Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks

Yih-Chun Hu (Carnegie Mellon University)
Adrian Perrig (Carnegie Mellon University)
David B. Johnson (Rice University)

Presented by: Jón T. Grétarsson
5 April, 2005

CS577: Advanced Computer Networks

Outline

- Introduction
- Problem Statement
- Related Work
- Assumptions and Notation
- Detecting Wormhole Attacks
- Temporal Leashes and the TIK Protocol
- Evaluation
- Conclusions

Introduction

The Authors

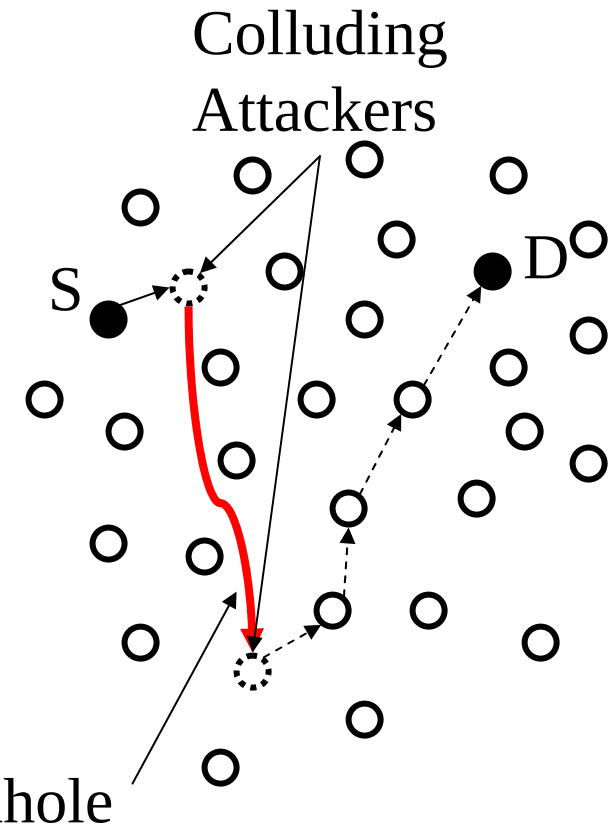
- Yih-Chun Hu
- Adrian Perrig
- David B. Johnson

Problem Statement

Wormholes!

Wormholes in MANET

- Packets are "tunneled" from one location to another
- If done reliably, no harm no foul
- If done selectively, much damage can be done!



The Threat

- Permanent Denial-of-Service
- Disruption to Routing Protocols
- Unauthorized Access

Related Work

Related Work

- RF Watermarking
- Intrusion Detection
- 802.11i

Assumptions and Notation

Assumptions & Notation

- Resource Constrained Nodes
- Existing key distribution system
- HMAC - a message authentication code used for authentication
- Bidirectional links are not necessary

Detecting Wormhole Attacks

Leashes

- Somehow restrict the transmission distance of the packet
- Geographical Leashes
- Temporal Leashes

Geographical Leashes

- Node Location
- Loosely Synchronized Clocks
- Bounded Velocity of packet
- d_{sr} is distance between two nodes
- Δ is error in time

$$d_{sr} \leq ||p_s - p_r|| + 2\nu \cdot (t_r - t_s + \Delta) + \delta$$

Temporal Leashes

- Requires tight synchronization of clocks
- MAC contention issues
- Digital signature scheme can guarantee timestamp

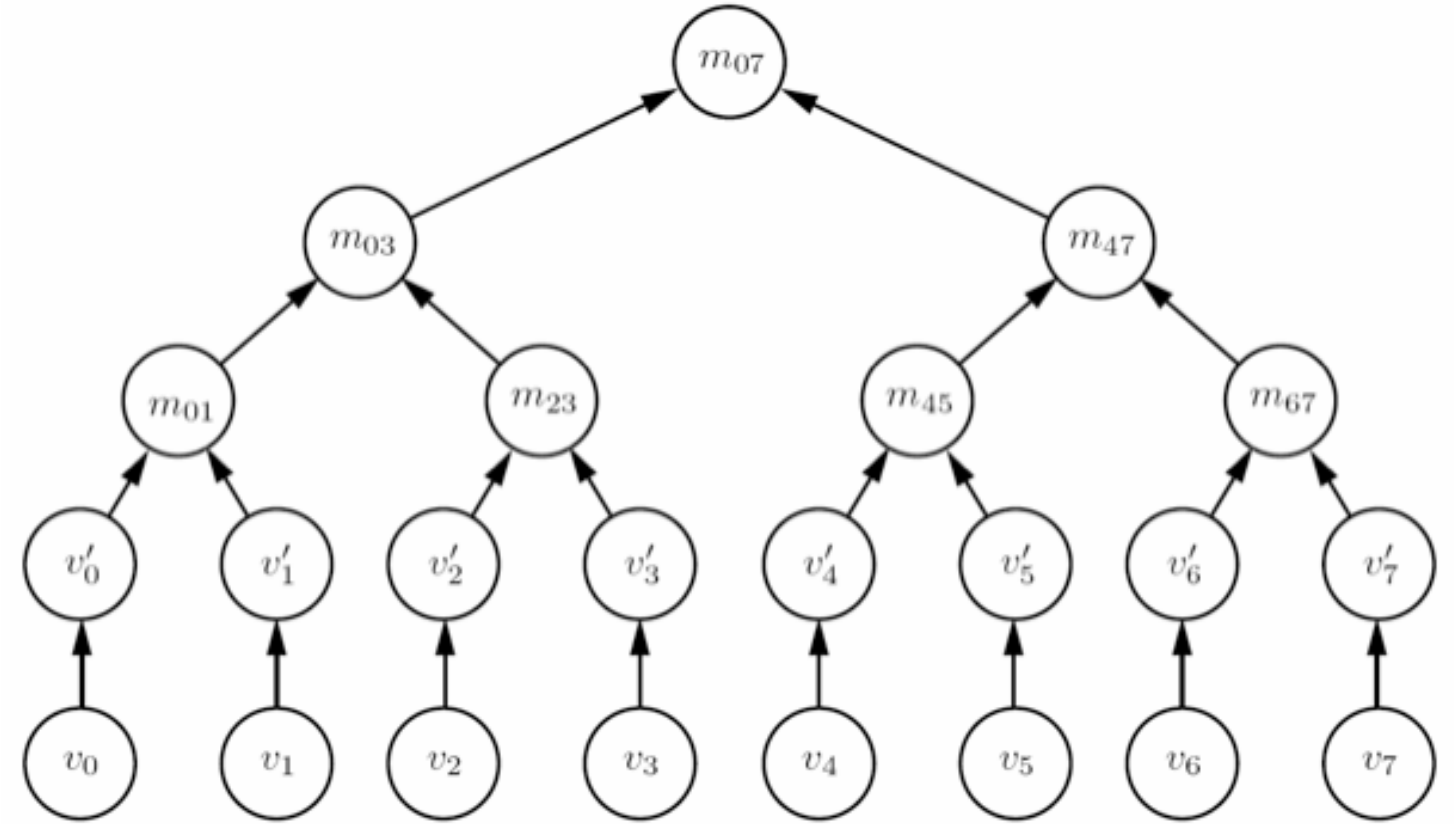
Temporal Leashes and the TIK Protocol

CS577: Advanced Computer Networks

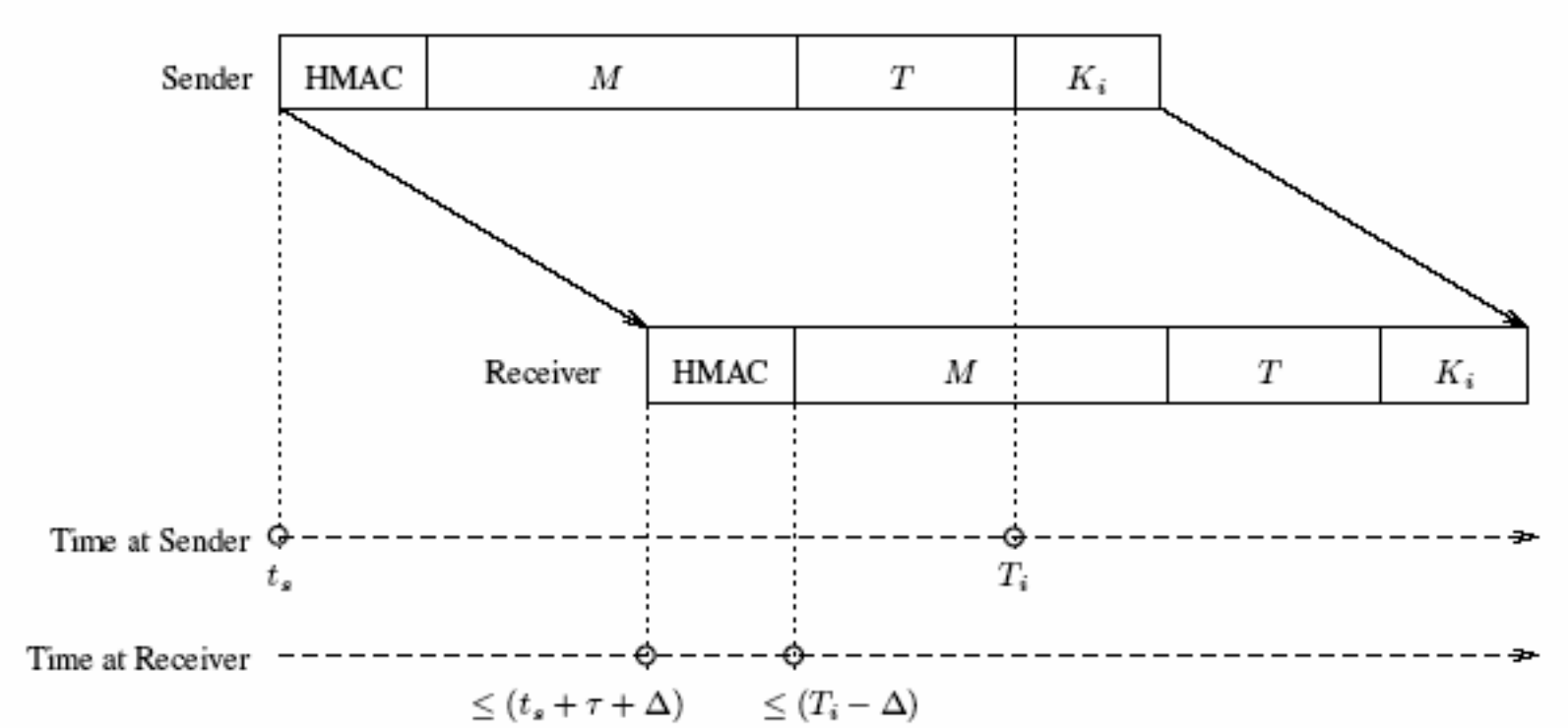
Authentication

- All information (timestamp, expiration, position) must be verified
- Traditional methods of verification are too expensive
- Merkle Hash Trees are the solution!

Merkle Hash Trees



TESLA with Instant Key Disclosure



Evaluation

How it was done

- Calculated required number of Hashes per second for algorithm
- Calculated computational power of portable devices

Results

- Suitable for laptops and PDA's, but not for resource scarce networks
- Not enough space to store the packet!

Conclusions

Conclusions

- Wormholes are dangerous! They can degrade performance of Mobile Ad Hoc routing algorithms
- Both Geographical and Temporal leashes can detect wormholes
- TIK is an implementation of Temporal leashes that can be used when there is sufficiently tight time synchronization
- TIK is not usable in resource-scarce networks

Questions? Comments?

Donations?

References

- Graphics borrowed from http://www.panda.uvic.ca/seminars/storage/PacketLeashes.ppt, http://www.ece.cmu.edu/~adrian/projects/ secure-routing/infocom2003.pdf