Alibi: A framework for identifying insider-based jamming attacks in multi-channel wireless networks

Hoang Nguyen, Thadpong Pongthawornkamol, Klara Nahrstedt
{hnguyen5, tpongth2, klara}@illinois.edu

Homepage: http://sanjose.cs.uiuc.edu/alibi

1. Introduction

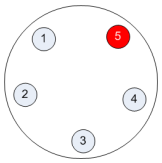
- Radio jamming vs. Spread spectrum
- "Shared secret" in FHSS, DSSS
- Knowledge of shared secrets = effective jamming

2. Problem Description

- Insider-based jammers = compromised nodes
- Identifying compromised nodes doing stealthy jamming attacks (**non-colluding** only)
- Identification vs. Detection

3. System Model

- Single-hop, N nodes with single transceiver, C channels
- Non-negligible tx-rx/rx-tx turnaround time and channel switching delay



1	2	3	4	5
5	1	2	3	4
4	5	1	2	3

TDMA-like scheduling

4. Challenges

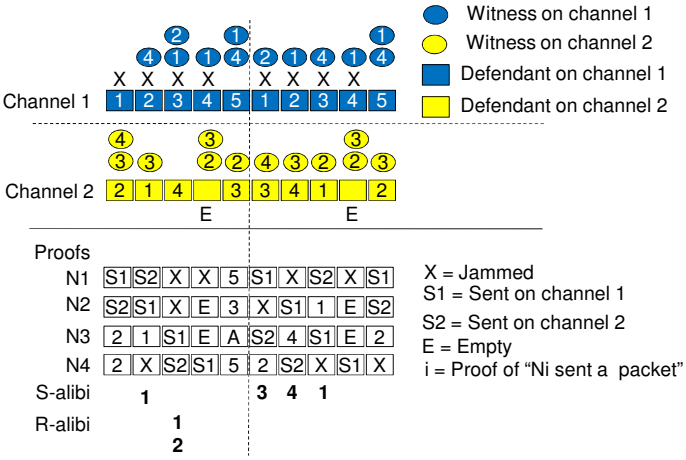
- No identity information in jammed packets
- Jammed packet ~ Collided packet ~ Corrupted packet
- Multiple attackers
- Possible slander attacks (i.e. making good nodes look bad)

5. Alibi framework

- Alibi framework to deal with insider-based jammers

  - Alibi of nodes = proof of nodes doing <u>legitimate actions</u> when jamming actions happen
- <u>Defendants</u> = nodes doing legitimate actions
- <u>Witnesses</u> = nodes observing defendants
- <u>Proofs</u> = time and channel information observed by witnesses
- <u>Alibi</u> = combination of proofs proving defendants' honesty
- Sending-based alibi vs. receiving-based alibis

6. An example



7. Lossy channel and collisions

- Lossy channels and collisions can cause "<u>false</u>" alibis
- However, honest nodes can obtain <u>both "true" and "false" alibis</u> and thus more alibis than attackers
- Sequential hypothesis testing to differentiate attackers and honest nodes according to the alibi rate

8. Non-colluding multiple attackers

- A jamming action by one attacker can <u>accidentally</u> help some other attackers to get an alibi
- The solution is similar to the case of lossy channels

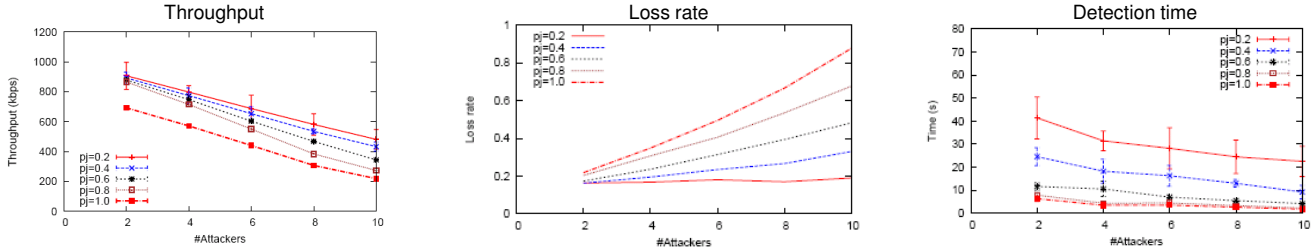
9. Attacks on alibi scheme

- Slander attacks: Attackers stop jamming whenever victim nodes are defendant (addressed in tech. report)
- Colluding attacks: Attackers can create fake alibis or exchange true alibis (addressed in tech. report)

11. Conclusions & Future work

- Alibi concept in the context of jamming
- Complement to current IDS approach: collecting good behaviors of nodes
- Multiple-hop topology, distributed detection and mote implementation

10. Simulation Results



Information Trust INSTITUTE
UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN