Developing Attacks Defense Ideas for Ad Hoc Wireless Networks


Institute of Technology at Mato Grosso, Purdue University, University of North Carolina at Charlotte, Air Force Research Laboratories
Outline

- Introduction to collaborative attacks in ad hoc networks
- Vulnerabilities and attacks in ad hoc networks
- Characterization and classification of collaborative/coordinated attacks
- Defense strategies
- Preliminary evaluations
- Conclusions and outlook
Collaborative Attacks

- Collaborative attacks (CA) occur when more than one attacker or running process synchronize their actions to disturb a target network
  - Multiple attacks occur when a system is disturbed by more than one attacker, but not necessarily in collaboration

- Features of collaborative attacks
  - Attackers can launch sequential disruptions in short intervals so the target network is not able to respond in time
  - Attackers can also concentrate on a group of nodes or spread to different groups of nodes just for confusing the detection/prevention system in place
  - Attacks may be long-lived or short-lived ones
  - Internal and external users can collaborate to launch attacks
  - ...

Open Issues

- Comprehensive understanding of the coordination among attacks and/or the collaboration among various attackers
- Characterization and classification of CAs
- Intrusion Detection Systems (IDS) capable of correlating CAs
- Coordinated prevention/defense mechanisms
Wireless environments are highly susceptible to packet interception

Cooperation among nodes for relaying packets

Routing protocols are focused on performance

Mobility and self-configuring property make it easy for intrusion

Low energy capacity is a well-known weakness explored by intruders
Vulnerabilities and Attacks in Ad Hoc Networks

Examples of Attacks that can Collaborate

- Distributed Denial of Service (DDoS)
- Denial-of-Messages (DoM) attacks
- Blackhole attacks
- Wormhole attacks
- Sybil attacks
- Rushing attacks
- Malicious flooding

We are investigating the interactions among these forms of attacks

Example of probably incompatible forms of attacks:

- Wormhole attacks need fast connections, but DoM attacks reduce bandwidth!
Examples of Attacks that can Collaborate

- **Denial-of-Messages (DoM) attacks**
  - Malicious nodes may prevent other honest ones from receiving broadcast messages by interfering with their radio signal

- **Blackhole attacks**
  - A node transmits a malicious broadcast informing that it has the shortest and most current path to the destination aiming to intercept messages

- **Wormhole attacks**
  - An attacker records packets (or bits) at one location in the network, tunnels them to another location, and retransmits them into the network at that location
Examples of Attacks that can Collaborate

- Replication attacks
  - Adversaries can insert additional replicated hostile nodes into the network after obtaining some secret information from the captured nodes or by infiltration. Sybil attack is one form of replicated attacks.

- Sybil attacks
  - A malicious user obtains multiple fake identities and pretends to be multiple, distinct nodes in the system. This way the malicious nodes can control the decisions of the system, especially if the decision process involves voting or any other type of collaboration.
Vulnerabilities and Attacks in Ad Hoc Networks (cont’d)

Examples of Attacks that can Collaborate

- **Rushing attacks**
  - An attacker disseminates a malicious control messages fast enough to block legitimate messages that arrive later (uses the fact that only the first message received by a node is used, preventing loops)

- **Malicious flooding**
  - A bad node floods the network or a specific target node with data or control messages
Example of Combined attacks

- To combat joint attacks

Example:
- Node A deceives node S informing it has shortest path to D
- A forwards any packets to X
- X sets up a tunnel to Y
- Any further packet will go through the tunnel
- In tunnel, packets can be selectively dropped or tampered with
Characterization/classification of attacks

- Groups by target goals or typical kinds of attacks
  - Paralyzing the network activities
  - Partitioning the network
  - Taking an unfair share of the network resources
  - Distributed passive attacks

- This grouping facilitates the development of mechanisms for characterization/classification
Preliminary ideas on characterizing/classifying CAs

- To identify the key features of combined attacks
- To use signal processing technique and machine learning technique to characterize/classify attacks
  - Wavelet transform for anomaly detection
  - Fuzzy logic for decision making process
Preliminary ideas on characterizing/classifying CAs (Cont’d)

- Real-time classification and defense
Implementation issues

- Energy consumption has to be considered
- Amount of control messages among the detection and defense mechanism is an issue
  - Bandwidth and energy concerns
- Centralized model is only feasible in semi-static networks
Intrusion Detection in Each Node

- Semi-centralized Approach
- The Wavelet-based system detects anomalies in each node
- Depending on the level of the anomaly, a packet is transmitted to the coordinator node
Detection and Response at Coordinator Node

- Incoming packets are inspected and the classification parameters are handed to the fuzzy engine.
- Parameters are mapped to the membership functions.
- Black list management is crucial to the efficiency of the system.
Experimental Study [Initial Evaluation]

- **Goal**
  - Study the effect of responsiveness of attack detection systems on the performance of the network
  - Study the effect of a collaborative attack on the network

- **Scenario**
  - **Low mobility**- like campus/library/office networks
  - **OPNET** simulator
  - **Simulation Period**: 900 Sec (removing the first 100Sec as a warm-up period of 1000 seconds of simulation)
  - We reset the attack every 200 seconds to eliminate the effect of simulation period on the results
More Details...

- Topology of 19 nodes (slide 10)
- DSR routing protocol
- Transmission Range: 250m

Parameters
- Reaction time (detection time + response time)
  - Detection time
  - Response time
- Case of TCP and UDP as transport layers

Performance Metrics
- Packet Delivery Ratio (PDR)
- Normalized Load or Overhead (OH)
- Average End to End Delay
Scenario I

- **Goal**: Analyzing the effect of wormhole attack on the mobile wireless network
Packet Delivery Ratio (PDR) and Throughput

- The main reason for drop in PDR metric is the loss of packet in the wormhole.
- Impact of reaction time on performance is high, implying that coordinator node must get fast feedback from other nodes and react properly and quickly.
- UDP achieves higher PDR, but drops more packets, resulting in lower throughput.
Overhead (OH) and End to End Delay

- TCP has higher OH and Delay due to the retransmission control
Scenario II

- **Goal**: Demonstrating the power of collaborative attacks which interrupts the operations of network

- **Fact**: almost all learning based attack detection schemes need a time period to discover the attack

- **Scenario**
  - Three collaborator attackers
  - Idea of transferring the attack control to the next collaborator before being detected
  - Attack detection time: 20Sec
  - Attack control transfer time: 7Sec

- We observed a **total failure** in the operation of the network using this simple collaborative strategy
Analyzing the results of Simulation

- This study gives us a good measure of acceptable level of responsiveness
  - This measure can be used to select appropriate mechanisms in detection and classification phases
- The second scenario highlights the power of collaborative attacks to bypass the detection mechanism effectively and interrupt the network operation without being detected easily.
- More sophisticated and effective adaptive approaches are needed to deal with collaborative attacks
Conclusions and Outlook

- Collaborative attacks is a serious threat to ad hoc nets
- **Reaction time** has to be bound to an acceptable level to guaranteed responsiveness
- Collaborative response appears to be feasible
- Intelligent systems to characterize and classify collaboration are an actual need
Future Work

- More parameters have to be tested, including proper membership functions in the fuzzy logic mechanism
- Evaluations: Energy consumption, efficiency, processing
Defending against Collaborative Packet Drop Attacks on MANETs

Weichao Wang
SIS Dept
UNC Charlotte

Bharat Bhargava
CS Dept
Purdue University

Mark Linderman
Rome Lab
Air Force RL
Organization of Presentation

• Problem Statement
• Related Work
• REAct System and Its Vulnerability
• Our Approach
• Analysis
• Conclusion
Problem Statement

Packet drop attacks put severe threats to Ad Hoc network performance and safety

- Directly impact the parameters such as packet delivery ratio
- Will impact security mechanisms such as distributed node behavior monitoring
- Different approaches have been proposed
  - Vulnerable to collaborative attacks
  - Have strong assumptions of the nodes
Problem Statement

Many research efforts focus on individual attackers

• The effectiveness of detection methods will be weakened under collaborative attacks
  • E.g., in “watchdog”, multiple malicious nodes can provide fake evidences to support each other’s innocence
  • In wormhole and Sybil attacks, malicious nodes may share keys to hide their real identities
Problem Statement

In this paper, we focus on collaborative packet drop attacks. Why?

• Secure and robust data delivery is a top priority for many applications
• The proposed approach can be achieved as a reactive method: reduce overhead during normal operations
• Can be applied in parallel to secure routing
Related Work

Detecting packet drop attacks

• Audit based approaches
  • Whether or not the next hop forward the packets
  • Use both first hand and second hand evidences
• Problems:
  • Energy consumption of eavesdropping
  • Can be cheated by directional antenna
  • Authenticity of the evidence
• Incentive based approaches
  • Nuggets and credits
• Multi-hop acknowledgement
Related Work

Collaborative attacks and detection

• Classification of the collaborative attacks
• Collusion attack model on secure routing protocols
• Collaborative attacks on key management in MANET
• Detection mechanisms:
  • Collaborative IDS systems
  • Ideas from immune systems
  • Byzantine behavior based detection
REAct system and vulnerability

REAct system:

• Proposed by researchers in Univ of Arizona
• Published in ACM WiSec 2009
• Random audit based detector of packet drop
• A reactive approach: will be activated only when something bad happens

Assumptions:
• At least two node disjoint paths b/w any pair of nodes
• Know the identity of the intermediate nodes
• Pair-wise keys b/w the source and the intermediate nodes
REAct system and vulnerability

Working procedure of REAct

• Destination detects the drop in packet arriving rate and notifies the source

• Source randomly selects an intermediate node and asks it to generate a behavioral proof of the received packets

• Intermediate node constructs a bloom filter using these packets

• Source compares the bloom filter to its own value
  • If match: the attacker is after the intermediate node
  • Otherwise, it is before the intermediate node

• Repeat the procedure until the bad link is located
Example of REAct: the source selects $n_4$ to be the first audited node. $N_4$ generates the correct bloom filter, so the attacker is between $n_4$ and $D$. 
Collaborative attacks on REAct

N1 and n4 are collusive attackers. N1 discards the packets but delivers the bloom filter to n4. Now the source will think that the attacker is between n4 and D.

Why REAct is vulnerable to this attack: the source can verify the bloom filter, but not the generator of the filter.
Proposed approach

Assumptions:

- Source shares a different secret key and a different random number with every intermediate node.
- All nodes in the network agree on a hash function \( h() \).
- There are multiple attackers in the network:
  - They share their secret keys and random numbers.
  - Attackers have their own communication channel.
  - An attacker can impersonate other attackers.
Proposed approach

Hash based approach:

• Every node will add a fingerprint into the packet

S1 sends out the packet to n1:

\[ S \rightarrow n1: (S, D, \text{data packet, random number } t0) \]

Node n1 will combine the received packet and its random number \( r1 \) to calculate the new fingerprint:

\[ t1 = h( r1 | | S | | D | | \text{data packet} | | t0 | | r1 ) \]

\[ n1 \rightarrow n2: (S, D, \text{data packet, } t1 ) \]

The audited node will generate the bloom filter based on the data packets and the fingerprints

The source will generate its own bloom filter and compare it to the value of the audited node
Proposed approach

Why our approach is safe

• The node behavioral proofs in our proposed approach contain information from both the data packets and the intermediate nodes.

• **Theorem 1.** If node $n_i$ correctly generates the value $t_i$, then all innocent nodes in the path before $n_i$ (including $n_i$) must have correctly received the data packet selected by $S$. 
Proposed approach

Why our approach is safe

• The ordered hash calculations guarantee that any update, insertion, and deletion operations to the sequence of forwarding nodes will be detected.

• Therefore, we have:
  • if the behavioral proof passes the test of S, the suspicious set will be reduced to \( \{ni, ni+1, \ldots, D\} \)
  • if the behavioral proof fails the test of S, the suspicious set will be reduced to \( \{S, n1, \ldots, ni\} \)
Discussion

- Indistinguishable audit packets
  - The malicious node should not tell the difference between the data packets and audited packets
  - The source will attach a random number to every data packet
- Reducing computation overhead
  - A hash function needs 20 machine cycles to process one byte
  - We can choose a part of the bytes in the packet to generate the fingerprint. In this way, we can balance the overhead and the detection capability.
Discussion

• Security of the proposed approach
  • The hash function is easy to compute: very hard to conduct DoS attacks on our approach
  • It is hard for attackers to generate fake fingerprint: they have to have a non-negligible advantage in breaking the hash function
  • The attackers will adjust their behavior to avoid detection
    • The source may choose multiple nodes to be audited at the same time
    • The source should adopt a random pattern to determine the audited nodes
Conclusion

• Previous approach is vulnerable to collaborative attacks
• Propose a new mechanism for nodes to generate behavioral proofs
  • Hash based packet commitment
  • Contain both contents of the packets and information of the forwarding paths
  • Introduce limited computation and communication overhead
• Extensions:
  • Investigate other collaborative attacks
  • Integrate our detection method with secure routing protocols
Thanks. Questions?