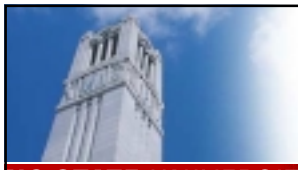


NC STATE UNIVERSITY Computer Science

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

Kun Sun

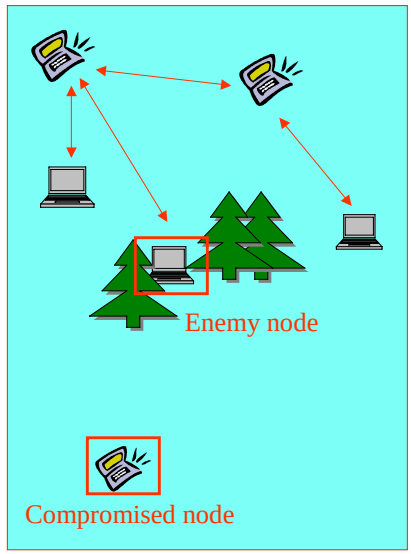
Department of Computer Science
North Carolina State University

Mobile Ad-hoc Networks (MANET)

- MANET
  - No infrastructure support
  - Wireless communication
  - Mobile
  - Each node functions as ahost and router
- Applications for MANET
  - Rescue missions
  - Scientific explorations
  - Military operations

Security in MANET

- Challenges
  - No physical boundary
  - No fixed topology
  - Unreliable communication
  - Nodes subject to capture ==> compromised nodes
  - It's likely to have insider attacks
- Existing work
  - Secure routing protocols
    - E.g., SAODV, SEAD, Ariadne
  - Intrusion detection
    - E.g., Watchdog and Pathrater, Anomaly detection in MANET
  - Insider attacks have not got enough attention.



Our Work

- Systematic analysis of insider attacks against ad-hoc routing protocols
  - The first step: insider attacks against AODV

Outline

- Part I:
  - Overview of AODV
- Part II:
  - Analysis scheme
  - Analysis results
  - Simulation results
  - Conclusion and future work

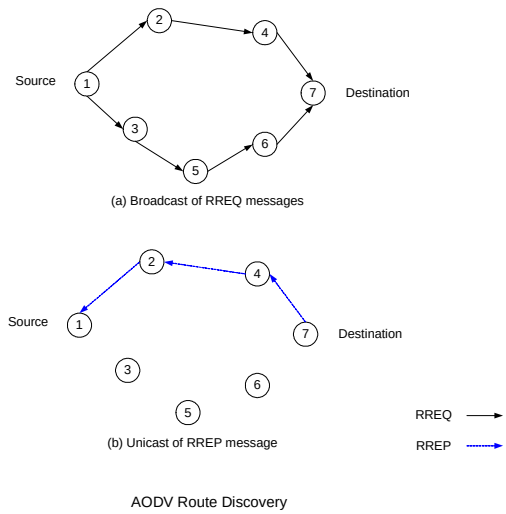
Overview of AODV

- Ad-hoc on-demand distance vector routing
  - Reactive (on-demand) routing protocol
    - Initiate route discovery only when desired by a source node
  - One of the 4 ad-hoc routing protocols considered by IETF MANET working group (with DSR, OLSR, and TBRPF)
  - Two phases
    - Route discovery
      - Route request message (RREQ)
      - Route reply message (RREP)
      - Route reply acknowledgment (RREP-ACK)
    - Route maintenance
      - Route error message (RERR)

AODV Route Discovery

1. When the desired route does not exist, a source node broadcasts a route request (RREQ) message to its neighbors.
2. Each node that receives the RREQ looks in its routing table to see if it is the destination or if it has a fresh enough route to the destination.
3. If it does, it unicasts a route reply (RREP) message back to the source, otherwise re-broadcast RREQ.
4. RREP is sent back along a reverse route that was created by RREQ.

AODV Route Discovery (Cont.)



AODV Route Discovery

AODV Route Maintenance

- When a node detects a link break in an active route, it sends out a RERR message to the nodes in the precursor list.
- When a node receives a RERR message from its neighbor, it further forwards the RERR message if its precursor list is not empty.
- Precursor list is updated when a node forwards the RREP messages.

RREQ Message Format

Type	J	R	G	D	U	Reserved	Hop Count
RREQ ID							
Destination IP address							
Destination Sequence Number							
Originator IP Address							
Originator Sequence Number							

- **Hop count** :the number of hops from the originator IP address to the node handling the request.
- **Sequence number**
- **Flag G:** Gratuitous RREP flag
- **Flag D:** Destination only flag

RREP Message Format

Type	R	A	Reserved	Prefix Sz	Hop Count
Destination IP address					
Destination Sequence Number					
Originator IP Address					
Lifetime					

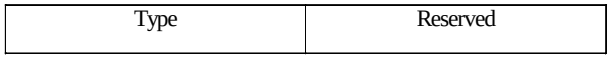
- **Lifetime**: the time in milliseconds for which nodes receiving the RREP consider the route to be valid.
- **Flag A:** Acknowledgment required

RERR Message Format

Type	N	Reserved	DestCount
Unreachable Destination IP Address (1)			
Unreachable Destination Sequence Number (1)			
Additional Unreachable Destination IP Addresses (if needed)			
Additional Unreachable Destination Sequence Numbers (if needed)			

DestCount: the number of unreachable destinations included in the message; MUST be at least 1.

RREP-ACK Message Format



- Deal with unidirectional links
- “Blacklist”

Analysis Scheme

- Basic idea
  - Identify misuse goals and misuse actions
    - Misuse goals: what an attacker wants
    - Misuse actions: misuses of AODV messages
  - Investigate how an inside attacker can achieve these goals by misuse actions.

Analysis Scheme (Cont'd)

- Atomic misuse actions
  - *Drop (DR)*
    - Simply drop the received message.
  - *Modify and forward (MF)*
    - After receiving a message, the attacker modifies it and forward the fake message to its neighbors.
  - *Forge reply (FR)*
    - Send fake message in response to a received message.
  - *Active forge (AF)*
    - Send fake message without receiving any message.

Analysis Scheme (Cont'd)

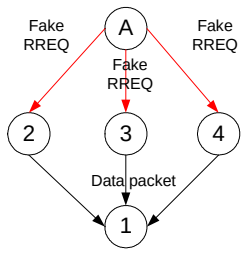
- Misuse goals
  - *Route disruption (RD)*
    - Break down an existing route or prevent a new route from being established
  - *Route invasion (RI)*
    - Attacker adds itself into an route
  - *Node isolation (NI)*
    - Prevent a victim node from communicating with any other nodes in the network
  - *Resource consumption (RC)*
    - Consume communication bandwidth, storage, or battery

Analysis Scheme (Cont'd)

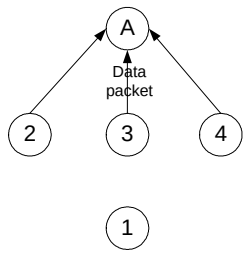
- Atomic and compound misuses
  - Atomic misuses
    - Misuses that can be done by manipulating one AODV message
  - Compound misuses
    - Combinations of atomic misuses and normal AODV messages
    - We will focus on "homogeneous compound misuses" which performed by repeating atomic misuses
      - Achieve more goals
      - Persistent impact
    - Other compound misuses can be analyzed through vulnerability analysis tools (e.g., Attack graphs)

Example: RREQ_AF_NI

- Actively forge one RREQ to prevent a victim node from receiving data packets for a short period time.



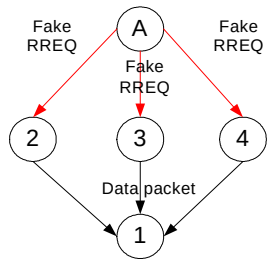
Attacker broadcasts fake RREQ message



Attacker drops data packets to node 1.

Example: RREQ_AF_NI (Cont'd)

- In the fake RREQ message
  1. Set the RREQ ID greater than the one maintained by node 1.
  2. Set Hop Count to 1.
  3. Set source IP address to node 1.
  4. Set the source sequence number greater than current sequence number of node 1.
  5. Set the destination IP address to a non-existent IP address.
  6. Replace the source IP address in IP header to a non-existent IP address or node A's IP address.



Attacker broadcasts fake RREQ message

Summary of Atomic Misuses

- Atomic misuses of a RREQ message

Atomic Misuse	Route Disruption	Route Invasion	Node Isolation	Resource Consumption
RREQ_DR	Yes *	No	No	No
RREQ_MF	Yes	Yes	Partial	No
RREQ_AF	Yes	Yes	Partial	No

Summary of Atomic Misuses (Cont'd)

- Atomic misuse of a RREP Message

Atomic Misuse	Route Disruption	Route Invasion	Node Isolation	Resource Consumption
RREP_DR	Yes *	No	No	No
RREP_MF	Yes	Yes	No	No
RREP_FR	Yes	Yes	No	No
RREP_AF	Yes	Yes	No	Yes

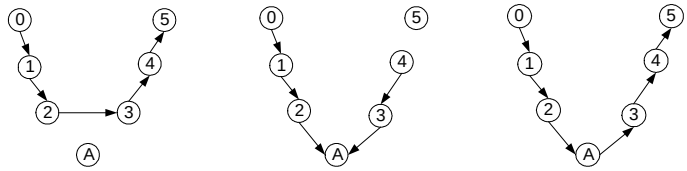
Summary of Atomic Misuses (Cont'd)

- Atomic misuse of a RERR message

Atomic Misuse	Route Disruption	Route Invasion	Node Isolation	Resource Consumption
RERR_DR	Yes	No	No	No
RERR_MF	Yes	No	No	No
RERR_AF	Yes	No	No	No

Example of Compound Misuses

- RREQs_AF_RI



(a) (b) (c)

A sends fake RREQ from 5 to 0

A sends RREQ from A to 5

Summary of Homogeneous Compound Misuses

Compound Misuses	Route Disruption	Route Invasion	Node Isolation	Resource Consumption
RREQs_DR	Yes *	No	No	No
RREQs_MF	Yes	Yes	Partial	Yes
RREQs_AF	Yes	Yes	Partial	Yes
RREPs_DR	Yes *	No	No	No
RREPs_MF	Yes	Yes	No	No
RREPs_FR	Yes	Yes	Partial	No
RREPs_AF	Yes	Yes	Partial	Yes
RERRs_DR	Yes	No	No	No
RERRs_MF	Yes	No	No	No
RERRs_AF	Yes	No	No	Yes

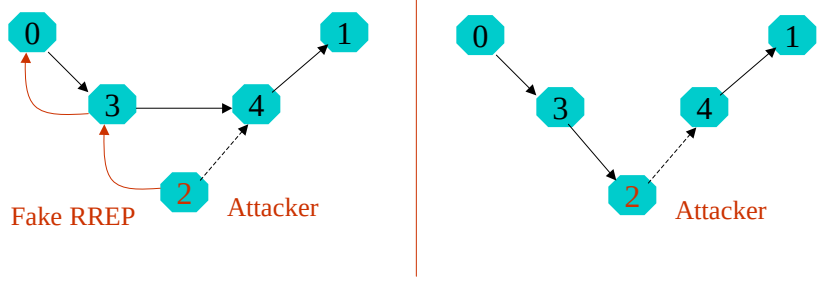
Simulation

- Network Simulator 2 (ns2) with CMU Monarch Extension
- Simulation Parameters

Communication Type	CBR
Number of Nodes	5 (atomic) or 20 (compound)
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

Example Scenario: RREP_AF_RI

- Attack Scenario



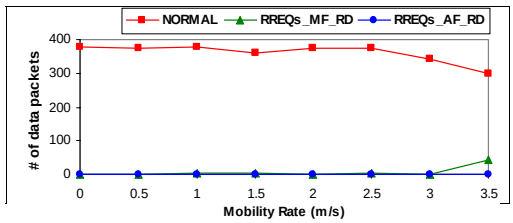
- Verify attacks by checking the trace files

RREP_AF_RI (Cont'd)

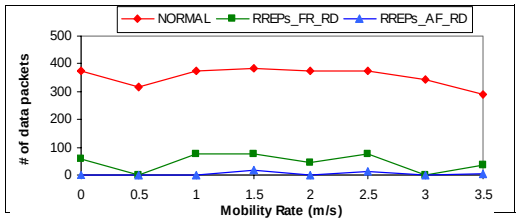
- Segments of RREP_AF_RI Trace File

```
s 7.693402932 _0_ RTR --- 0 cbr 68 [0 0 0 0] ------- [0:0 1:0 30 3] [0] 0 0
r 7.695563792 _3_ RTR --- 0 cbr 68 [13a 3 0 800] ------- [0:0 1:0 30 3] [0] 1 0
f 7.695563792 _3_ RTR --- 0 cbr 68 [13a 3 0 800] ------- [0:0 1:0 29 4] [0] 1 0
r 7.697885792 _4_ RTR --- 0 cbr 68 [13a 4 3 800] ------- [0:0 1:0 29 4] [0] 2 0
f 7.697885792 _4_ RTR --- 0 cbr 68 [13a 4 3 800] ------- [0:0 1:0 28 1] [0] 2 0
r 7.700206910 _1_ AGT --- 0 cbr 68 [13a 1 4 800] ------- [0:0 1:0 28 1] [0] 3 0
...
s 10.671253994 _2_ RTR  --- 0 AODV 44 [0 0 0 0] ------- [2:255 0:255 30 3] [0x4 1 [1 7] 10.000000] (REPLY)
r 10.680841103 _3_ RTR  --- 0 AODV 44 [13a 3 2 800] ------- [2:255 0:255 30 3] [0x4 1 [1 7] 10.000000] (REPLY)
f 10.680841103 _3_ RTR  --- 0 AODV 44 [13a 3 2 800] ------- [2:255 0:255 29 0] [0x4 2 [1 7] 10.000000] (REPLY)
r 10.682829964 _0_ RTR  --- 0 AODV 44 [13a 0 3 800] ------- [2:255 0:255 29 0] [0x4 2 [1 7] 10.000000] (REPLY)
...
s 11.619037018 _0_ RTR  --- 17 cbr 68 [0 0 0 0] ------- [0:0 1:0 30 3] [15] 0 0
r 11.620773878 _3_ RTR  --- 17 cbr 68 [13a 3 0 800] ------- [0:0 1:0 30 3] [15] 1 0
f 11.620773878 _3_ RTR  --- 17 cbr 68 [13a 3 0 800] ------- [0:0 1:0 29 2] [15] 1 0
r 11.623295681 _2_ RTR  --- 17 cbr 68 [13a 2 3 800] ------- [0:0 1:0 29 2] [15] 2 0
f 11.623295681 _2_ RTR  --- 17 cbr 68 [13a 2 3 800] ------- [0:0 1:0 28 4] [15] 2 0
r 11.625537484 _4_ RTR  --- 17 cbr 68 [13a 4 2 800] ------- [0:0 1:0 28 4] [15] 3 0
f 11.625537484 _4_ RTR  --- 17 cbr 68 [13a 4 2 800] ------- [0:0 1:0 27 1] [15] 3 0
r 11.627638602 _1_ AGT  --- 17 cbr 68 [13a 1 4 800] ------- [0:0 1:0 27 1] [15] 4 0
…
```


Experiment Results of Compound Misuses

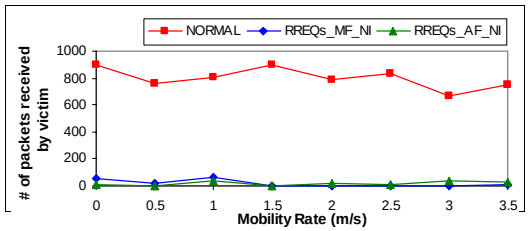


(a) Route Disruption by misuses of RREQ messages.

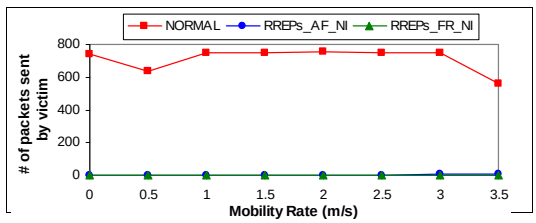


(b) Route Disruption by misuses of RREP messages.

Compound Misuses (Cont'd)

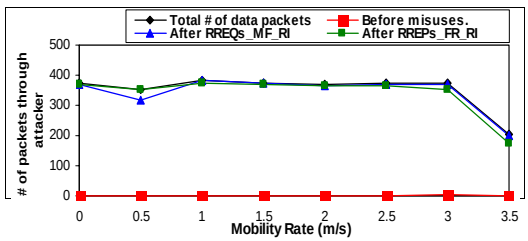


(c) Node Isolations by misuses of RREQ messages.

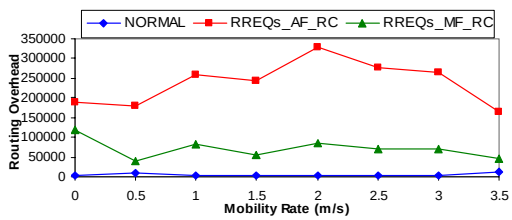


(d) Node Isolations by misuses of RREP messages.

Compound Misuses (Cont'd)



(e) Route Invasion



(f) Resource Consumption

Conclusion

- First step to systematically understand insider attacks in MANET
  - An analysis scheme
  - Misuses of AODV
  - Further information
    - Full paper: NCSU Computer Science Technical Report TR-2003-07
    - Software package available at

      http://discovery.csc.ncsu.edu/software/MisuseAODV/
- Future work
  - Analysis of secure ad-hoc routing protocols
    - Secure AODV, SEAD, Aridane
  - Prevention of possible misuses
  - Efficient and effective detection

Thank You!