

# Security Topics in Networking and Distributed Systems

## CS 590D

### **Lecture 18: Wormhole and Flood Rushing Attacks**

Department of Computer Sciences  
Purdue University

# References

- Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks. Yih-Chun Hu, Adrian Perrig, David B. Johnson, INFOCOM 2003.
- Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols. Yih-Chun Hu, Adrian Perrig, and David B. Johnson WiSe 2003.



# Wormhole Attack

- Nodes act in collusion to inject false information
- Take a message and tunnel it to the colluding node in its payload
- Attacker records a packet at one location in the network, tunnels the packet to another location, and replays it there.
- It's a replay so authentication does not help

# Detecting Wormhole Attacks

- Main idea : add to a packet to restrict the packet's maximum allowed transmission distance (leash)
- **Geographical leash**: insures that the recipient of the packet is within a certain distance from the sender.
- **Temporal leash**: ensures that the packet has an upper bound of its lifetime (restricts the maximum travel distance).

# Geographical Leash

- Each nodes adds its location and timestamp on the packet
- Authentication techniques used to allow a receiver to authenticate the location and timestamp in the received packets
- Receiver verifies based on the location and timestamp on the packet, its own location and local time, and the speed of moving nodes, if the packet could indeed travel that distance

$$d \leq \|P_s - P_r\| + 2v \cdot (t_r - t_s + \epsilon) + \epsilon$$

# Geographical Leashes (cont.)

- Do not require tightly synchronized clocks
- can be used in conjunction with radio propagation model, allowing them to detect tunnels through obstacles
- Location info increases overhead on the packer
- require more general broadcast p and authentication mechanism
- can be used until maximum range is  $< 2v\epsilon$  ( $v$  is the maximum speed of any node and  $\epsilon$  is the difference between the clocks)

# Temporal Leash

- A temporal leash prevents the packet from travelling further than distance  $L$ ,  $L > \epsilon * c$ , where  $c$  is propagation speed of the wireless signal and  $\epsilon$  is the error in the clocks synchronization
- Sender includes the time on the packet, and receiver uses the time on the packet and the local time at the receiver to ensure above condition
- Receiver needs to authenticate the expiration time

# Authentication

- Digital signatures too expensive, also issues with the time when the packet is actually sent (802.11 has delays between each packet to avoid collisions)
- HMAC requires shared keys,  $n(n-1)/2$  keys in network with  $n$  nodes, not good for broadcast
- Separate HMAC can be avoided by multiple receivers sharing the same key, BUT it might allow colluding receivers to impersonate the sender
- TESLA, delays the release of the keys, not appropriate for this environment

# TIK Protocol

- Implements a temporal leash and enables the receiver to detect a wormhole attack
- Uses efficient symmetric cryptographic primitives
- Requires accurate time synchronization between all communicating parties
- Requires each communicating node to know just one public value for each sender

# TIK Protocol (cont.)

- Relies on Tesla, but the synchronized clocks allows them to release the key immediately
- Hash chains, then builds the Merkle authentication tree to be able to do efficient authentication
- Tricks to be able to store just part of the tree and not all tree (still require MB storage)

# Flood Rushing Attack

- On-demand routing protocols use duplicate suppression at each node: first RREQ that reaches a node is considered legitimate, next are discarded (all have the same identifier, higher identifiers denote new requests)
- Attacker disseminates RREQ quickly throughout the network suppressing any later legitimate RREQ

# Why is the Attack Possible?

- An attacker can send faster, by avoiding the delays that are part of the design of both routing and MAC (802.11b) protocols
- Attacker can send at a higher wireless transmission level
- An attacker can take advantage of a wormhole, to create flood rushing attacks, use the wormhole to rush the packets ahead of the normal flow

# What Protocol Are Vulnerable?

- On-demand unsecure (AODV, DSR) and secure (ARAN, Ariadne, etc) protocols
- Result: when under attack, the routing protocol will not be able to discover paths longer than 2 hops

# Rushing Attack Prevention (RAP)

- Use a secure mechanism to infer if a node is indeed a neighbor or not
- Use route delegation to allow other nodes to propagate flows (S-BGP like)
- Do not always forward the first flood, but wait for several and then use randomization to select one of the  $n$  floods and then send it

# Summary

- Many attacks in wireless network can be prevented by providing authentication, integrity and non-repudiation
- Requires some form of key management
- Wormholes and flood rushing can not be addressed by authentication only...

