CS 6910-ACIS
Wormhole attack effects in various routing protocols
Yih Chun Hu, Andrian Perrig
Carnegie Mellon University
David B Johnson-Rice University
Presented by- Akshitha Guduru

Department of Computer Science
Western Michigan University
Instructor: Prof. Leszek T. Lilien, Fall 2006
Wormhole attack

- A malicious node records control and data transfer at one location and tunnels it to a colluding node, which replays it locally.

- Possible even if attacker has not compromised any hosts
Effects in various routing protocols

- DSR - prevents any routes apart from wormhole to be discovered
- Routing protocol fails to find routes in:
  - TBRPF - Topology broadcast based on Reverse path forwarding
  - OLSR - Optimized link state routing
Assumptions

- Bi-directional links
- Wireless network may drop, corrupt, duplicate or re-order packets
- Nodes in ad-hoc network may be resource constrained
- Node can obtain an authenticated key for any other node
What is packet leash?

A mechanism to detect and defend against wormhole attacks

Leash is any information added to a packet designed to restrict packets maximum allowed transmission distance.
Types of packet leashes

- Geographical Leashes: Ensures that the recipient of the packet is within a certain distance from sender

- Temporal Leashes: Ensures that packet has an upper bound on its lifetime, restricting the maximum travel distance
Constructing geographical leash

- Geographical leash: Each node must know its own location
- All nodes must have loosely synchronized clocks
- RSA authentication can be used to allow a receiver to authenticate the location and timestamp
Explanation for geographical leash

- Sender node includes its own location $p_s$ and the time at which the packet is sent $t_s$.
- The receiving node compares this with its location $p_r$ and the time when it received the packet $t_r$.
- If the clocks are synchronized to a difference of ‘D’ and ‘v’ is an upper bound on the velocity of any node, the receiver can compute the distance $d_{sr}$. 
Constructing temporal leash

- Tightly synchronized clocks such that maximum difference is $d$
- Value of ‘$d$’ is known by all known nodes
- Includes expiration time for each node
Explanation for temporal leash

- Sender includes time at which it sent the packet $t_s$
- The receiver node compares this value to the time at which it received the packet $t_r$
- Receiver can detect if the packet traveled too far based on the transmission distance
- Sender can also set an expiration time $t_e$ after which the receiver should not accept the packet.
What is TIK?

- TIK stands for TESLA (Timed efficient stream loss-tolerant authentication) with Instant key disclosure.
- Provides instant authentication and broadcast communication for temporal leashes in ad-hoc networks.
- Novel observation that a receiver can verify TESLA security condition
Temporal leash with TIK protocol

- We use a hash tree structure for more efficient authentication of values.
- To authenticate a sequence of values $v_0, v_1, \ldots, v_n$, these values are placed at leaf nodes of a binary tree.
- First the values are binded using a one way hash function $v_i' = H(v_i)$.
Merkle hash tree

Diagram:
- $m_p$
- $m_l$
- $m_r$
- $a_1$
- $b_1$
- $c_1$
- $d_1$
- $m_1$
- $m_2$
- $m_3$
- $m_4$
Derivation of tree values

- Let parent node be $m_p$ and its child nodes be $m_l$ and $m_r$
  
  $$m_r|m_p = H(m_l|m_r)$$

- Levels of the tree are computed recursively from leaf node to root node

- Root value is used to authenticate all leaf values
TIK Protocol Description

- TIK is based on efficient symmetric cryptographic primitives (MAC)
- It is an extension of TESLA broadcast authentication mechanism
- Requires accurate time synchronization between all communicating parties
- Each communicating node should know the public value for each sender node thereby enabling scalable distribution
Stages in TIK

- Sender setup: Sender uses a pseudo random function (PRF)
  - $F$ is the PRF and $M$ is the master key
- Set of keys are derived say $k_0, \ldots, k_i$ where $K_i = F_M(i)$
- Sender can efficiently access the keys in any order
- It is intractable for attacker to find the master key even if all key values are known
Continued...

- Receiver bootstrapping:
  we assume that all nodes have synchronized clocks
  Each receiver knows every senders hash tree

- Sending and verifying authenticated packets:
  Sender picks a key that is kept secret when the receiver gets the packet
Security benefits

- Ensures that wormhole attacker is not causing the signal to propagate farther than specified radius

- In geographical leash nodes detect tunneling across obstacles.

- Geographical leash when used in conjunction with digital signatures, can detect a malicious node and spread that information to other nodes.
Application in Oppnets

- A novel method in providing security against wormhole attacks.
- Can provide a means of multi hopping in a Bluetooth environment
- Ability to accurately measure location during disaster
Conclusions

- Wormhole can have devastating consequences on many proposed routing protocols
- TIK has computational and memory requirements that are satisfiable today
- Message authentication codes using TIK efficiently protects against spoofing, eavesdropping, wormhole attacks and ensures lot of freshness
- Implementable with current technologies
Packet leashes—A defense against wormhole attacks in wireless adhoc networks—
Yi Chun Hu, Adrian Perrig – Carnegie Mellon University
David.B.Johnson -Rice university