Packet Leashes: A defence against Wormhole Attacks in Wireless Networks

Yih-Chun Hu, Adrian Perrig, David B. Johnson
Packet Leashes: A defence against Wormhole Attacks in Wireless Networks

Ahmet İlhan AYŞAN
Packet Leashes: A defence against Wormhole Attacks in Wireless Networks

Ahmet İlhan AYŞAN
The wormhole attack, an attacker records packets (or bits) at one location in the network, tunnels them (possibly selectively) to another location, and retransmits them there into the network.
• Radio frequency watermarking

• Intrusion Detection Approaches

• TESLA protocol

• IEEE 802.11i

• Medium Access Control Protocol
A **leash** is any information that is added to a packet designed to restrict the packet’s maximum allowed transmission distance.

- Geographical leashes (certain distance)
- Temporal leashes (lifetime)
Geographical leashes;

Sending nodes:
• Own location
• Time

Receiving nodes compare
• Own location
• Time
Temporal leashes:

- All nodes must have tightly synchronized clocks
- Based on the allowed maximum transmission distance and the speed of light
Packet Leashes: A defence against Wormhole Attacks in Wireless Networks

- HMAC \( \frac{(n^2-n)}{2} \) key requires
- Digital Signature \( n \) keys
Fig. 1. Merkle hash tree
• Sender Setup
• Receiver Bootstrapping
• Sending and Verifying Authenticated Packets
\[ K_i = \mathcal{F}_X(i) \]

\[ K_0, K_1, \ldots, K_{w-1}. \]
They assume that all nodes have

- synchronized clocks
- sender’s hash tree root \( m \),
- the associated parameters \( T_0 \)
- key expiration interval \( l \)
$S \rightarrow R : \langle \text{HMAC}_{K_i}(M), M, T, K_i \rangle$
The TIK Protocol

Fig. 2. Timing of a packet in transmission using TIK

\[ \leq (t_s + \tau + \Delta) \leq (T_i - \Delta) \]
They optimized MD5 hash code

- Pentium III 1 Ghz 1.3 million per seconds
- Compaq iPaq 3870 PocketPC 222,000 hashes per second
QUESTIONS?
Packet Leashes: A defence against Wormhole Attacks in Wireless Networks

Yih-Chun Hu, Adrian Perrig, David B. Johnson