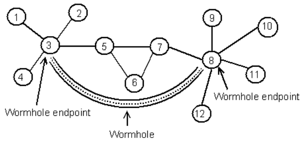
Detection of In-band Wormholes Using Sequential Change Detection Algorithms

Shanshan Zheng, Tao Jiang, John. S. Baras

Background

Wormhole Attacks in Wireless Ad Hoc Networks:



❑ Malicious nodes 3 and 8 create the illusion that they are one-hop neighbors by using a covert communication tunnel.

❑ Based on the tunneling scheme, wormholes can be classified as *in-band* wormholes and *out-band* wormholes.

In-band wormhole	Out-band wormhole
Purported neighbors are connected via multi-hop tunnels over existing wireless medium, do not need additional hardware, more likely to be used by adversaries	Purported neighbors are connected using an external communication medium, (e.g., a wired link), may need additional specialized hardware
consume network capacity	add channel capacity to network
Countermeasures not depend on attack mechanism	Countermeasures depend on attack mechanism

Our work deals with in-band wormholes.

❑ Threats of the wormhole attack

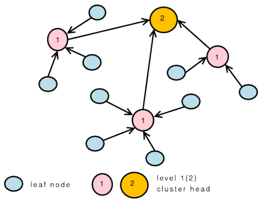
- Undermines shortest path routing calculations
- Create artificial traffic choke points under control of the attacker

Framework of Our Detection Scheme

❑ Motivation

A in-band wormhole attack leads an abrupt change in the transmission delay along a path ⟹ formulate in-band wormhole detection as a sequential change detection problem

❑ Detection Scheme



Leaf nodes: collect 3-hop transmission delay, make individual inferences, send them to the cluster head

Cluster head: correlates individual inferences it receives to make final decision and locate the wormhole

Sequential Change Detection Algorithms for the Leaf Nodes

❑ Two *Sequential Change Detection algorithms* are proposed to help the leaf node make individual inferences about whether there is a wormhole or not

- ➢ Non-parametric Cumulative Sum (NP-CUSUM)
- ➢ Repeated Sequential Probability Ratio Test (R-SPRT)

❖ *NP-CUSUM*

- Used when an attack model is not available (e.g., network topology changes quickly, makes it difficult to estimate the distributions of the path delay measurement)
- Statistic, decision rule and stopping time for NP-CUSUM:

Statistic: $g_n = (g_{n-1} + x_n - c)^+$

Decision rule: $d(n) = \begin{cases} 1, & \text{if } g_n \geq h \\ 0, & \text{if } g_n < h \end{cases}$

Stopping time: $\tau = \min\{k : d(k) = 1\}$

x_n is the delay measurement obtained by the leaf node at time n, h is a threshold and c is some pre-defined constant

❖ *R-SPRT*

- Used when an attack model is available
- Statistic, decision rule and stopping time for *a single SPRT*:

Statistic: $S_n = \ln \dfrac{f_1(x_1, x_2, \cdots, x_n)}{f_0(x_1, x_2, \cdots, x_n)}$

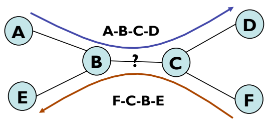
Decision rule: $d(n) = \begin{cases} 1, & \text{if } S_n \geq B \\ 0, & \text{if } S_n \leq A \\ \text{defer decision}, & \text{if } A < S_n < B \end{cases}$

Stopping time: $\tau = \min\{k : (S_k \geq B) \cup (S_k \leq A)\}$

- In *R-SPRT*, the single SPRT is restarted whenever a ‘0’ decision is made. This setup enables continuous monitoring of wormhole detection

Correlation Algorithm for the Cluster Head

❑ For the cluster head, locating a wormhole requires at least two anomalous observations with a common intersecting link but disjoint end nodes.



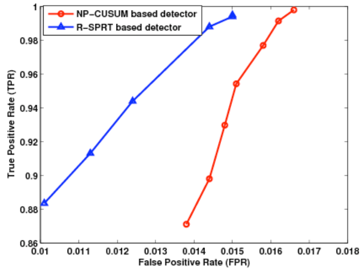
Simulations

❑ Simulation setting:

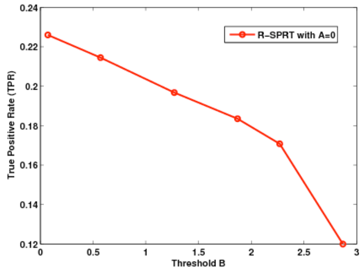
- ❖ NS-2 simulator, OLSR based wireless ad hoc network
- ❖ 50 nodes in a 1000x1000 square field
- ❖ 2 attackers form an 8-hop wormhole

❑ Some results:

❖ Performance of an NP-CUSUM based detector and a R-SPRT based detection



❖ Performance of a R-SPRT based detector using improper training set



- Better performance of R-SPRT than NP-CUSUM comes at the cost of more attack information and higher computational complexity
- Using improper training data for R-SPRT can seriously degrade its performance

Acknowledgement

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