

Background

Colluding and coordinated attacks in MANETs:

- ❑ Attackers provide a degree of consistency that may foil detection mechanisms by corroborating each other's lies.
- ❑ Coordinated attacks are typically multi-stage and dynamic.
- ❑ Attackers are 'intelligent': they can detect the defenders' detection schemes and defense strategies and re-plan in real-time as to how to adjust their strategies.

Proposed methods:

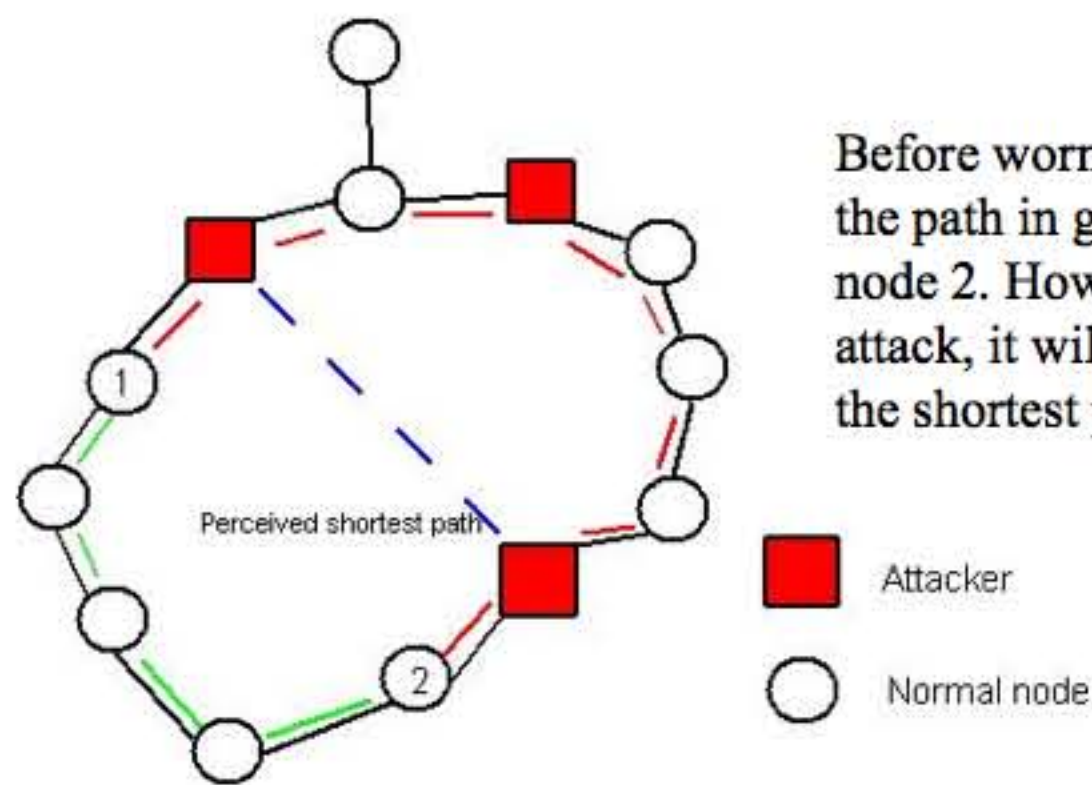
- ❑ model-based distributed detection and classification;
- ❑ spatio-temporal methods for detection and classification;
- ❑ learning attack strategies and applying game theoretic methods

We study one type of colluding attacks: wormhole attacks

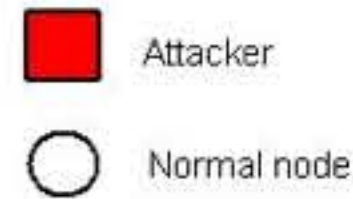
- ❑ Colluding nodes create the illusion that two remote regions of a MANET are directly connected through nodes that appear to be neighbors but are actually distant from one another.
- ❑ Threats of wormhole attack
 - Undermines the shortest path routing calculations;
 - Creates artificial traffic choke points that can be utilized at an opportune future time to degrade and analyze the traffic stream.

In-band Wormhole

Prior research on wormholes in MANETs has concentrated primarily on out-of-band wormholes. Our work deals with in-band wormholes.



Before wormhole attack, node 1 chooses the path in green as the shortest path to node 2. However, after the wormhole attack, it will perceive the path in red as the shortest path to node 2.



In-band wormhole	Out-of band wormhole
Connect purported neighbors via multi-hop tunnels through the primary link layer, do not need additional hardware, more likely to be used by adversaries	Connect purported neighbors via a separate communication mechanism, such as a wire line network, may need additional specialized hardware
Continually consume network capacity	Actually add channel capacity to network
Countermeasures not depend on its mechanism	Countermeasures depend on its mechanism

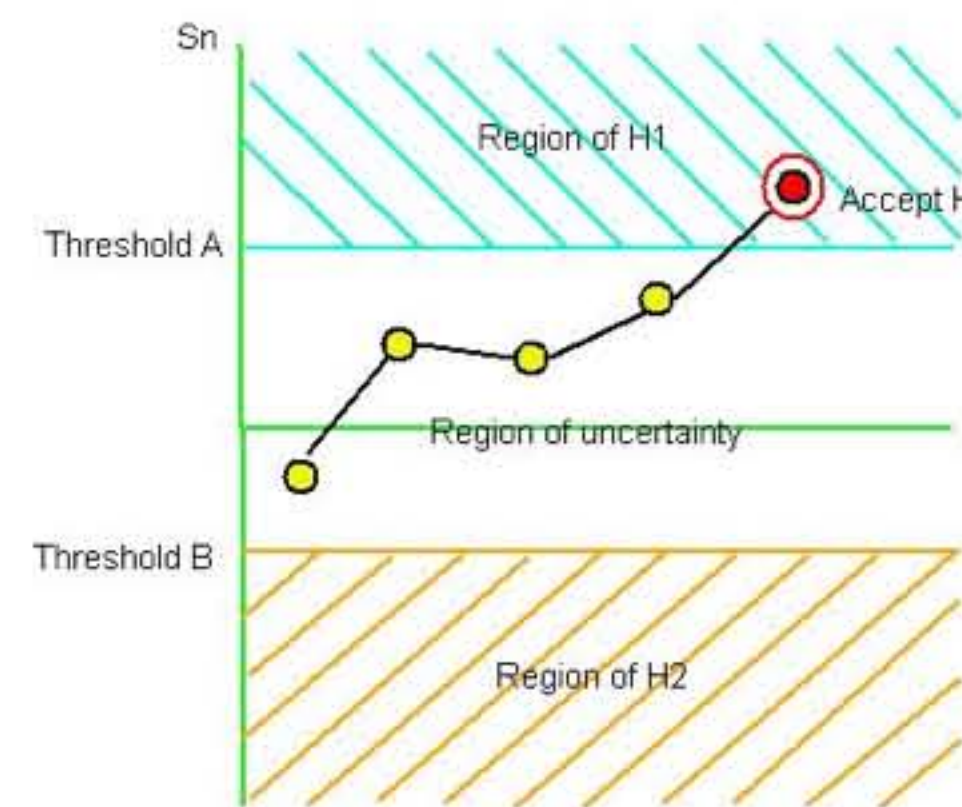
Sequential Detection

Sequential Probability Ratio Test (SPRT)

- ✓ For given values of the probability of false alarm and missed detection, SPRT minimizes average number of required observations to reach a decision among all sequential or non-sequential tests.
- ✓ Given a sequential observations x_1, x_2, \dots, x_n , SPRT decision parameter is

$$S_n = \log(L_n) = \log \frac{f(x_1, x_2, \dots, x_n | H_1)}{f(x_1, x_2, \dots, x_n | H_0)}$$

- ✓ The decision criterion is: if $S_n \geq A$, choose H_1 ; if $S_n \leq B$, choose H_2 ; otherwise SPRT continues to collect data since there are not enough data to make a reliable decision.



SPRT Test

Voting

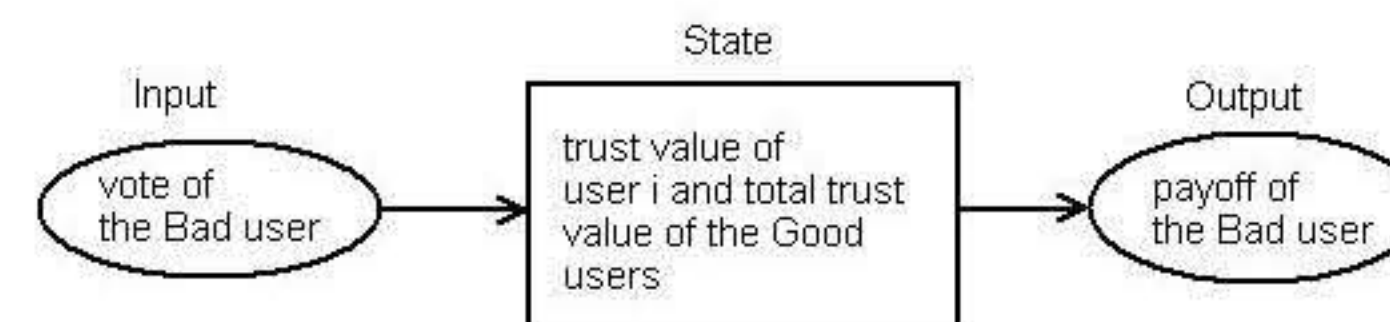
Opportunity voting with the majority rule:

- To prevent false accusation, more than one detection decisions are required. Each decision is regarded as a vote.
- Trust mechanism: punish users who often vote in minority and reward those often in the majority by reducing or increasing the weight of their votes respectively.

Attackers' dilemma:

- voting against a large sum of trust values vs. waiting for future time when it may be more convenient to swing the vote.
- We can view the above as a stochastic game, and use stochastic dynamic programming to solve it.

Stochastic Dynamic Programming



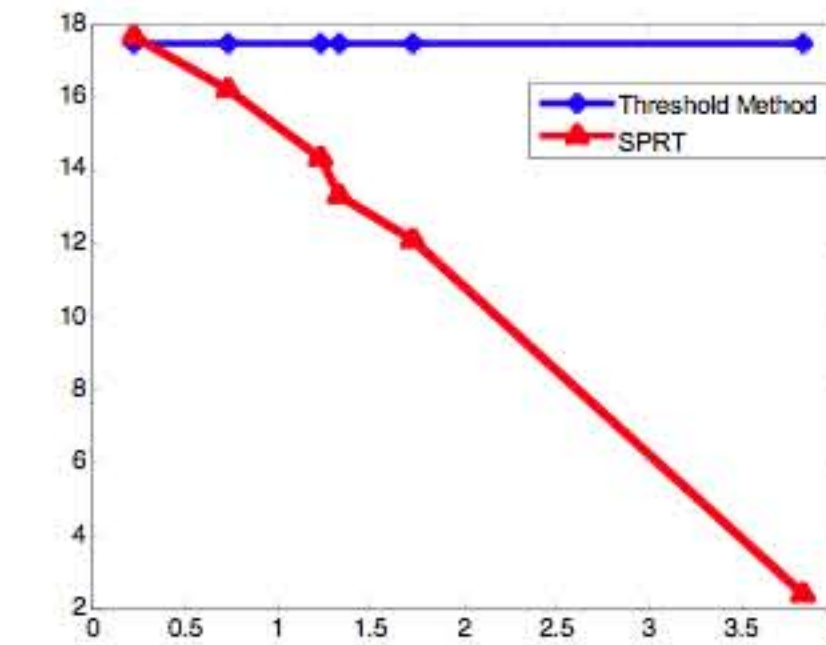
Testing

Network testbeds:

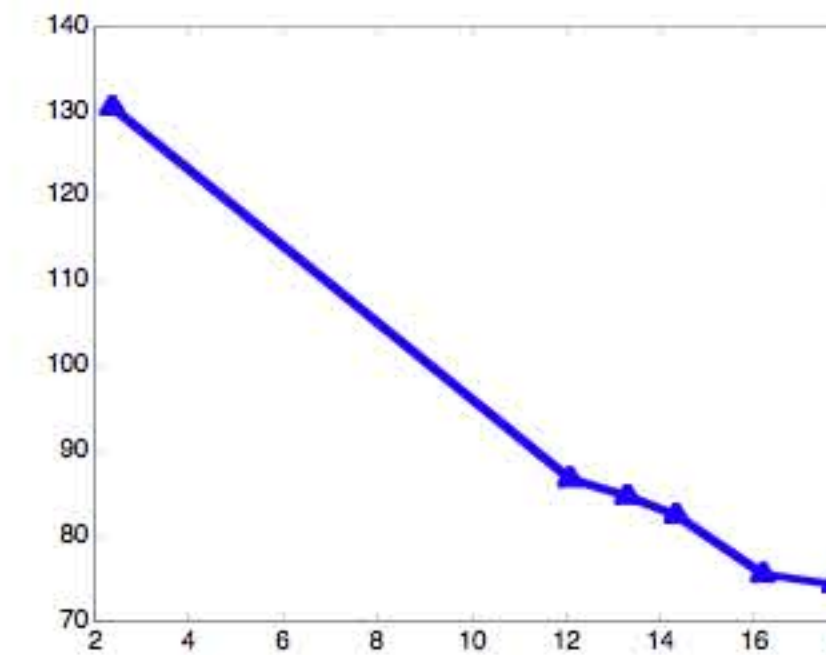
- NRL's Mobile Ad-hoc Network Emulator (MANE) in ARL;
- 48 test nodes and MANE servers emulating node positions, mobility, and radio connectivity;
- Each test node runs the Fedora Core 3 operating system and the OLSR daemon developed at University of Oslo.

Test scenarios:

- Two nodes with wide horizontal spacing are selected as attack nodes;
- Round trip delays of probes are used as the measurements;
- Comparison: simple threshold method.



False alarm rate vs. threshold A



Delay time vs. false alarm rate

Future Work

- ❑ Apply game theory to min-max robust detection which finds the worst case results given uncertainty.
- ❑ Investigate more complex scenarios and find the least favorable adversarial setting and estimate the corresponding detection delay.
- ❑ Make the user votes not just binary but real numbers from 0 to 1, in order to include partial detection.

Acknowledgement

This work is sponsored by the U.S. Army Research Laboratory under cooperative agreement DAAD19-01-2-0011.