicious codes for application layer; authentication and end-to-end secrecy for transport layer; protecting ad-hoc control and forwarding plane at the network layer; protecting wireless MAC protocol & handling link layer secrecy and finally preventing signal jamming for physical layer. The network layer security is the key with respect to performance of the network. Significant research efforts have been made towards increasing the survivability of MANET either by developing secure routing algorithms or by improving the robustness of MAC layer protocol in the presence of selfish or compromised nodes. Malicious nodes that disobey the standard, degrades the performance of well-behaved nodes significantly. For example, to gain the access of the forwarding path, malicious node may rush a packet by skipping some of the routing or MAC layer process [1]. Once gained the access, it may drop all packets or even selectively drop the packets to implement blackhole attack [3], or the node may channel all the packets to another compromised node to implement wormhole attack [4]. Again a malicious node is possible to correctly participate in route discovery phase but fails to correctly forward data packets. So, the security solution should also ensure that each node indeed forward the packet according to its routing tables. The rushing attack can be implemented in the network layer as well as in the MAC layer and as a result the entire network has to be compromised.

In this paper, we focus on the impacts of rushing attack implemented by malicious nodes (MNs) on ad hoc routing protocol. We consider rushing attack as it can also be used as a pre-requisite for launching some other types of Denial-of-Service attacks and can be implemented with no extra hardware. We belief that, the attack that can be implemented with the help of software manipulation are more vulnerable and hard to detect. We show that such attack can cause devastating effects on the network performance. We measure the performance of a popular on-demand ad hoc routing protocol AODV [6] under rushing attack.

Although, the research focus has been made towards the detection and handling of routing layer misbehavior [11] [6] [7] and several routing protocol have been proposed [9] [13] [14], none of them are resilient to DoS attacks [1] [3] [4]. Moreover, little work has been done on quantifying the impact of these misbehaviors on the performance of ad hoc routing protocols.

The rest of the paper is organized as follows. In Section 2, we present different types of DoS attacks. In Section 3, we briefly review the previous work. Section 4, we discussed the rushing attack model to show the possibility of the impact of rushing attack on the AODV and DSR routing mechanism. In Section 5, we compare the performance of AODV and DSR under Rushing attack via simulation. In Section 6, we conclude the paper and mention our future work.

2. RELATED WORK

2.1 Routing Misbehavior in MANET

DoS attacks are hard to detect and easy to implement by an attacker as no hardware is required to do so. These are considered to be the most vulnerable category of attacks for network layer thus needs more attention. Entire network may fail in presence of such an attack. Most common types of Denial-of-service attacks are categorized by the researchers [1] [2] [3] [4] discussed here in brief.

• Rushing Attack – In an on demand routing protocols, whenever source nodes flood the network with the Route Request packets in

order to discover the new routes to the destination, each intermediate forwarding node processes the first Route Request Packet from a particular node to suppress the duplicate forwarding. It discards the duplicate packets that arrive later. A rushing attacker by skipping some of the routing or MAC layer process can quickly forward these packets. As a result it gains the access of valid routes further data transmission. All most all the on-demand routing protocols are prone to the rushing attacks [1].

• Black hole Attack-In black hole attack [3], an attacker first introduce itself in the forwarding group (e.g., by implementing rushing attack), and then instead of forwarding the data packet to the proper destination, it simply drops all the packets it receive resulting a poor packet delivery ratio.

• Wormhole Attack-In this type of attack [4], after gaining access to the forwarding groups, an attacker simply forwards all the control packets received to a particular node. A tunnel is formed in the network where packet reaching one end of the tunnel broadcasted to the other end.

• Neighbor Attack- An intermediate node records its ID in the packet before forwarding it to the next node. In this type of attack, an attacker simply forwards the packet without recording its ID in the packet. This makes two nodes that are not within the communication range of each other believe that they are neighbors (i.e., one hop away of each other), resulting in a disrupted route.

• Jellyfish Attack- After gaining the access of the forwarding group, the attacker in this case, delayed the packet forwarding process for a certain period of time, resulting in a high end-to-end delay. Preventing rushing attacks will give a certain amount of protection against all the other attacks discussed above as for all of them getting access to the forwarding group is mandatory before introducing a specific type attack.

2.2 AODV and DSR

There are two major differences between AODV [6] and DSR [7]; DSR uses route cache while AODV uses source routing. But both the routing protocol is on-demand and best route is chosen by both of them using minimum hop-count. By route cache, the source maintains the path information it gets during the route discovery. Through a single RREQ packet, a source node will learn the routes to each intermediate node along the route to the destination node. The intermediate nodes can also learn the routing information on this route by caching learned routing information. Overhearing ongoing data transmission will also allow the node to learn more route information for future use. In DSR, the destination will reply to all the RREQ packets and send back a RREP packet for each received RREQ. Hence, the source node gets multiple paths to reach each destination and best path will be decided based on minimum hop-count. Again the aggressive use of route cache will allow DSR to find a current existing path without any new route discovery or choose an alternate path to the destination in the presence of route failure or link breakage due to mobility. This will save large route discovery overhead and effectively reduce the time delays. This route cache works fine with low traffic load and lower mobility; however it will face some problems when the routes in its cache become expired due to host mobility. Under these conditions, the source node will continue to use these expired routes without any notice Furthermore, the expired routes information could also be learned by other nodes and cause pollution to their route caches as a result throughput sacrifices. On the other hand, AODV uses timer based routing table entry to keep the route information fresh.

Again duplicate-suppression method [12] is used by both the routing protocols while forwarding the packet to avoid congestion and misuse of the valuable band-width of ad hoc network. The goal our simulation is to analyze how the routing misbehavior changes the performance of ad hoc routing protocol. Since both of them share similar on-demand characteristics, we would also like to compare their routing performance to see if there is difference showed by them.

2.3 Rushing Attack Model

We presented an attacking model for rushing attack in our previous work [12]. We assume all the nodes with equal transmission range and it selects the best path based on the hop count. For the similar hop-count it selects the best path based on the utility value which means the path with less congestion. Utility value is incremented by on every time the path is accessed by a team leader. This makes rushing attack implementation easy by the malicious node. If a attacker node can increases its transmission range to get access of the far off nodes or by removing the MAC layer delays that is required between receiving a request and forwarding it, or can quickly forward the packets by skipping some of the routing table operations, then the malicious node can increase the probability that the route that include the attacker will be discovered rather than other valid routes.

Currently proposed protocols choose to forward at most one RREQ message for each discovery, by default AODV and DSR consider the first packet to reach to a node for forwarding thus giving a clear indication of which packet will be chosen at each hop will be vulnerable to a variant of rushing attack modeled here.

2.4 S-HTMRP

Security remains as a concern in MANET. To achieve this goal, a security mechanism has been provided in this paper [12] for pure ad hoc networks which deals with both routing and packet forwarding. The proposed trust model ensures security against rushing attack, a variety of denial of services attack that may exist in the MANET. An alternative idea of implementing distributive security mechanism by computing trust levels from the inherent knowledge of the network has been proposed here, along with randomized packet forwarding mechanism to ensure security. Hop-count had been replaced by a parameter called weight which assigns a value for every path and the value will change dynamically to reflect reliability of that path. The routes calculated through this mechanism may not be optimal but certainly have an accurate measure of reliability in them.

3. TRUST MODEL & RUSHING ATTACK

In S-HTMRP [12], a security mechanism has been implemented by

- Replacing hop-count by an observation based trust value named weight and
- Traditional packet forwarding method has been replaced by Randomized Route Request Forwarding method.

In trust model, every node maintains a parameter called weight for all the neighbors. The parameter value changed dynamically based on node behavior. When the source will receive multiple RREP in response of a RREQ, the source calculates the reliability of the paths by calculating AVG of all the weight parameters for the forwarding nodes. Then best path is selected based on the average weight parameter rather than using hop-count.

Dynamic nature of the parameter ensures reliability of the selected path. Randomized message forwarding ensures that the paths with less delay are only slightly more likely to be selected than other paths. The idea is to gather n RREQ packet and choose any one arbitrarily for forwarding procedure. In case of not getting the desired number of RREQ packet, a node will wait for a source defined Γ period of time before randomly choosing and forwarding a packet. In each route discovery, the source will include the number of RREQ packet to gather before forwarding one along with the value (NO_DELAY) + Γ and adjust the parameter adaptively based on reply latency. NO_DELAY parameter is used by the AODV routing protocol while forwarding a packet in no attack scenario. Initially, the values can be set as n=1 and Γ = 0 such that the protocol can work without an extra overhead. The forwarding mechanism for RREQ is described with the help of a flowchart shown in Figure – 1.

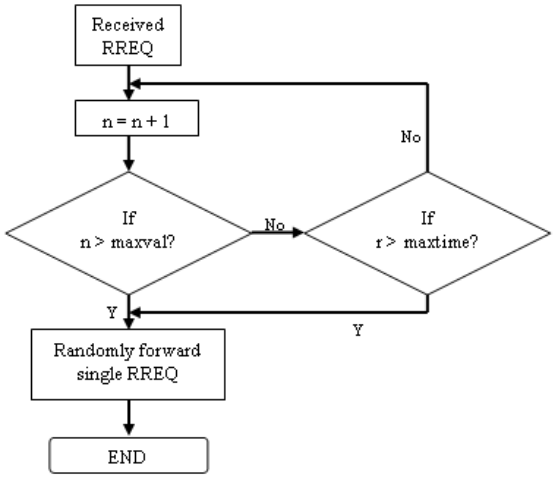

Figure – 1 RREQ forwarding mechanism

4. SIMULATION RESULTS

Simulations are made using NS-2 [8] simulation program that consists of the collection of all network protocols to simulate many of the existing network topologies. We simulate rushing attack by skipping some of the network layer responsibilities. Nodes were set to use 802.11 radios with 2 Mbps bandwidth and 250 meters nominal range. We considered only static scenario so link breakage due to mobility is zero. The simulated time was 100 seconds. We randomly placed 10 nodes within 800 X 800 meter area and the malicious node is in the center of the coordinates. TCP connections are established between nodes. The CBR (Constant Bit Rate) application generates constant packets through the TCP connection. Duration of the scenario is 10 seconds. The Packet Size is 1000 byte. The simulation scenario has been repeated for 0 and single malicious nodes for AODV and we also made a comparison of two very popular routing protocol AODV and DSR. DSR used route cache for the routes of same destination, while AODV every time uses route discovery process. As in our case link breakage due to mobility is negligible, Figure – 2 shows that DSR out performs AODV where we are averaging out the packet delivery ratio for the same source-destination pair.

We have also measured the network performance in presence of rushing attack, where after gaining access of the forwarding path, the compromised node drops all the packets. In Figure – 3 simulation results shows that the entire network fails in this scenario. Since there is a compromised node it is hard to find a new path. Even if there is a valid route, the RREP is difficult to arrive back to the source.

5. CONCLUSION AND FUTURE WORK

In this paper, we have considered rushing attack to model the impact of routing misbehavior on network layer performance as a significant extension of our previous work [12].

We see that the malicious node that disobey the standard, degrades the performance of the well-behaved nodes drastically, even the entire network may collapse, supports the claim made in our previous work. Although, the research focus has been made towards the detection and handling of routing layer misbehavior and several routing protocol have been proposed [9] [13] [14], none of them are resilient to DoS attacks [1] [3] [4].

We plan to extend our work by implementing rushing attacks for some of the very popular on-demand and even secure routing protocols and compare them and also implementing and evaluating the our proposed solution mechanism for the same.

6. REFERENCES:

[1] Y. C. Hu, A. Perrig and D. B. Johnson “Rushing Attacks and Defense in Wireless Ad Hoc Networks Routing Protocol”; Proceedings of ACM WiSe2003, Sep, 2003.

[2] Hoang Lan Nguyen and Uyen Trang Nguyen “Study of Different Types of Attacks on Multicast in Mobile Ad Hoc Networks”, Proceedings of the International Conference of Networking, International Conference on Systems and International Conference on Mobile Communication and Learning Technologies.

[3] Tamilselvan, L. Sankaranarayanan, V. “Prevention of Blackhole Attack in MANET”, Proceedings of the 2nd International Conference on Wireless Broadband and Ultra Wideband Communications, 2007. (AusWireless 2007).

[4] Yih-Chun Hu, Adrian Perrig and David B. Johnson, “Packet Lashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks” Proc. of the 22nd Conf. of the IEEE Computer and Communication Societies (INFOCOM), 2003.

[5] H. Yang, H Y. Luo, F Ye, S W. Lu and L Zhang “Security in mobile ad hoc networks: Challenges and solutions” Proceedings of IEEE Wireless Communications, pp 38-47, 2004.

[6] C. Perkings, E. Royer, “Ad Hoc On-Demand Distance Vector Routing,” 2nd IEEE Wksp. Mobile Comp. Sys and Apps., 1999.

[7] D. B. Johnson, D. A. Maltz and Yih-Chun Hu available at: http://tools.ietf.org/html/draft-ietf-manet-dsr-10

[8] “The network simulator - ns2,” http://www.isi.edu/nsnam/ns/.

[9] M. G. Zapata “Secure Ad hoc On-Demand Distance Vector (SAODV) Routing” Available at - http://personals.ac.upc.edu/guerrero/papers/draftguerrero-manet-saodv-06.txt

[10] M.Raja, J. P. Hubaux, I. Aad, “DOMINO: A System to Detect Greedy Behavior in IEEE 802.11 Hotspots” ACM MobiSys 2004, June 2004, Boston, USA.

[11] Rahman,, A. A., Hailes, "A distributed trust Model"(1997), Proceedings of the ACM New Security Paradigms Workshop, pp. 48-60, 1997.

[12] M. Dasgupta, S. Choudhury and N. Chaki, "Secure Hypercube based team multicast routing protocol (S-HTMRP)", Proceedings of First IEEE International Advanced Computing Conference (IACC'09), March 2009.

[13] K. Sanzgiri, B. Dahill, B.N. Levine, C. Shields, E. M. Belding-Royer "A Secure Routing Protocol for Ad Hoc Networks (ARAN)"

[14] Yih-Chun Hu, Adrian Perrig, David B. Johnson. "Ariadne: A secure On-Demand routing protocol for Ad hoc networks"; Proceedings of the 8th Annual International Conference on Mobile Computing and Networking, pp. 12-23, 2002.

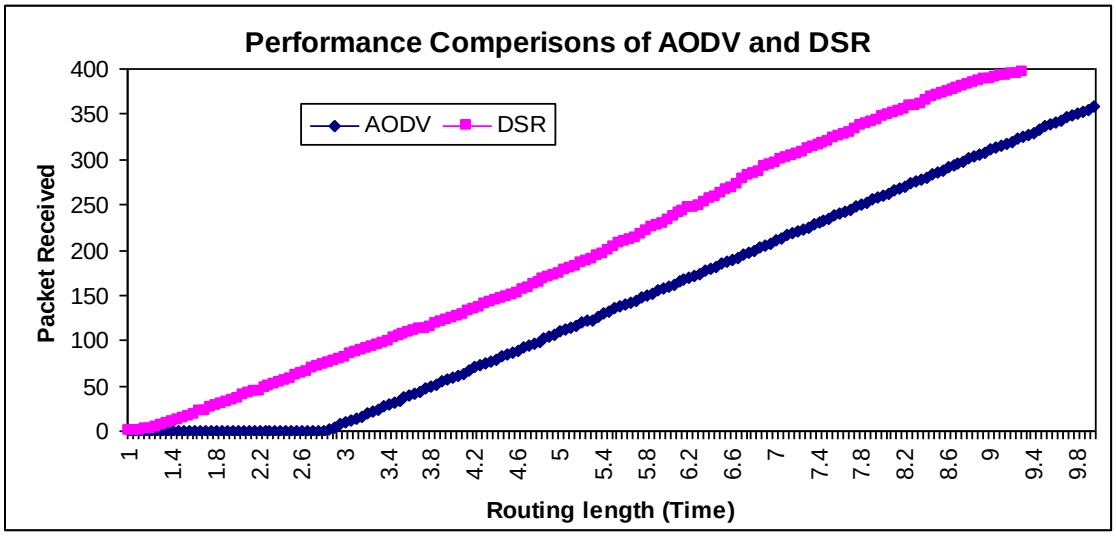

Figure – 2 Packet received Vs Time

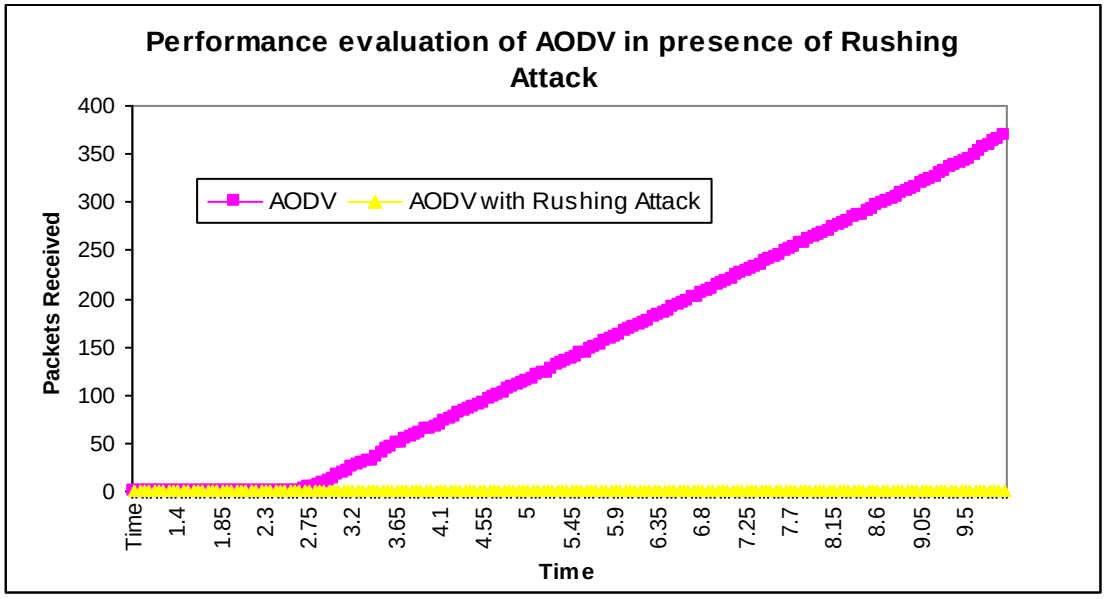

Figure – 3 Packet distributions with or without attacks