Proceedings of the 2003 IEEE
Workshop on Information Assurance
United States Military Academy, West Point, NY June 2003

How to Misuse AODV: A Case Study of Insider Attacks against Mobile Ad-hoc Routing Protocols

Peng Ning and Kun Sun
Computer Science Department, North Carolina State University
Raleigh, NC 27695-8207
Emails: ning@csc.ncsu.edu, ksun3@unity.ncsu.edu

Abstract— **This paper presents a systematic analysis of insider attacks against mobile ad-hoc routing protocols, using the Ad hoc On-Demand Distance Vector (AODV) protocol as an example. It identifies a number of attack goals and then studies how to achieve these goals through misuses of the routing messages. To facilitate the analysis, this paper classifies the insider attacks into two categories:** ***atomic misuses*** **and** ***compound misuses.*** **Atomic misuses are performed by manipulating a single routing message, which cannot be further divided; compound misuses are composed of combinations of atomic misuses and possibly normal uses of the routing protocol. The analysis results in this paper reveal several classes of insider attacks, including** ***route disruption, route invasion, node isolation,*** **and** ***resource consumption.*** **This paper also includes simulation results that demonstrate the impact of these attacks.**

I. Introduction

Mobile Ad-hoc Networks (MANET) have attracted substantial research efforts recently, partially due to their attractive applications in infrastructureless situations such as battle fields and disaster recovery. Among all the research issues, security in MANET is particularly challenging due to the nature of wireless communication and the lack of infrastructure supports. Several efforts (e.g., Security-aware AODV [1], Ariadne [2], SEAD [3], CONFIDANT [4], watchdog and pathrater [5]) are under way to provide security services in ad-hoc routing protocols.

Most of the current security mechanisms (e.g., Ariadne [2], SEAD [3]) are preventive approaches that depend on cryptography to ensure the security of the network. However, in a typical mobile ad-hoc network such as a battle field, mobile nodes are extremely vulnerable to capture or key compromise. Even if critical keying materials are protected by tamper proof hardware, it is still difficult to ensure that the same hardware will not be misused by an attacker. Thus, to ensure the overall security of the network, it is important to develop security mechanisms that can survive malicious attacks from "insiders" who have full control of some nodes. In order to protect against insider attacks, it is necessary to understand how an insider can attack a wireless ad-hoc network. Several attacks (e.g., routing disruption attacks and resource consumption attacks [2], [3]) have been discussed in the literature. However, these attacks have not been seriously studied and verified.

In this paper, we adopt a systematic way to study the insider attacks against mobile ad-hoc routing protocols. We first identify a number of misuse goals that an inside attacker may want to achieve, and then enumerate all possible actions that an attacker may apply to a routing message. Our analysis is then to examine whether the attack goals may be achieved through these misuse actions. To facilitate the analysis, we further classify misuses of the AODV protocol into two categories: *atomic misuses* and *compound misuses.* Intuitively, atomic misuses are performed by manipulating a single routing message, which cannot be further divided. In contrast, compound misuses are composed of multiple atomic misuses, and possibly normal uses of the routing protocol.

Since atomic misuses are potentially building blocks of compound misuses, in this paper, we start with analyzing atomic misuses. In addition, we also study compound misuses that can achieve more powerful effects than simple compositions of atomic misuses when carefully composed together. We do not discuss simple compositions of atomic misuses, though we do perform simulation experiments to study their impacts. We pick the AODV protocol [6] as a target, performing our analysis from an attacker's perspective. It is easy to see that our analysis scheme is also applicable to other ad-hoc routing protocols, possibly with slight changes. To validate the analysis results, we have implemented the misuses based on the AODV extension in ns2, and evaluated the effectiveness of the misuses through simulations.

The rest of this paper is organized as follows. The next section briefly describes the AODV protocol. Section III describes our analysis scheme. Section IV focuses on analyzing the atomic misuses of AODV routing message. Section V discusses compound misuses. Section VI presents the experimental results. Section VII discusses the related

This work is partially supported by the U.S. Army Research Office under grant DAAD 19-02-1-0219, by the National Science Foundation under grants CCR-0207297 and ITR-0219315.

ISBN 0-7803-7808-3/03/$17.00 © 2003 IEEE

work in security of wireless ad-hoc networks. Section VIII concludes this paper and points out future research directions.

II. An Overview of AODV Protocol

The Ad-hoc On-Demand Distance Vector (AODV) [6] protocol is an on-demand routing protocol, which initiates a route discovery process only when desired by a source node. When a source node wants to send data packets to a destination node but cannot find a route in its routing table, it broadcasts a Route Request (RREQ) message to its neighbors. Its neighbors then rebroadcast the RREQ message to their neighbors if they do not have a *fresh enough* route to the destination node. (A fresh enough route is a valid route entry for the destination node whose associated sequence number is equal to or greater than that contained in the RREQ message.) This process continues until the RREQ message reaches the destination node or an intermediate node that has a fresh enough route.

Every node has its own sequence number and RREQ ID[1]. AODV uses sequence numbers to guarantee that all routes are loop-free and contain the most recent routing information. RREQ ID in conjunction with source IP address uniquely identify a particular RREQ message. The destination node or an intermediate node only accepts the first copy of a RREQ message, and drops the duplicated copies of the same RREQ message.

After accepting a RREQ message, the destination or intermediate node updates its *reverse route* to the source node using the neighbor from which it receives the RREQ message. The reverse route will be used to send the corresponding Route Reply (RREP) message to the source node. Meanwhile, it updates the sequence number of the source node in its routing table to the maximum of the one in its routing table and the one in the RREQ message. When the source or an intermediate node receives a RREP message, it updates its forward route to the destination node using the neighbor from which it receives the RREP message. It also updates the sequence number of the destination node in its routing table to the maximum of the one in its routing table and the one in the RREP message. A Route Reply Acknowledgement (RREP-ACK) message is used to acknowledge receipt of a RREP message. Though not required, AODV may utilize the HELLO message to maintain the local connectivity of a node.

Route maintenance is done with Route Error (RERR) messages. If a node detects a link break in an active route, it sends out a RERR message to its upstream neighbors that use it as the next hop in the broken route. When a node receives a RERR message from its neighbor, it further forwards the RERR message to its upstream neighbors.

AODV is a stateless protocol; the source node or an intermediate node updates its routing table if it receives a RREP message, regardless of whether it has sent or forwarded a corresponding RREQ message before. If it cannot find the next hop in the reverse routing table, it simply drops the RREP message. Otherwise, it unicasts the RREP message to the next hop in the reverse route.

In general, a node may update the sequence numbers in its routing table whenever it receives RREQ, RREP, RERR, or RREP-ACK messages from its neighbors.

III. Analysis Scheme

We adopt a systemic way to analyze the insider attacks against the AODV protocol. We first identify a number of misuse goals that an inside attacker may want to achieve, and then study how these goals may be achieved through misuses of the routing messages. These misuse goals are listed as follows.

- *Route Disruption (RD).* Route Disruption means either breaking down an existing route or preventing a new route from being established.
- *Route Invasion (RI).* Route invasion means that an inside attacker adds itself into a route between two endpoints of a communication channel.
- *Node Isolation (NI).* Node isolation refers to preventing a given node from communicating with any other node in the network. It differs from Route Disruption in that Route Disruption is targeting at a route with two given endpoints, while node isolation is aiming at all possible routes.
- *Resource Consumption (RC).* Resource consumption refers to consuming the communication bandwidth in the network or storage space at individual nodes. For example, an inside attacker may consume the network bandwidth by either forming a loop in the network.

There may be other attack goals (e.g., denial of service); however, we do not consider them in our current work.

To facilitate the analysis, we further classify misuses of the AODV protocol into two categories: *atomic misuses* and *compound misuses.* Intuitively, atomic misuses are performed by manipulating a single routing message, which cannot be further divided. In contrast, compound misuses are composed of multiple atomic misuses, and possibly normal uses of the routing protocol. It is easy to see that atomic misuses may be used as building blocks of compound misuses.

We perform our analysis of atomic misuses through understanding the effects of possible *atomic misuse actions.* Each atomic misuse action is an indivisible manipulation of one routing message. Specifically, we divide the atomic misuse actions in AODV into the following four categories:

- *Drop (DR).* The attacker simply drops the received routing message.
- *Modify and Forward (MF).* After receiving a routing message, the attacker modifies one or several fields in the mes-

[1] It is also known as flood ID in earlier versions of AODV specifications.

ISBN 0-7803-7808-3/03/$17.00 © 2003 IEEE

sage and then forwards the message to its neighbor(s) (via unicast or broadcast).

- *Forge Reply (FR).* The attacker sends a faked message in response to the received routing message. Forge Reply is mainly related to the misuse of RREP messages, which are in response of RREQ messages.
- *Active Forge (AF).* The attacker sends a faked routing message without receiving any related message.

At first glance, compound misuses seem to be simple compositions of atomic uses. However, when carefully aggregated together, some compositions of atomic misuses become more powerful attacks due to the changes in the number of messages. For example, if an attacker regularly broadcasts RREQ messages with false information in the neighborhood of a victim node, the attacker can successfully prevent the victim node from receiving any messages. In our analysis of compound misuses, we focus on the aforementioned, "powerful" compound misuses; simple compositions of atomic misuses (and possibly the normal routing messages as well as the above compound misuses) can be analyzed via automatic vulnerability analysis tools (e.g., attack graphs [8]).

It is easy to see that our analysis scheme is also applicable to other mobile ad hoc routing protocols, possibly with slight modification. However, in this paper, we only focus on the AODV protocol, while considering the analysis of the other protocols as possible future work.

Since atomic misuses form the foundation of compound misuses, in the following, we first perform a systematic analysis of atomic misuses of the AODV protocol, and then study how atomic misuses and normal routing messages may be combined to launch compound misuses.

IV. Atomic Misuses of AODV

In this section, we present our analysis results about atomic misuses of the AODV protocol. Due to the space limit, we only summarize the results and discuss a few atomic misuses in detail. For the complete set of atomic misuses, please refer to the appendix of our technical report [7].

In our analysis, we use a simple naming scheme to identify atomic misuses, which combines routing message type and atomic misuse action. Specifically, each atomic misuse is named in the form of `MessageType_Action`, which means that an inside attacker applies the "`Action`" to a routing message of type "`MessageType`." For brevity, we use the abbreviations introduced in the previous section to represent atomic misuse actions. For example, `RREP_DR` represents that an attacker drops (DR) a RREP message. We also use names in the form of `MessageType_Action_Goal` to represent that an inside attacker attempts to achieve the "`Goal`" by applying the "`Action`" to a routing message of type "`MessageType`." For example, `RREP_DR_RD` represents that an attacker attempts to disrupt (RD) a route by dropping (DR) a RREP message.

A. Atomic Misuses of RREQ Messages

Table I summarizes the atomic misuses of a RREQ message. The atomic misuse action *Forge Reply* is not applicable to RREQ messages, since RREQ messages are not used to reply to any other routing message.

Atomic misuse `RREQ_DR` refers to simply dropping the received RREQ message. If an attacker applies such attacks to all the RREQ messages it receives, this kind of misuses is equivalent to not having the attacking node in the network. An inside attacker may also selectively drop RREQ messages. Attackers that launch such misuses are in nature similar to the selfish nodes mentioned in [5].

Atomic misuse `RREQ_MF` refers to the atomic misuses with which an inside attacker modifies one or several fields in a RREQ message that it just receives, and then broadcasts the modified RREQ message. Table II lists the RREQ message fields that an attacker may modify as well as the possible modifications.

Several fields have immediate security implications when modified. RREQ ID along with the source IP address uniquely identifies a RREQ message; they indicate the freshness of a RREQ message. Since a node only accepts the first copy of a RREQ message, an increased RREQ ID along with the source IP address can guarantee that the faked RREQ message is accepted by other nodes.

To ensure loop freedom in AODV, after receiving a RREQ message, a node updates its reverse routing table only if the source sequence number field in the RREQ message is greater than that in its routing table, or the source sequence numbers are equal, but the hop count field in the RREQ message is smaller than that in the routing table. An inside attacker may also change these fields to affect other nodes' routing table.

An intermediate node or a source node updates its forward routing table if the destination sequence number in the RREP message is greater than the one in its routing table, or the destination sequence numbers are the same, but the hop count in the RREP message plus one is smaller than the one in its routing table. An inside attacker may increase the sequence numbers or decrease the hop count in a faked RREQ message to update other nodes' routing tables, or decrease the sequence numbers or increase the hop count to invalidate a RREQ message.

When a node updates its routing table, the next hop in the route entry is assigned as the node from which it receives the RREQ message. An inside attacker may manipulate the source IP address in the IP header to change the reverse route.

Both `RREQ_DR` and `RREQ_MF` must be triggered by an incoming RREQ message. In contrast, an inside attacker may perform a `RREQ_AF` misuse to forge a RREQ message without receiving a RREQ message. An inside attacker

ISBN 0-7803-7808-3/03/$17.00 © 2003 IEEE

TABLE I
ATOMIC MISUSES OF A RREQ MESSAGE AND ACHIEVABLE MISUSE GOALS.

Atomic Misuse	Route Disruption	Route Invasion	Node Isolation	Resource Consumption
RREQ_DR	Yes (in some cases)	No	No	No
RREQ_MF	Yes	Yes	Partial[2]	No
RREQ_AF	Yes	Yes	Partial	No

TABLE II
POSSIBLE MODIFICATIONS OF FIELDS IN A RREQ MESSAGE.

RREQ Message Field	Modifications
Type	Change the message type.
RREQ ID	Increase it to make the faked RREQ message acceptable, or decrease it to make the RREQ message unacceptable.
Hop Count	Decrease it to update other nodes' reverse routing tables, or increase it to invalidate the update.
Destination IP Address	Replace it with another IP address.
Destination Sequence Number	Increase it to update other nodes' forward route tables, or decrease it to suppress its update.
Source IP Address	Replace it with another IP address.
Source Sequence Number	Increase it to update other nodes' reverse route tables, or decrease it to suppress its update.
Flags	Reverse the setting.

may need to collect some necessary information to forge RREQ messages (e.g., by listening to the traffic). Theoretically, the attacker may forge any field in a RREQ message, generating the effects we just discussed.

Now let us look at an atomic misuse of a RREQ message, RREQ_MF_NI, with which an inside attacker prevents a victim node from receiving data packets from other nodes for a short period of time. The attacker may make the following modifications after it receives a RREQ message from the victim node: (1) Increase the RREQ ID by a small number; (2) Replace the destination IP address with a non-existent IP address; (3) Increase the source sequence number by at least one; (4) Set the source IP address in IP header to a non-existent IP address. The attacker then broadcasts the forged message. When the neighbors of the attacker receive the faked RREQ message, they will update the next hop to the source node to the non-existent node, since the faked RREQ message has a greater source sequence number. Due to the non-existent destination IP address, the faked message can be broadcast to the farthest nodes in the ad-hoc network. When other nodes want to send data packets to the source node, they will use the routes established by the faked RREQ message, and the data packets will be dropped due to the non-existent node.

This atomic misuse can prevent a victim node from receiving data packets for a short period of time; however, it cannot fully isolate the victim node, due to the local repair mechanism in the AODV protocol [6]. The other nodes will initiate another round of route discovery if they note that the data packets cannot be delivered successfully. In addition, the victim node may still be able to send data packets to other nodes.

Several of the atomic misuses of RREQ messages use RREQ messages to add entries to the routing tables of other nodes. These entries are different from those established through normal exchange of RREQ and RREP messages. In particular, the lifetime of these entries is set to a default value (e.g., 3 seconds as in our experiments). Thus, to make such entries effective, an attacker needs to launch the atomic misuses periodically.

B. Atomic Misuses of RREP Messages

Table III summarizes the atomic misuses of a RREP message and whether they can achieve the misuse goals. The premise of atomic misuses of RREP messages is that the inside attacker must already be in a reverse route involving a victim node, so that it can receive a RREQ or RREP message, or send a forged RREP through some other nodes. Due to this restriction, most of the atomic misuses of RREP messages, including RREP_DR RREP_MF, have limited impact.

Atomic misuse RREP_FR is specific to RREP messages. It refers to the misuse with which an attacker forges a RREP message in response to a RREQ message. For example, after receiving a RREQ message, an inside attacker may forge a RREP message as if it had a fresh enough route to the destination node. In order to suppress other legitimate RREP messages that the source node may receive from other nodes, the attacker may forge a faked RREP message by increasing the destination sequence number. An attacker may disrupt the route between the victim node to a given destination, or invade in the route between by suppressing other alternative routes.

An interesting atomic misuse is RREP_AF_RI. If an inside attacker has routes to both the source and the destination

TABLE III
Atomic Misuses of A RREP Message and Achievable Misuse Goals.

Atomic Misuse	Route Disruption	Route Invasion	Node Isolation	Resource Consumption
RREP_DR	Yes (in some cases)	No	No	No
RREP_MF	Yes	Yes	No	No
RREP_FR	Yes	Yes	No	No
RREP_AF	Yes	Yes	No	Yes

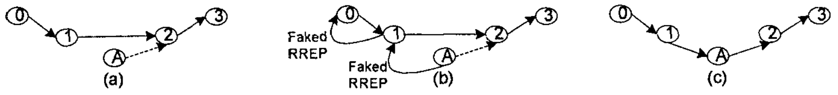


Fig. 1. An Attacker Invades A Route by Sending A Faked RREP Actively.

nodes of an existing route (as shown in Figure 1(a)), it can invade the route by sending a faked RREP message to the source node. In Figure 1, assume node A is the attacking node, which already has a route to nodes 0 and 3, respectively. Node A can forge a RREP message as follows: (1) Set the source IP to node 0; (2) Set the destination IP to node 3; (3) Set the destination sequence number to node 3's sequence number plus at least one; (4) Set the source IP in the IP header to node 2; (5) Set the destination IP in the IP header to node 1. Node A then sends the faked RREP message to node 1, which forwards the faked RREP message to node 0 (Figure 1(b)). When nodes 0 and 1 receive the faked RREP message, they will update the sequence number of node 3 in their routing tables to the destination sequence number in the faked RREP message. Node 0 will still use node 1 as the next hop to node 3, but node 1 will update node A as the next hop to node 3. Note that node A already has a route to node 3. As a result, node A successfully becomes a part of the route from node 0 to node 3 (Figure 1(c)).

C. Atomic Misuses of RERR Messages

Table IV summarizes the three types of atomic misuses of RERR messages and the misuse goals that they can achieve. The misuse action *Forge Reply* is not applicable to RERR messages, since RERR messages are not used to reply to any routing messages.

RERR_DR has limited impact on the network except for causing delays in the identification of route errors, since the upstream nodes will eventually discover the problematic routes and establish new routes.

In order to know which neighbors should receive a RERR message, each node keeps a "precursor list" of its neighbors for each route entry. When a link break is detected, the node sends a RERR message to all the nodes in the corresponding precursor list. To launch RERR_MF misuses, an inside attacker may modify the RERR message after it receives a RERR message, and send the faked RERR message to the neighbors in the precursor list. Table V lists the fields in a RERR message that the attacker may manipulate. Sometimes, the attacker may modify the IP addresses in the IP header as well.

V. Compound Misuses

One or several inside attackers may combine atomic misuses, and possibly normal uses of routing messages, in any order to launch compound misuses. For example, an attacker may repeatedly launch the same type of atomic misuses to make the impact persistent. As another example, an attacker may launch some early atomic or compound misuses to prepare for some later ones. A crucial issue here is to understand the compound misuses that can be used as "building blocks" of more complex attacks. Once we understand "building blocks," we may analyze the complex atomic scenarios through automatic vulnerability analysis tools such as the attack graphs [8].

For convenience, we extend the naming scheme for atomic misuses to denote compound misuses of the same type of atomic misuses. Specifically, we put an "s" after the type of routing message that is being misused in the corresponding atomic misuse. For example, RREQs_AF represent that an attacker actively forges multiple RREQ messages.

In our analysis, we observe that most atomic misuse targeted at disrupting services can only generate temporary impact due to the local repair mechanism that is commonly seen in mobile ad hoc routing protocols. Thus, to make the impact of these misuses persistent, an attacker needs to repeat the atomic misuses regularly. We do not discuss such misuses in detail; however, our experimental results will show that an attacker can indeed achieve its goals through such compound misuses.

Another class of compound misuses is more interesting than simply repeating the same type of atomic misuses. We discovered that an attacker may achieve some misuse goals through well planned combinations of atomic misuses. Let's see an example as follows.

An inside attacker may invade into a route through a RREQs_AF compound misuse. Consider the scenario shown

TABLE IV
ATOMIC MISUSES OF A RERR MESSAGE AND ACHIEVABLE MISUSE GOALS.

Atomic Misuse	Route Disruption	Route Invasion	Node Isolation	Resource Consumption
RERR_DR	Yes (in some case)	No	No	No
RERR_MF	Yes	No	No	Yes
RERR_AF	Yes	No	No	Yes

TABLE V
POSSIBLE MODIFICATIONS OF FIELDS IN A RERR MESSAGE.

RERR Message Field	Modifications
Type	Change the value of Type.
DestCount	Modify it according to the number of unreachable destinations included in the RERR message.
Unreachable Destination IP Address	Replaces it with another IP address.
Unreachable Destination Sequence Number	Increases it to update other nodes' routing table, or decreases it to invalidate this entry.
Additional Unreachable Destination IP address (if needed)	Add a new destination IP address which is still reachable.
Additional Unreachable Destination Sequence number (if needed)	Increases it to update other nodes' routing table, or decreases it to invalidate this entry.

in Figure 2(a). Suppose nodes 0 through 5 are normal nodes, and node A is the attacker node. Further assume there is a route from node 0 to node 5. The attacker at node A may forge a RREQ message as follows: (1) Set the source IP address as node 5; (2) Set the destination IP address as node 0; (3) Set the source sequence number to a number greater than node 5's current sequence number; (4) Set the source IP address in IP header as node A. Node A then broadcasts the faked RREQ message. After receiving this message, nodes 2 and 3 will both set node A as the next hop to node 5, as in Figure 2(b).

To further establish the route from node A to node 5, the attacker may generate the second RREQ message as follows: (1) Set the source IP address as node A; (2) Set the destination IP address as node 5; (3) Set the destination sequence number to a number greater than node 5's current sequence number; (4) Set the source IP address in the IP header as node A. Node A can then broadcast this RREQ message. This message will help node A establish a route to node 5, as in Figure 2(c).

As discussed earlier, one or several inside attackers may compose attacks by arbitrarily combining atomic and/or compound misuses. In particular, the attackers may use different misuses to complement each other. For example, RREQs_AF is effective in preventing a victim node from receiving messages from other nodes, and RREP_AF is effective in preventing other nodes from receiving from the victim node. By combining them together, the attacker(s) may successfully isolate a node. In addition, one or several inside attackers may use some misuses or normal routing messages to prepare for later misuses. For example, all RREP related misuses require a route involving both the attacker and the victim node. To prepare for such misuses, an attacker may use a normal RREQ message or an atomic misuse (e.g., RREQ_AF) to establish the required route. These misuses are interesting; however, we do not consider them in this paper. Indeed, manually analyzing such attacks is not the best option due to the potentially large search space for possible complex attack scenarios. A better solution is to model the individual misuses and then construct attack strategies through automatic tools. Our work in this paper provides the foundation required by such tools.

VI. EXPERIMENTAL RESULTS

In order to validate our analysis results, we have implemented all the misuses and performed a series of experiments through simulation. The simulation is based on ns2 version 9[3] with the CMU Monarch extension for the AODV protocol[4]. To take advantage of the existing AODV code, we implemented the atomic misuses by simply overriding the AODV agent's receive and send functions. Compound misuses are performed by repeating/combining the atomic misuses.

Table VI shows the parameters used in our experiments. We used continuous bit rate (CBR) in all our experiments. In each simulation scenario, there are 5 mobile nodes if it is for atomic misuses, and 20 nodes if it is for compound misuses. In all the experiments, there is only one inside attacker in the ad hoc network. The field configuration is 1000 m × 600 m. The simulation runs for 100 simulated seconds. After arriving at a location, a node stays there for 2.0 seconds before moving to the next location. A source node sends 4 data packets per simulated seconds. There are at most 20 connections during each simulation run.

[3] http://www.isi.edu/nsnam/ns/.
[4] http://www.monarch.cs.rice.edu/.

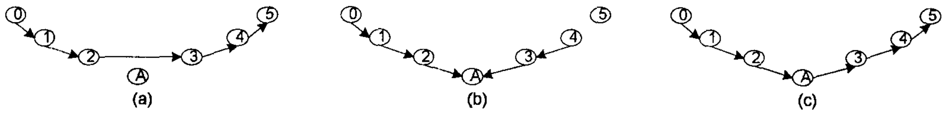


Fig. 2. Route Invasion by Two Faked RREQ Messages.

In a node's transmission range (250m), other nodes can receive signals from this node directly. The physical link bandwidth is 2 Mbps.

TABLE VI
SIMULATION PARAMETERS

Communication Type	CBR
Number of Nodes	5 or 20
Simulation Area	1000m*600m
Simulation Time	100 seconds
Pause Time	2.0 seconds
Packet Rate	4 pkt/sec
Number of Connections	20
Transmission Range	250m
Physical Link Bandwidth	2Mbps
Number of Inside Attackers	1

We have verified all the atomic misuses through analyzing the trace files generated by the simulations. We found that all the atomic misuses intended for *Route Disruption* and *Node Isolation* succeeded; however, the effect can last for a short period of time due to the local repair mechanism in the AODV protocol. This is due to two reasons. First, the impact caused by such atomic misuses are detectable by the normal nodes, which then attempt to recover from the failures by establishing new routes. Second, all the atomic misuses are performed with a single routing message. They do not have further impact once the affected nodes perform local repair successfully.

In contrast, the atomic misuses intended for *Route Invasion* are much more subtle. Unless the routes established via atomic misuses are disrupted, the victim nodes will continue to use the routes involving the inside attacker to transmit data packets. Details of the experiments about atomic misuses can be found in the appendix.

Though atomic misuses for *Route Disruption* and *Node Isolation* are not effective when they are used individually, our experiments show that they are quite powerful when they are used in compound misuses.

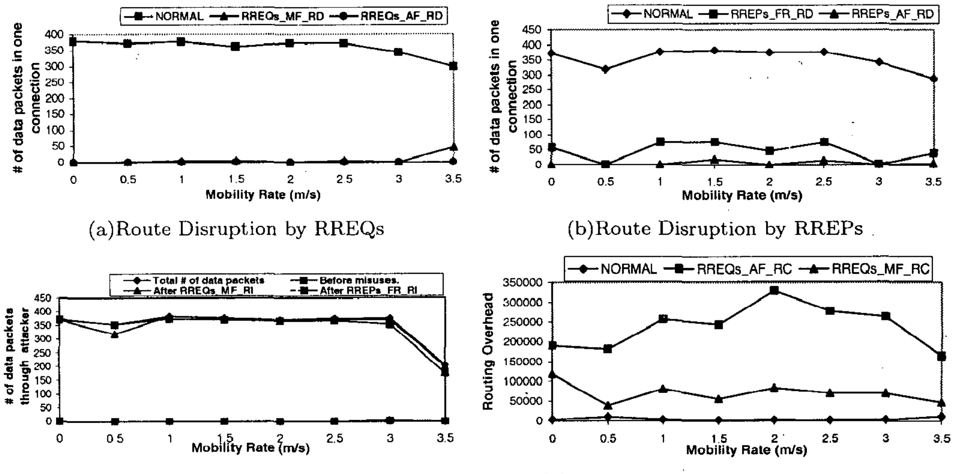
Figure 3 shows the experimental results for compound misuses for *Route Disruption, Route Invasion*, and *Resource Consumption.* Figure 3(a) displays the numbers of data packets transmitted between two victim nodes when using compound misuses of RREQ messages. It clearly shows that when RREQs_MF_RD and RREQs_AF_RD are used against these two nodes, the number of data packets drops almost to zero. Figure 3(b) shows the same measure when compound misuses of RREP messages are used. The number of data packets transmitted between the two victim nodes is slightly better than in Figure 3(a); however, it is still much lower than the number of packets transmitted in normal situations. Figure 3(c) shows the number of data packets transmitted through an inside attacker with or without *Route Invasion* misuses. It is easy to see that the misuses effectively make the attacker a part of the route between the two victim nodes. Finally, Figure 3(d) shows that the routing overhead with RREQs_MF_RC is higher than the overhead in normal situations, and RREQs_AF_RC misuse is much higher than the RREQs_MF_RC.

VII. Related Work

Research in MANET has been rather active. Several routing protocols have been proposed to discover and maintain routes in MANET environments, including secure routing protocols. Early proposals for secure ad hoc routing (e.g., [9], [1], [10], and [11]) use public key cryptography to protect ad hoc routing messages. However, due to the heavy computation involved in public key cryptography, these proposals are too expensive for nodes in mobile ad hoc networks, which are usually powered by batteries.

Recent results usually use symmetric cryptography to authenticate the routing messages. Papadimitratos and Haas proposed to authenticate the route discovery process with a secret key shared between the source and the destination nodes [12]. Basagni et al. use a network-wide secret key to secure the routing messages [13]. Yi et al. modified AODV to include security metrics for route discovery, using different trust levels with a shared symmetric key for each level [1]. Hu, Perrig, and Johnson have proposed a sequence of secure mobile ad hoc routing protocols, including Ariadne [2] and SEAD [3], as well as security mechanisms for routing protocols [14]. Their techniques include authenticating routing messages through a one-way key chain with delayed disclosures of keys, and authentication code with secret keys shared by mobile nodes.

Intrusion detection can provide another layer of protection to mobile ad hoc networks. Zhang and Lee proposed a distributed and cooperative IDS architecture in mobile adhoc networks [15]. They use data on the node's physical movements and the corresponding change in its routing table as the trace data to build the anomaly detection model. In Marti et al.'s proposal [5], each node uses a component



(a)Route Disruption by RREQs

(b)Route Disruption by RREPs

(c)RREPs_FR_RI and RREQs_MF_RI

(d)Resource Consumption by RREQs

Fig. 3. Experimental Results about Compound Misuses

called *watchdog* to detect misbehaving nodes, and another component called *pathrater* to choose a reliable route based on the information collected by the watchdog. In Buchegger and Boudec's proposal [4], each node not only monitors the bad behaviors of neighbors, but collects the list of malicious nodes from warnings sent from other trusted nodes.

VIII. Conclusions

In this paper, we reported the results of a systematic analysis of insider attacks against the AODV protocol. We classified the possible insider attacks into atomic misuses and compound misuses, and identified a number of atomic as well as compound misuses. We also performed a series of experiments (based on simulation) to validate these misuses. Our results showed that an inside attacker can effectively invade into routes or disrupt the normal operations of the AODV protocol.

The results in this paper represent our initial attempt in understanding insider attacks against mobile ad hoc routing protocols. As a part of our future work, we plan to investigate insider attacks against secure mobile ad hoc routing protocols such as Ariadne [2].

Acknowledgement We would like to thank the anonymous reviewers for their valuable comments.

References

[1] S. Yi, P. Naldurg, and R. Kravets, "Security-aware routing protocol for wireless ad hoc networks," in *Proc. of ACM MobiHoc 2001*, Oct 2001.

[2] Y. Hu, A. Perrig, and D. B. Johnson, "Ariadne: A secure on-demand routing protocol for ad hoc networks," in *Proc. of (MobiCom 2002)*, Sept. 2002.

[3] Y.-C. Hu, D. B. Johnson, and A. Perrig, "SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks," in *4th IEEE Workshop on Mobile Computing Systems and Applications*, June 2002.

[4] S. Buchegger and J. L. Boudec, "Performance analysis of the CONFIDANT protocol (cooperation of nodes: Fairness in dynamic ad-hoc networks)," in *Proc. of ACM MobiHoc 2002*, pp. 226–236, June 2002.

[5] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in *Proc. MobiCom 2000*, pp. 255–265, 2000.

[6] C. Perkins, E. Belding-Royer, and S. Das. Internet Draft, June 2002. draft-ietf-manet-aodv-11.txt.

[7] P. Ning and K. Sun, "How to misuse AODV: A case study of insider attacks against mobile ad-hoc routing protocols," Tech. Rep. TR-2003-07, CS Department, NC State University, 2003.

[8] O. Sheyner, J. Haines, S. Jha, R. Lippmann, and J. Wing, "Automated generation and analysis of attack graphs," in *Proc. of IEEE Symposium on Security and Privacy*, May 2002.

[9] L. Zhou and Z. J. Haas, "Securing ad hoc networks," *IEEE Network*, vol. 13, no. 6, pp. 24–30, 1999.

[10] J. Hubaux, L. Buttyan, and S. Capkun, "The quest for security in mobile ad hoc networks," in *Proc. ACM MobiHoc 2001*, 2001.

[11] K.Sanzgiri, B.Dahill, B.N.Levine, C.Shields, and E.M.Belding-Royer, "A secure routing protocol for ad hoc networks," in *Proc. of the Tenth IEEE Int'l Conf. on Network Protocols*, 2002.

[12] P. Papadimitratos and Z. J. Haas, "Secure routing for mobile ad hoc networks," in *Proc. of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference*, pp. 27 – 31, Jan 2002.

[13] S. Basagni, K. Herrin, D. Bruschi, and E. Rosti, "Secure pebblenets," in *Proc. of ACM MobiHoc 2001*, pp. 156–163, 2001.

[14] Y. Hu, A. Perrig, and D. V. Johnson, "Efficient security mechanisms for routing protocols," in *Proc. of the 10th Annual Network and Distributed System Security Symposium*, 2003.

[15] Y. Zhang and W. Lee, "Intrusion detection in wireless ad hoc networks," in *Proc. of ACM MobiCom 2000)*, pp. 275–283, 2000.