Security Analysis of TORA Routing Protocol

Vee Liem Chee and Wei Chuen Yau

Faculty of Engineering, Multimedia University,
Jalan Multimedia, 63100 Cyberjaya, Selangor Darul Ehsan, Malaysia
cheevl@yahoo.com, wcyau@mmu.edu.my

Abstract. In this paper, we present security analysis on Temporally-Ordered Routing Algorithm (TORA) routing protocol. We first identify three attack goals, namely route disruption, route invasion and resource consumption. Then, we study on how to achieve these attack goals through misuses of routing messages. The analysis shows that three misuse actions on the routing messages, including drop, modify and forward, and active forge, enable the malicious attacker to conduct real time attacks on TORA protocol. We demonstrate the attacks using NS-2 software and then analyze the simulation results. The simulation results verify our analysis and we observe that through certain misuses, an inside attacker can degrade the network performance, disrupting the route creation process and consume scarce network resource.

Keywords: Ad Hoc Networks, TORA, Routing Protocols.

1 Introduction

Mobile Ad Hoc Network (MANET) is a collection of wireless hosts that can be rapidly deployed as a multi hop packet radio network without the aid of any established infrastructure or centralized administration [1]. Each of the wireless nodes cooperates by forwarding packets for each other to allow them to communicate beyond direct transmission range. Applications such as disaster relief, military applications, and emergency search and rescue significantly benefit from ad hoc networking due to its infrastructureless situations. A routing protocol is used to discover routes between nodes in order to facilitate the communications within the network. Primary purpose for ad hoc routing protocol is to establish truthful and efficient route between a pair of nodes so that data packets can be delivered in a timely manner with minimum resource in terms of routing overhead and bandwidth consumption.

However, the original MANET does not consider much in the communication security. It assumes all wireless nodes are legitimate and trustable. In reality, adversary nodes exist and make MANET extremely vulnerable to be compromised. For instance, malicious nodes can perform the attack in network through disseminate false routing information or drop the packets instead of forwarding it out. Realizing the seriousness of this situation, substantial research and efforts have been made to protect the routing information from both the internal attackers which try to compromise nodes within the network and external attackers which try to inject

O. Gervasi and M. Gavrilova (Eds.): ICCSA 2007, LNCS 4706, Part II, pp. 975–986, 2007.

forged routing information to the network. A lot of effort has been put into researches to strengthen the ad hoc security and to protect the network, for instance, routing information encryption, comprehensive public key infrastructure and user identification.

This research is inspired by the work in [4]. In [4], Ning and Sun analyzed systematically how inside attackers misuse the AODV routing protocol. Their work shows that various attack goals can be achieved by manipulating different types of routing messages of AODV. We extend their work by applying the analysis method to another type of on demand routing protocol, namely Temporally-Ordered Routing Algorithm (TORA) [9], as the security issues of this routing protocol is not discussed widely. We also conduct some simulations to verify the attacks on TORA.

The remainder of this paper is organized as follows: Section 2 examines the basic functional operation of TORA protocol. Section 3 analyses the misuses on TORA routing messages. Section 4 presents the simulation results using NS-2. Section 5 discusses related work in security of MANETs. Section 6 concludes the paper and presents future research direction.

2 Description of TORA

The Temporally-Ordered Routing Algorithm (TORA) is an adaptive routing protocol for multihop networks [9]. The protocol is essentially an optimized hybrid of the Gafni Bertsekas (GB) protocol and the Lightweight Mobile Routing (LMR) protocol [8]. It provides loop freedom, multiple routes and minimal communication overhead via localization of algorithmic reaction to topological changes even in highly dynamic environments. It also supports a mixture of reactive and proactive routing. Reactive routing is beneficial in dynamic networks with relatively light traffic patterns. While proactive routing is desirable when routing is consistently or frequently required.

TORA maintains routing state on a per-destination basis. As it assigns a height value based on the direction of a link towards the destination, the flow of the traffic is always directed from a higher source node to a lower destination node. This mechanism ensures that a node can only forward packets downstream but not upstream. Each node i is associated with a height H_i represented by a quintuple (τ_i, oid_i, r_i, δ_i, i). The first three values in the quintuple represent the reference level while the remaining two represent the change with respect to the reference level. Table 1 summarizes the description of each height metrics.

Table 1. Descriptions of height metrics

Height Metrics	Descriptions
τ	Logical time of a link failure
oid	Unique ID of the node that defined the new level
r	Reflection Indicator bit
δ	Propagation ordering parameter
i	Unique ID of the node

The on-demand TORA protocol performs three basic functions: creating routes, maintaining routes and erasing routes. These three functions are accomplished using the following control packets: QUERY (QRY), UPDATE (UPD), and CLEAR (CLR).

The route creation function is initiated if a node without any directed links requires a route to the destination. The process is accomplished using query-and-reply mechanism by exchanging QRY and UPD packets between the routers. At the end of the route creation process, a directed acyclic graph (DAG) is created with the destination as the root (i.e., the destination is the only node without downstream links).

Route maintenance is performed when there is any topological change in the network. This is to ensure that routes to the destination can be re-established within a finite time. In this process, each node (except the destination) that has no downstream links modifies its height based on one of five possible cases. For example, when a node has no downstream links due to a link failure, the node reacts by defining a new reference level.

When a node detects a partition, links in the portion of the partitioned network are marked as undirected and all invalid routes are erased. During this erasing routes process, the node sets its heights and the height entry of each neighbor to NULL and broadcast CLR packets.

3 Security Analysis

3.1 Analysis Scheme

The security deficiencies of TORA make it vulnerable to various malicious attacks. In this paper, we exploit some attacks on TORA to expose the potential security flaws in the protocol. To facilitate the analysis, we refer the work in [4], and identify three misuse goals that an inside attackers may want to accomplish. The followings are these misuse goals:

- *Route Disruption (RD).* Route Disruption means either deterring the discovery of new route from being established or breaking down an existing route.
- *Route Invasion (RI).* Route invasion is achieved by adding an inside attacker itself into a route between two endpoints of a communication channel.
- *Resource Consumption (RC).* Resource consumption is achieved by consuming the communication bandwidth of the network or wasting system resources of a node, such as its battery power or CPU usage.

We also examine how attackers manipulate routing messages (i.e. Query, Update and Clear) to achieve the abovementioned attack goals. Three manipulation actions [4] is listed as follows:

- *Drop (DR).* The attacker discards the received routing message.
- *Modify and Forward (MF).* Upon receiving a routing message, the attacker modifies one or several fields in the routing message with incorrect information and then forwards it to its neighbor(s).
- *Active Forge (AF).* The attacker actively sends a faked routing message.

Throughout this paper, we present each misuse with a name in the form of *RoutingMessageType_Action_Goal*. This means that an inside attacker applies the "*Action*" to a routing message of type "*RoutingMessageType*" to achieve the "*Goal*". For example, an inside attacker modifies and forwards (MF) a received Update (UPD) routing message to achieve the goal of route disruption (RD) is represented in the form of UPD_MF_RD.

3.2 Misuses of Query (QRY) Messages

In this section, we present four misuses of Query messages, namely QRY_DR_RD, QRY_MF_RD, QRY_MF_RC, and QRY_AF_RC.

QRY_DR_RD. If an inside attacker is the only node that connects the two parts of the network, it can separate the nodes in these two parts by dropping the received QRY message. In this case, all the in-transit QRY packets are discarded before reaching the destination. Therefore, no QRY message is able to reach the destination to complete the route discovery process. In another case, the attacker node may also choose to selectively drop QRY messages destined to a specific destination. This node is called selfish node. However, this misuse can only last for a short period, as the source node will initiate another QRY packet to find the route to the destination. Therefore, the malicious attacker has to conduct QRY_DR_RD attacks repeatedly in order to achieve the misuse goal.

QRY_MF_RD. In this misuse, the inside attacker attempts to prevent a path from being establish by modifying and forwarding the QRY message it received. Several possible modifications are listed as follows:

- Change the value of Type in QRY packet to any value other than 1.
- Substitute the IP address with another IP address or a non-existent IP address.

QRY messages become invalid after malicious modifications. This disrupts the requested route from being established. As a result, no UPD message is generated and the route creation is incomplete. Even if a route is discovered (i.e. the attacker replace the IP address with a different IP address that exists in the network), the route is treated invalid by the source node as the destination IP address in the UPD packet that propagates back is not the same as requested. However, the attack does not work if there exists other routes between two given nodes. QRY packet may still propagate to the destination using other alternative path through the uncompromised node.

Fig. 1 shows an example of successful QRY_MF_RD attack. As the malicious node *X* is the only node that connects two parts of the ad hoc network, the original QRY message from the source must pass through this attacker *X* before it can reach the destination node. If the attacker *X* modifies the received QRY and forwards to its neighbor nodes *B* and *C*, destination node *E* will receive an invalid QRY message that cause the route discovery process to fail. While in Fig. 2, the route discovery is not affected even if the attacker *X* modifies the QRY message. This is because another valid QRY message may propagate to the destination via the alternate path provided by node *B*.

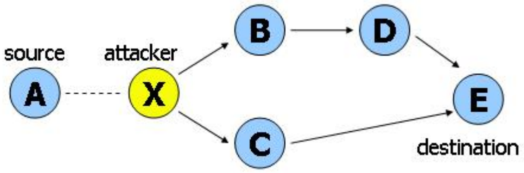

Fig. 1. A successful QRY_MF_RD attack

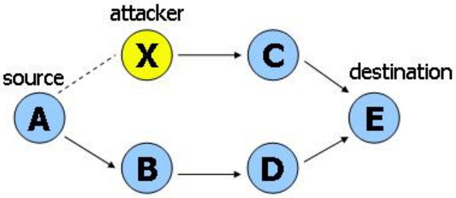

Fig. 2. An unsuccessful attack situation

QRY_MF_RC. In this attack, the attacker modifies the abovementioned fields of TORA packets. After its neighbor receives this invalid packet, battery power as well as channel bandwidth are wasted to retransmit it out. If the source node fails to create the path it needed, it will initiate another round of discovery. The same attack technique is repeated again by the attacker. However, it is difficult to consume significant resources with this attack.

QRY_AF_RC. The attacker actively forges and sends extraneous QRY packets to the network. This results consumptions of neighbor nodes' battery supply or causes network congestion. The attacks are required to perform continuously in order to create a practical impact on the network. However, the routing mechanism of TORA prevents retransmission of QRY packet to the same destination repeatedly as the Route-Requested flag is set in the protocol. Therefore, the attacker has to flood the network with different IP addresses in every round of attacks.

3.3 Misuses of Update (UPD) Messages

In this section, we present three misuses of Update messages, namely UPD_DR_RD, UPD_MF_RD, and UPD_AF_RI.

UPD_DR_RD. In a route creation process, a UPD message may be dropped by an inside attacker and this results the source node does not receive any UPD for completing the route creation process. Hence, the source node has to initiate another round of route creation to find its required route. However, this attack will not work if the source node has multiple neighbors and not all of them are malicious. In other words, the prerequisite condition is the attacker node must be the only node that connects the two parts of the network. Thus, this misuse has a limited impact.

UPD_MF_RD. During a route creation process, the attacker node can prevent a path from being established by modifying the in-transit UPD packet as follows:

- Change the packet type.
- Substitute destination IP address and IP mask.
- Change the reference level value.
- Replace the originator ID value.

The modifications on the UPD message cause the source node to receive an invalid or no UPD at all, thus resulting that specific round of route creation to end prematurely. However, if there exists another route from the source to the destination (As shown in Fig. 2), the source node is still able to receive a legitimate UPD message from there. The misuse does not work in that case.

UPD_AF_RI. In this attack, the malicious node collects information about the network topology by analyzing sniffed routing packet. As soon as it detects a route is being requested (i.e. malicious node receives an incoming QRY), it reacts by actively forging a UPD message, claiming it has a trusted route to the destination being requested. As shown in Fig. 3, the attacker sets the reference level value (H.delta) of the faked UPD to 1, and propagates back to the node where it just received the QRY message. This sender node will then assume that the next hop to the destination is the attacker node. In addition, the attacker also generates another QRY message to its neighbors (except to the node where it received the original QRY message), to request the route to the same destination. Therefore another path from attacker node to destination is created here. As a result, the attacker can successfully be a part of the route from the source to the destination (As shown in Fig. 4).

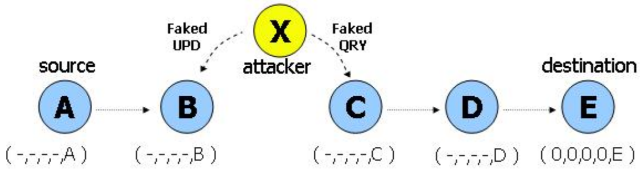

Fig. 3. The attacker *X* forges faked UPD and QRY in UPD_AF_RI

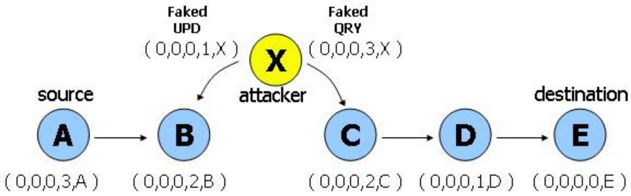

Fig. 4. Attacker *X* successfully invade the route

3.4 Misuses of Clear (CLR) Messages

In this section, we present two misuses of CLR messages, namely CLR_DR_RD and CLR_AF_RD.

CLR_DR_RD. An inside attacker who drops the received CLR can prevent upstream nodes in the network from receiving any CLR message. Thus, these upstream nodes do not know about the link failure and continue to send data packets through the broken route. But the routing packets will eventually be dropped due to the broken link. The node that drops these routing packets executes route maintenance and generates another CLR message. Therefore, this attack will only work if an inside attacker is the only neighbor in the precursor list of node that sends a CLR message.

CLR_AF_RD. This attack allows the attacker to create a fake link failure with respect to its downstream node, thus disable the route from the upstream to the downstream node. Prior to this attack, the attacker needs to perform a route maintenance process by actively forging a UPD message that defines a new reference level. Fig. 5 shows an example of this attack. The attacker node *X* pretends that a link failure to its downstream victim *D* (which in fact the link between node *X* and node *D*

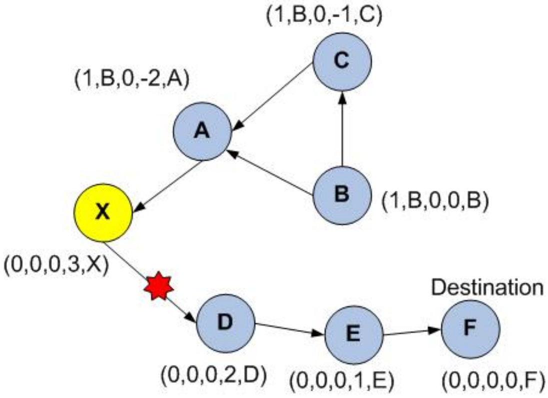

Fig. 5. Attacker *X* pretends a link failure to node *D*

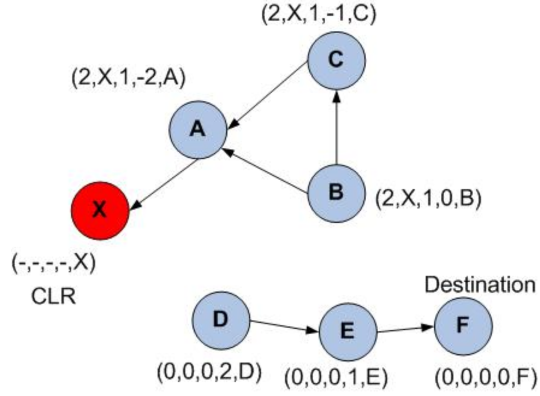

Fig. 6. Route erasure process

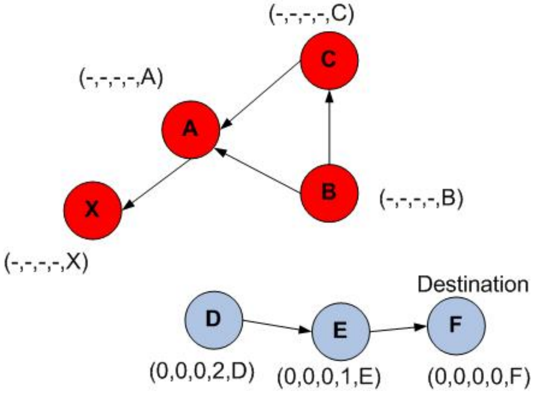

Fig. 7. Route from upper stream to the destination is disrupted

is not broken). It performs the route maintenance process by defining a new reference level and sends the forging UPD to its upstream neighbor *C*. Fig. 6 shows the node metrics after route maintenance has completed. Upon receiving the reflected UPD from node *C*, the attacker node sends CLR message to its upstream node to finish the route erasure process. Fig. 7 shows the final network topology. It is clearly shown that the attacker has disabled the route to the destination.

4 Simulation Results

4.1 Simulation Environment

To verify various types of attacks in TORA, we have implemented three types of misuses on QRY messages through simulations. The other misuses on UPD and CLR messages can be verified using similar simulations as well. The ns-allinone-2.29 simulation software [13] is compiled and run in Mandriva Linux 2006 Kernel 2.6.12-12mdksmp. Apart from the original TORA routing protocol, another malicious routing protocol named MYTORA is introduced in the simulations. Both protocols inherit the same packet format and routing mechanisms. But the send and receive functions of MYTORA agent are overridden with attacking code. For all the simulations, Node 2 is chosen as the inside attacker, while node 0 and 1 represent the source and destination respectively. Table 2 summarizes the simulation parameters.

Table 2. Simulation parameters

Network Size	800 * 600 m^2
Number of Nodes	8
Communication Type	CBR
Transmission Range	250 m
Transmission Capacity	2Mbps
MAC	802.11
Packet Size	512 bytes
Number of Inside Attackers	1

4.2 Simulation Results

Normal Communication. Fig. 8 shows the trace for normal communication in the simulated ad hoc network. At t = 6.888s, node 0 initiated the route discovery process by sending out a QRY message to its neighbor. Data packet from source node 0 was successfully delivered to the destination node 1 at t = 6.970763501s.

```
T 6.888000000 _0_ tora enq 0->1
T 6.888000000 _0_ tora sendQRY 1
s 6.894572565 _0_ RTR   --- 186 IMEP 58 [0 0 0 0] ------- [0:255 -1:255 1 0] [- H O 0x0026]
T 6.895853142 _4_ tora sendQRY 1
s 6.904398697 _4_ RTR   --- 190 IMEP 70 [0 0 0 0] ------- [4:255 -1:255 1 0] [A H O 0x0032]
T 6.905995180 _2_ tora sendQRY 1
s 6.906410910 _2_ RTR   --- 194 IMEP 78 [0 0 0 0] ------- [2:255 -1:255 1 0] [A H O 0x003a]
T 6.908111574 _6_ tora sendQRY 1
s 6.908665040 _6_ RTR   --- 200 IMEP 78 [0 0 0 0] ------- [6:255 -1:255 1 0] [A H O 0x003a]
s 6.915700590 _5_ RTR   --- 205 IMEP 102 [0 0 0 0] ------- [5:255 -1:255 1 0] [A H O 0x0052]
s 6.916333691 _7_ RTR   --- 206 IMEP 118 [0 0 0 0] ------- [7:255 -1:255 1 0] [A H O 0x0062]
s 6.917528699 _6_ RTR   --- 211 IMEP 86 [0 0 0 0] ------- [6:255 -1:255 1 0] [A - O 0x0042]
s 6.920887262 _2_ RTR   --- 220 IMEP 102 [0 0 0 0] ------- [2:255 -1:255 1 0] [A - O 0x0052]
s 6.929541387 _4_ RTR   --- 225 IMEP 90 [0 0 0 0] ------- [4:255 -1:255 1 0] [A - O 0x0046]
s 6.931137964 _0_ RTR   --- 184 cbr 532 [0 0 0 0] ------- [0:0 1:0 32 4] [0] 0 1
s 6.931217311 _0_ RTR   --- 229 IMEP 90 [0 0 0 0] ------- [0:255 -1:255 1 0] [A - O 0x0046]
s 6.938260074 _3_ RTR   --- 233 IMEP 94 [0 0 0 0] ------- [3:255 -1:255 1 0] [A H O 0x004a]
f 6.941806005 _4_ RTR   --- 184 cbr 532 [13a 4 0 800] ------- [0:0 1:0 31 2] [0] 1 1
f 6.952939202 _2_ RTR   --- 184 cbr 532 [13a 2 4 800] ------- [0:0 1:0 30 7] [0] 2 1
f 6.962050907 _7_ RTR   --- 184 cbr 532 [13a 7 2 800] ------- [0:0 1:0 29 1] [0] 3 1
r 6.970763501 _1_ AGT   --- 184 cbr 532 [13a 1 7 800] ------- [0:0 1:0 29 1] [0] 4 1
```

Fig. 8. Fragment trace file for the simulated attacker-free network

QRY_DR_RD. Fig. 9 shows that no data packet was delivered from the source node as the route creation process was disrupted by the attacker node 2. The QRY packet propagated from node 4 to node 2 has been discarded by node 2.

```
T 6.888000000 _0_ tora enq 0->1
T 6.888000000 _0_ tora sendQRY 1
s 6.894572565 _0_ RTR   --- 186 IMEP 58 [0 0 0 0] ------- [0:255 -1:255 1 0] [- H O 0x0026]
T 6.895853142 _4_ tora sendQRY 1
s 6.904398697 _4_ RTR   --- 190 IMEP 70 [0 0 0 0] ------- [4:255 -1:255 1 0] [A H O 0x0032]
s 7.000000000 _0_ RTR   --- 193 IMEP 36 [0 0 0 0] ------- [0:255 -1:255 1 0] [A - - 0x0010]
s 7.053463980 _0_ AGT   --- 196 cbr 512 [0 0 0 0] ------- [0:0 1:0 32 0] [1] 0 1
T 7.053463980 _0_ tora enq 0->1
```

Fig. 9. Fragment trace file for compromised network (QRY_DR_RD)

QRY_MF_RD. As shown in Fig. 10, the malicious node 2 modified the destination node to a non-existent node 88 after it received the QRY message from node 4 at t = 6.906875180s. After that, the attacker node forwarded the false QRY message to its neighbor node 4. This resulted all the propagated QRY messages containing an invalid address. In this case, the source node would not be able to find its path to the destination.

```
T 6.888880000   _0_ tora enq 0->1
T 6.888880000 _0_ tora sendQRY 1
s 6.895452565 _0_ RTR   --- 186 IMEP 58 [0 0 0 0] ------- [0:255 -1:255 1 0] [- H O 0x0026]
T 6.896733142 _4_ tora sendQRY 1
s 6.905278697 _4_ RTR   --- 190 IMEP 70 [0 0 0 0] ------- [4:255 -1:255 1 0] [A H O 0x0032]
T 6.906875180 _2_ tora sendQRY 88
s 6.907290910 _2_ RTR   --- 194 IMEP 78 [0 0 0 0] ------- [2:255 -1:255 1 0] [A H O 0x003a]
T 6.908991392 _4_ tora sendQRY 88
T 6.908991574 _6_ tora sendQRY 88
T 6.908991582 _7_ tora sendQRY 88
s 6.911134766 _4_ RTR   --- 201 IMEP 58 [0 0 0 0] ------- [4:255 -1:255 1 0] [A - O 0x0026]
T 6.912135249 _2_ tora sendQRY 88
T 6.912135343 _0_ tora sendQRY 88
………………………..
T 6.917379507 _5_ tora sendQRY 88
T 6.917379902 _1_ tora sendQRY 88
```

Fig. 10. Fragment trace file for compromised network (QRY_MF_RD)

QRY_AF_RC. In this simulation, a function is added in the simulation program to generate extraneous QRY packets. The huge amount of QRY messages is used to flood the network and consume the bandwidth or to drain power supply of victim nodes. This function also enables the inside attacker to spoof a fresh source IP and destination IP in every round to conceal itself. We also modify the simulation parameters. Total number of nodes is increased to 20, and total cbr data connections are also increased to 20 connection. In addition, an energy model with an initial energy of 100 Watts is considered. Transmission and reception power is set to 0.6 Watts and 0.3 Watts respectively. The attacker node continuously generates 20 QRY messages per second to flood network.

Table 3 shows the remaining energy left in a node for a duration of 30 seconds and 80 seconds. The nodes are randomly chosen from the 20 nodes in the simulated network. The initial energy of each node is set to 100W. From the result, it is clearly shown that the energy consumption in the attacker-free network is less than the compromised network.

Table 3. The remaining energy left in a node for a duration of 30 seconds and 80 seconds

Node	Remaining Energy (Watts)			
	Duration: 30 seconds		Duration: 80 seconds	
	Normal	Compromised	Normal	Compromised
Node 0	99.201974	91.623927	96.182657	76.647517
Node 1	99.719094	89.140990	99.130456	68.513623
Node 3	99.215722	91.077395	96.493301	74.825234
Node 5	98.831571	90.830407	94.708739	73.973073
Node 6	99.055924	91.733302	95.694659	76.761668
Node 7	99.165023	91.643021	96.060147	76.663506

5 Related Work

Many MANET's routing protocols fail to provide adequate security. A number of studies on vulnerabilities and attack analysis on MANET's routing protocols have been published in [4, 14, 15]. To protect MANETs from malicious attacks, some security mechanisms have been proposed. In general, there are two types of security mechanisms: preventive and detective. Preventive mechanisms include identification, authentication and authorization where cryptography serves as the main building component [2, 6, 7, 10]. These secure routing protocols can be used to guarantee the acquisition of correct network topological information. While in detective mechanism, intrusion detection systems (IDSs) are introduced [3, 5, 11, 12, 16]. This approach enables the participating nodes to detect and avoid malicious behavior in the network without altering the underlined routing protocol or infrastructure.

6 Conclusions

Due to some specific characteristics such as dynamic environments and lack of physical infrastructure supports, MANETs are more vulnerable than traditional wired networks. Various attacks especially those targeting in routing are rather simple to be launched by misbehaving nodes in ad hoc networks. This paper present a systematic analysis of insider attacks against the TORA routing protocol. The attacks goals and the misuse actions are identified. The misuse actions can be effectively manipulated to attack the vulnerabilities in TORA routing protocols for achieving certain attacks objectives. The simulation results have shown that the malicious node can degrade the network performance, disrupt the route discovery process and consume scarce resource of the victim nodes.

There are still a lot of works for improving the security in TORA routing protocol. We plan to study more complicated attacks against TORA. The effect of the attacks on network performance will be analyzed based on the metrics such as latency, routing overhead, and packet delivery ratio. The results will serve as a guideline for designing a robust and secure TORA routing protocol.

References

1. Corson, M.S., Ephremides, A.: A Distributed Routing Algorithm for Mobile Radio Networks. In: Proceedings of the IEEE Military Communications Conference, Piscataway, NJ (October 1989)
2. Hu, Y., Perrig, A., Johnson, D.B.: Ariadne. A Secure On-Demand Routing Protocol for Ad Hoc Networks. Department of Computer Science, Rice University, Tech. Rep. TR01-383 (December 2001)
3. Marti, S., Giuli, T., Lai, K., Baker, M.: Mitigating Routing Misbehavior in Mobile Ad Hoc Networks. In: Proceedings of the Sixth Annual International Conference on Mobile Computing and Networking (MobiCom 2000) (August 2000)
4. Ning, P., Sun, K.: How to Misuse AODV: A Case Study of Insider Attacks Against Mobile Ad hoc Routing Protocols. In: Proceedings IEEE Information Assurance Workshop, West Point, NY (June 2003)

5. Orset, J.-M., Alcalde, B., Cavalli, A.: An EFSM-Based Intrusion Detection System for Ad Hoc Networks. In: Third International Symposium on Automated Technology for Verification and Analysis (ATVA 05), Taipei, Taiwan (October 2005)
6. Papadimitratos, P., Haas, Z.J.: Secure Routing for Mobile Ad Hoc Networks. In: SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS2002), San Antonio, TX (January 2002)
7. Papadimitrators, P., Haas, Z.J.: Secure Message Transmission in Mobile Ad Hoc Networks. In: Ad Hoc Networks 2003, pp. 193–209 (2003)
8. Park, V., Corson, S.: A Highly Adaptive Distributed Routing Algorithm for Mobile Wireless Networks. In: Proceedings of IEEE INFOCOM '97, pp. 1405–1413. IEEE Computer Society Press, Los Alamitos (1997)
9. Park, V., Corson, S.: Temporally-ordered Routing Algorithm (TORA) Version 1: Functional Specification, Internet Draft, draft-ietf-manet-tora-spec-04.txt (July 2001)
10. Perrig, A., Canetti, R., Tygar, D., Song, D.: The TESLA Broadcast Authentication Protocol. RSA Cryptobytes (RSA Laboratories) 5(2), 2–13 (2002)
11. Sterne, D., Balasubramanyam, P., Carman, D., Wilson, B., Talpade, R., Ko, C., Balupari, R., Tseng, C.-Y., Bowen, T., Levitt, K., Rowe, J.: A General Cooperative Intrusion Detection Architecture for MANETs. In: Proceedings of the 3rd IEEE International Workshop on Information Assurance (March 2005)
12. Tseng, C.Y., Balasubramanyam, P., Ko, C., Limprasittiporn, R., Rowe, J., Levitt, K.: A Specification-Based Intrusion Detection System for AODV. In: ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN '03) (October 21, 2003)
13. UCB/LBNL/VINT. The Network Simulator - ns-2. Information Sciences Institute (ISI), University of Southern California, CA, available at http://www.isi.edu/nsnam/ns/
14. Wang, W., Lu, Y., Bhargava, B.K.: On Vulnerability and Protection of Ad Hoc On-demand Distance Vector Protocol. In: Proceedings of IEEE International Conference on Telecommunication (ICT). IEEE Computer Society Press, Los Alamitos (2003)
15. Yang, H., Luo, H., Ye, F., Lu, S., Zhang, U.: Security in Mobile Ad Hoc Networks: Challenges and Solutions. IEEE Wireless Communications 11(1), 38–47 (2004)
16. Zhang, Y., Lee, W.: Intrusion Detection in Wireless Ad Hoc Networks. In: Proceedings of the Sixth Annual International Conference on Mobile Computing and Networking (MobiCom 2000) (August 2000)