Effect of Selfish Attack and Prevention Scheme on TCP and UDP in MANET

Archana Shukla and Sanjay Sharma

Abstract
Mobile Ad-hoc networks are a collection of mobile hosts that communicate with each other without any infrastructure and centralized administration. Due to security vulnerabilities of the routing protocols, Mobile ad hoc networks may be unprotected against attacks by the malicious nodes. One of these attacks is the Selfish Attack against network integrity absorbing all routing packets as well as data packets in the network. Since the data packets do not reach the destination by that due to this attack, intense data loss will occur. The damage will be serious if malicious node in a network working as an attacker node absorbs all data packets and routing packets delivered through them. In this paper we proposed a simple IDS scheme against selfish attack and measure the performance of TCP and UDP packets after applying IDS. We simulated selfish node attacks in network simulator 2 (ns-2) and measured the packet loss in the presence of selfish node and in presence of Intrusion Detection System against Selfish node attack.. Our solution improved the 80% network performance in the presence of a selfish attack.

Keywords
MANET, Selfish node attack, AODV, ns-2.

1. INTRODUCTION

Mobile ad hoc networks are composed of autonomous nodes that are self- managed without any infrastructure. They usually have a dynamic topology such that nodes can easily join or leave the network at any time and they move around freely which gives them the name Mobile Ad hoc Networks or MANETs. They have many potential applications, especially in military and rescue operations such as connecting soldiers in the battle field or establishing a temporary network in place of one which collapsed after a disaster like an earthquake. In these networks, besides acting as a host, each node also acts as a router and forwards packets to the correct node in the network once a route is established. To support this connectivity nodes use routing protocols such as AODV (Ad hoc On-Demand Distance Vector) or DSR (Dynamic Source Routing). Mobile ad-hoc networks are usually susceptible to different security threats and selfish attack is one of these. In Selfish attack, a malicious node which absorbs and drops all data packets and routing packets makes use of the vulnerabilities of the on demand route discovery protocols, such as AODV.

In the route discovery process of AODV protocol, intermediate nodes are responsible to connect a fresh path to the destination, sending discovery packets to the neighbor nodes. Malicious node abuse this process and they immediately respond to the source node with false information as though they have a fresh enough path to the destination. Therefore source node sends its data packets via this malicious node assuming it is a true path.

Selfish node behavior may also be due to damaged nodes dropping packets unintentionally. In any case, the end result of the presence of a selfish node in the network is lost packets (both routing as well as data). In our study, we simulated selfish node attacks in wireless ad hoc networks and evaluated their effects on the network performance. We made our simulations using ns-2 (network simulator version 2.31). Having implemented a new routing protocol which simulates the selfish node behavior in ns-2, we performed tests on different topologies to compare the network performance with and without selfish nodes in the network.

The paper organization is as follows: section 2 describes the AODV protocol and selfish attacks are described in section 3. Related works are described in section 4 and the Proposed solution is described in section 5. Network simulation results are presented in section 6 followed by conclusions in section 7.

2. AODV Routing Protocol

Ad Hoc On-Demand Vector Routing (AODV) protocol is a reactive routing protocol for ad hoc and mobile networks that maintain routes only between nodes which need to communicate. The AODV routing protocol is the enhancement of DSDV protocol. AODV [1,2] is an improvement on DSDV because it typically minimizes the number of required broadcasts by creating routes on an on-demand basis, as opposed to maintaining a complete list of routes as in the DSDV algorithm. The authors of AODV classify it as a pure on-demand route gaining scheme, as nodes that are not on a selected path do not maintain routing information. That means, the routing messages do not contain information about the whole route path, but only about the source and the destination. Therefore, routing messages do not have an increasing size. It uses destination sequence numbers to specify how fresh a route is (in relation to another), which is used to grant loop freedom. Fig.1 showing the routing procedure of AODV routing protocol.

Manuscript received August 5, 2013
Manuscript revised August 20, 2013

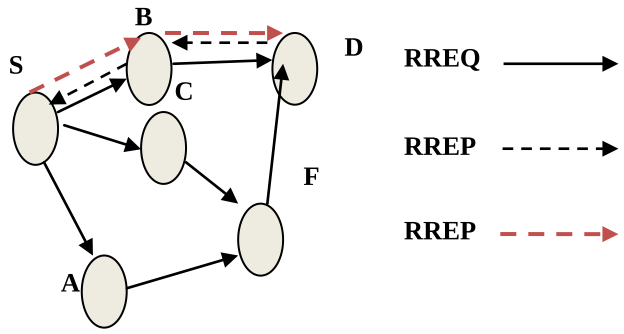

Fig. 1 AODV connection establishment process.

Whenever a node S needs to send a packet to a destination for which it has no route (i.e., a valid route entry for the destination whose associated sequence number is at least as great as the ones contained in any RREQ that the node has received for that destination D) it broadcasts a route request (RREQ) message to its neighbors. Each node that receives the broadcast sets up a reverse route towards the originator of the RREQ (unless it has a 'fresher' one).When the intended destination (or an intermediate node that has a route to the destination) receives the RREQ, it replies by sending a Route Reply (RREP). It is important to note that the only mutable information in a RREQ and in a RREP is the hop count (which is being monotonically increased at each hop). The RREP travels back to the originator of the RREQ (unicast). At each intermediate node, a route to the destination is set (again, unless the node has a 'fresher' route than the one specified in the RREP). In the case that the RREQ is replied to by an intermediate node (and if the RREQ had set this option), the intermediate node also sends a RREP to the destination. In this way, it can be granted that the route path is being set up bi-directionally. In the case that a node receives a new route and then fresh route will be created according to shortest path without any condition. The source node starts sending the data packet to the destination node through the neighboring node that first responded with an RREP. The AODV protocol is susceptible to the well-known selfish node attack.

3. Selfish node Attack

Routing protocols are exposed to a variety of attacks. Selfish node attack is one such attack in which a malicious node doing a routing misbehavior in the route discovery packets of the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept [3,4]. This attacks aims at modifying the routing protocol so that traffic flows through a specific node controlled by the attackers. During the route discovery process, the source node sends route discovery packets to the intermediate nodes to find fresh path to the intended destination. Malicious nodes respond immediately to the source node as these nodes do not refer the routing table and drop all the routing packets. The source node assumes that the route discovery process is complete, ignores other route reply messages from other nodes and selects the path through the malicious node to route the data packets. The malicious nodes do this by assigning a high sequence number to the reply packet. The attackers now drop the received messages instead of relaying them as the protocol requires. Malicious nodes take over all routes by attacking all route request messages. Therefore the quantity of routing information available to other nodes is reduced. The malicious nodes are called selfish node or nodes. The attack can be proficient either selectively or in bulk. Selective dropping means dropping packets for a specified destination or a packet every seconds or a packet every packets or a randomly selected portion of packets. Selfish attack results in dropping all packets. Both result in degradation in the performance of the network. Attacker nodes receive a request message, and send reply message to the source node. So that the source node considers the message has arrived and the communication has been successfully performed. In fact, the message did not reach the destination node.

In figure 1, source node S wants to send data packets to a destination node D in the network. Node M is a malicious node which acts as a Selfish node. The attacker replies with false reply RREP having higher modified sequence number. So, data communication initiates from S towards M instead of D.

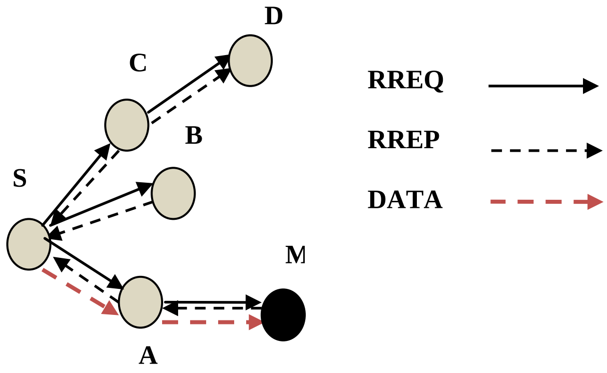

Fig. 2 Routing in presence of Selfish node attack.

4. Related Work

There are basically two approaches to secure MANET:

(1) Securing Ad hoc Routing and
(2) Intrusion Detection

Secure Routing

The Secure Efficient Ad hoc Distance vector routing protocol (SEAD) [5] employs the use of hash chains to validate hop counts and sequence numbers in DSDV. Another secure routing protocol, Ariadne [6] assumes the existence of a shared secret key between two nodes based on DSR (reactive) routing protocol. The Authenticated Routing for Ad hoc networks (ARAN) is a standalone protocol that uses cryptographic public-key certificates in order to achieve the security goals [9]. Security-Aware Ad hoc Routing (SAR) uses security attributes such as trust values and relationships [10]. The computation overhead involved in the above mentioned protocols is awful and often suffer from scalability problems. As a preventive measure, the packets are carefully signed, but an attacker can simply drop the packet passing through it, therefore, secure routing cannot resist such internal attacks. So our solution provides a reactive scheme that triggers an action to protect the network from future attacks launched by this malicious node.

Intrusion Detection System

Zhang and Lee [11] present an intrusion detection technique for wireless ad hoc networks that uses cooperative statistical anomaly detection techniques. The use of anomaly based detection techniques results in too many number of false positives. Stamouli proposes architecture for Real-Time Intrusion Detection for Ad hoc Networks (RIDAN) [7]. The detection process relies on a state-based misuse detection system. Therefore, each node requires extra processing power and sensing capabilities. In [12], the method requires the intermediate node to send Route Confirmation Request (CREQ) to next hop towards the destination. This operation can increase the routing overhead resulting in performance degradation. In [13], source node verifies the authenticity of node that initiates RREP by finding more than one route to the destination, so that it can recognize the safe route to destination. This method can cause the routing delay, since a node has to wait for RREP packet to arrive from more than two nodes. In [14], the feature used is destination sequence number, which reflects the trend of updating the threshold and hence reflecting the adaptively change in network environment. Therefore, a method that can prevent the attack without increasing routing overhead and delay is required. Certificate chaining is a self organized PKI authentication by a chain of nodes without the use of a trusted third party [15]. This technique is for securing ODMRP.Here authentication is represented as a set of digital certificates that form a chain. Each node in the network has identical roles and responsibilities thereby achieving maximum level of node participation. Every node in the network can issue certificates to every other node within the radio communication range.

5. Proposed Solution Against Selfish node Attack

Every packet in MANETs has a unique sequence number. This number is an increasing value, i.e., the next packet must have higher value that the current packet sequence number. The node in regular routing protocols keeps the last packet sequence number that it has received and uses it to check if the received packet was received before from the same originating source or not.

In Intrusion detection system (IDS) , every node needs to have two additional small-sized tables; one to keep last-packet-sequence-numbers for the last packet sent to every node and the other to keep last-packet-sequence-numbers for the last packet received from every node (from node through node). These tables are updated when any packet arrived or transmitted. The sender broadcasts the RREQ packet to its neighbors. Once this RREQ reach the destination, it will initiate a RREP to the source, and this RREP will contain the last-packet-sequence-numbers received from this source. When an intermediate node has a route to the destination and receives this RREQ, it will reply to the sender with a RREP contains the last- packet-sequence-numbers received from the source by this intermediate node. This solution provides a fast and reliable way to identify the suspicious reply. No overhead will be added to the channel because the sequence number itself is included in every packet in the base protocol.

6. Simulation Environment

The detailed simulation model is based on network simulator-2 (ver-2.34) [8], is used in the evaluation. The NS instructions can be used to define the topology structure of the network and the motion mode of the nodes, to configure the service source and the receiver to create the statistical data track file and so on.

A. Simulation Parameters for Case Study.

TABLE I Simulation Parameters for Case Study

Number of nodes	30
Selfish node	1
Dimension of simulated area	800×600
Routing Protocol	AODV
Simulation time (seconds)	100
Transmission Range	250m
Traffic type	CBR
Packet size (bytes)	512
Number of traffic connections (TCP or UDP)	20
Maximum Speed (m/s)	30

In our scenario we take 30 nodes in which nodes 1-27 are simple nodes, and node 28 is a malicious nodes or Selfish node . The simulation is done using ns-2, to analyze the performance of the network by varying the nodes mobility. The evaluated performances are given below. We are taking the following parameters for case study shown in table 1.

B. *Performance Metrics*

In this paper we focus on evaluating the protocols under Selfish node or malicious nodes attack and measure the network performance after applying intrusion detection system with following criteria [2, 3, 8, 9, and 13].

1) *Packet Delivery Fraction (PDF): The ratio of data the delivered to the destination to the data send out by source.*

2) *End to End Delay*: The difference in the time it takes for a sent packet to reach the destination.

3) *Throughput:* Numbers of packets send or received in per unit of time. The higher value of throughput is performance is better.

4) *Normalized routing overhead:* This is the ratio of routing-related transmissions (RREQ, RREP, RERR etc) to data transmissions in a simulation.

5) *Packet lots:* Total number of packets dropped during simulation.

C. *Results*

In this section we present a set of simulation experiments to evaluate this protocol by comparing with the original AODV [5].

Scenario of Selfish Node and IDS Node: In this figure we represent the nam scenario of thirty nodes in which node 28 are the Selfish node node and 29 are IDS node and rest of them are normal nodes. All the nodes are mobile nodes first they sensing the neighbor for route establishment and after that starting data transferring.

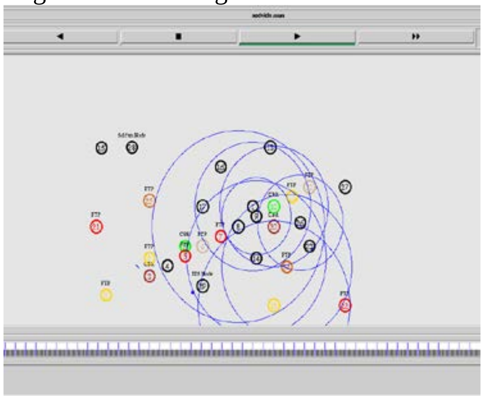

Fig. 3 A nam scenario of Selfish node and IDS node.

Analysis of UDP packets: Here in attack case negligible data packets are reached to destination about 300 packets rest of them are dropped. But after applying IDS on Selfish node attack we observe that about 90% of data packets are received. In case of UDP packets the acknowledgement are not received then difficult to recover data. Here we notice that after applying IDS packet receiving increases and dropping of packets decreases.

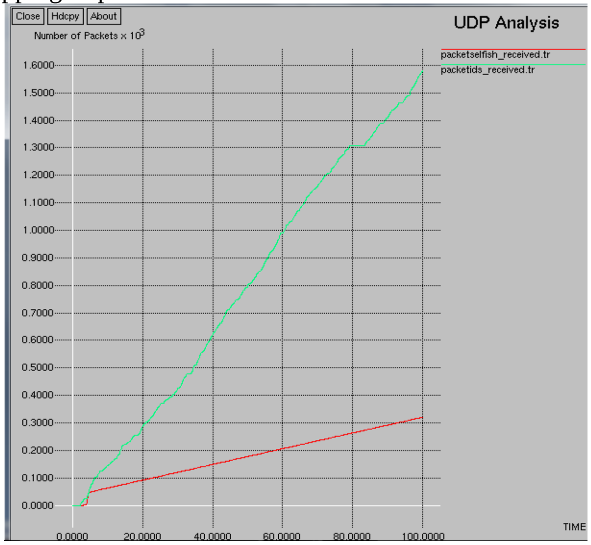

Fig.4 UDP Analysis in Case of Attack and IDS

Analysis of TCP Congection Window: At the time of attack the TCP packets receiving rate are negligible. But after applying IDS receiving rate are increases. In case of TCP packets having a field of acknoledgement then if the sender not receiving the reply of successful delivery, it stops their packets transmission. So, here packet lost posibility are not more.

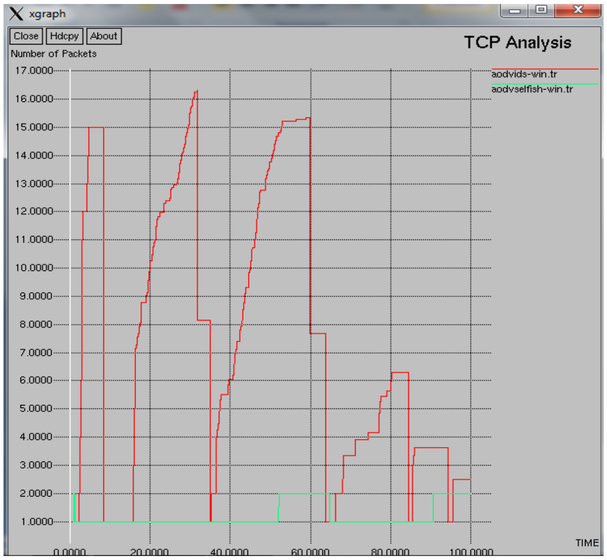

Fig.5 TCP analysis of nodes in case of attack and IDS

7. Conclusion and Future Work

Finally after visualize the results, it can be concluded that the Selfish node effect on the UDP packets and TCP congestion window. Effect on packet loss is clearly visualized in UDP packets. As malicious node is the main security threat that effect the performance of the AODV routing protocol. Its detection is the main matter of concern. Therefore the proposed IDS scheme work will be excellent to detect and defense the network from Selfish node attack.

In Future we also detect the effect of selfish attack in performance matrices and also Selfish node for AODV can be implemented in real life scenario and its analysis can be compared with the analysis results.

References

[1] Hao Yang, Haiyun Luo. Fan Ye, Songwu Lu, and Lixia Zhang. "Security in mobile ad hoc networks: Challenges and solutions". IEEE Wireless Communications , February 2004.

[2] Shree Murthy and J. J. Garcia-Luna-Aceves. "An Efficient Routing Protocol for Wireless Networks". Mobile Networks and Applications, 1(2):183–197, 1996.

[3] Charles E. Perkins and Elizabeth M. Royer. "Ad-Hoc On-Demand Distance Vector Routing". In Proceedings of the Second IEEE Workshop on Mobile Computing Systems and Applications (WMCSA'99), pages 90–100, February 1999.

[4] C. Perkins, E. B. Royer, S. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing - Internet Draft", RFC 3561, IETF Network Working Group, July 2003.

[5] Y.-C. Hu, D.B. Johnson, and A. Perrig, "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad hoc Networks," Proc. 4th IEEE Workshop on Mobile Computing Systems and Applications, Callicoon, NY, June2002, pp. 3-13.

[6] Y.-C. Hu, A. Perrig, and D.B. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad hoc Networks," Proc.8th ACM Int'l. Conf. Mobile Computing and Networking (Mobicom'02), Atlanta, Georgia, September 2002, pp. 12-23.

[7] Ioanna Stamouli, "Real-time Intrusion Detection for Ad hoc Networks" Master's thesis, University of Dublin, Septermber 2003.

[8] www.cs.cmu.se/education/examina/Rapporter/ClaesGahlin.pdf.

[9] Kimaya Sanzgiti, Bridget Dahill, Brian Neil Levine, Clay shields, Elizabeth M, Belding-Royer, "A secure Routing Protocol for Ad hoc networks In Proceedings of the 10thIEEE International Conference on Network Protocols (ICNP' 02), 2002.

[10] S. Yi, P. Naldurg, and R. Kravets, "Security-Aware Ad hoc Routing for Wireless Networks," Proc. 2nd ACM Symp.Mobile Ad hoc Networking and Computing (Mobihoc'01), Long Beach, CA, October 2001, pp. 299-302.

[11] Y. Zhang and W. Lee, "Intrusion detection in wireless ad – hoc networks," 6th annual international Mobile computingand networking Conference Proceedings, 2000.

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

[13] M. A. Shurman, S. M. Yoo, and S. Park, "Selfish node attack in wireless ad hoc networks," in ACM 42nd Southeast Conference (ACMSE'04), pp. 96-97, Apr. 2004.

[14] E. A .Mary Anita, V. Vasudevan ," Selfish node Attack Prevention in Multicast Routing Protocols for Mobile Ad hoc networks using Certificate Chaining", International Journal of Computer Applications, Volume 1 – No. 12, 2010.

[15] Monika Roopak , Dr. Bvr Reddy, "Performance Analysis of Aodv Protocol under Selfish node Attack", International Journal of Scientific & Engineering Research, Volume 2, Issue 8, 2011.