NC STATE UNIVERSITY Computer Science

LHAP: A Lightweight Hop-by-Hop Authentication Protocol for Ad-Hoc Networks

Review by: Pan Wang

April 23, 2003

Content Outline

- Background
  - Problem Statement
  - Related Work
- A lightweight Hop-by-Hop Authentication Protocol(LHAP)
  - One-way Key Chain
  - TESLA
  - Proposed Scheme
- Security and Performance Analysis
- Future Work
- Reference

NC STATE UNIVERSITY Computer Science

Background : *Problem Statement*

- The natures of wireless ad-hoc network
  - No preexisting infrastructure,
  - Lack well pre-defined relationship
  - Constrained resources
  - Mobility and routing
- Why we need a lightweight authentication mechanism?
  - Without access control, a network is very vulnerable
  - To against *spoofing, replay and resource consumption* attacks

Background: *Related Work*

- Previous work focus on following topics
  - Trust and key management
    - Threshold signature, KDC, probabilistic key sharing, group key
  - Secure routing
    - Identify the security vulnerabilities in AODV and DSR
    - SEAD protocol to secure DSDV, TESLA protocol to secure DSR
  - Intrusion detection
    - Intrusion detection and response mechanism, detecting selfish intermediate nodes

LHAP : *Overview*

- LHAP stands for *Lightweight Hop-by-Hop Authentication Protocol*
- LHAP provides network access control to prevent unauthorized nodes injecting traffic into network
- LHAP makes use of *one-way key* chains for traffic authentication and *TESLA* for bootstrapping trust.

LHAP: *Assumptions*

- Bidirectional wireless link
- A packet sent by a node is received by a neighboring node before a third node can replay the packet to it
- Each node has a public key signed by a trusted CA
- Each node has limited resources
- Loose time synchronization of the network
- TESLA is secure

LHAP : *One-way Key Chain*

- A one-way key chain is a chain of keys generated through repeatedly applying a one-way hash function on a random number. For instance, $K_{N-1}=F(K_N)$, $K_{N-2}=F(K_{N-1})$ … $K_0=F(K_1)$
- K_0 serves as a commitment to the entire chain to allow anybody to authenticate the following values of the chain.
- One-way key chain provides an efficient solution to authenticate messages in sequence.

LHAP : *TESLA*

- A symmetric-key cryptography based broadcast authentication protocol, proposed by Perrig et.al[2]
- The main idea of TESLA:
  - Sender attaches to each packet a MAC computed with a key *k* known only to itself.
  - The receiver buffers the received packet without being able to authenticate it.
  - A short while later, the sender disclose *k* and the receiver is able to authenticate the packet
- Implements One-way key chain and requires loose time synchronization and large storage.

LHAP : *Scheme Overview*

- Nodes use digital signatures to bootstrap a TESLA key chain to setup their trust relationships.
- TESLA keys are then used to provide authentic TRAFFIC keys.
- Nodes use TRAFFIC key chains to authenticate packets
- To maintain the trust relationship, a node broadcast KEYUPDATE message periodically.
- When a node does not receive a valid KEYUPDATE message from a neighbor within a TESLA interval, it terminates its trust of this neighbor.

LHAP : *Scheme Details*

- Trust Bootstrapping
  - When a node *A* wants to join the network, it pre-computes a one-way key chain and a TESLA key chain, and broadcast a JOIN message.

$$A \rightarrow *: Cert_A, Sign_A\{K_A^T(0) | K_A^F(0) | T_A^T(0) | T_A^F(0)\}$$

  - Neighbors unicasts the ACK message to *A*

$$B \rightarrow A: Cert_B, Sign_B\{K_B^T(0) | K_B^F(0) | T_B^T(0) | T_B^F(0)\}, MAC(K_B^T(i), K_B^F(j))$$

  - After Receiving and verifying TESLA key $K^T_B(i)$, A starts to forward valid traffic from B (Delay!!)

LHAP : *Scheme Details (Cont)*

- Traffic Authentication
  - When node *A* wants to send message *M*, it appends its next TRAFFIC key $K^F(i)$, to *M*, and broadcasts the packet.
  - Each receiving node verifies the authenticity of the packet by verifying the TRAFFIC key $K^F(i)$, based on the correspondent most recent TRAFFIC key $K^F(j)$ $(j<i)$ of *A*. If correct, forwards the packet and updates the TRAFFIC key.
  - A node only authenticates traffic packets from its directly neighbors

LHAP : *Scheme Details (Cont)*

- Trust Maintenance
  - Each node broadcasts an KEYUPDATE message to its neighbors periodically to maintain the trust relationship.
  - KEYUPDATE Message contains the most recently disclosed TRAFFIC key and is authenticated with the next TESLA key.

$$A \rightarrow *: A, K_A^T(i-1), MAC(K_A^T(i), K_A^F(j))$$

- Trust Termination
  - When a compromised node is detected
  - Not receiving KEYUPDATE message from a neighbor within a TESLA interval.

Security Analysis

- Outsider Attacks
  - Single attacker
    - Replay attack
    - *Solution: Trust Termination?*
  - Collaborative attackers
    - Wormhole attack
    - *Solution: GPS?*
  - Hidden Terminal
- Insider Attacks
  - Can't prevent
  - Needs other security protocols

Performance Analysis

- Light computational overhead
- Neglectable Latency
- Moderate traffic byte overhead
  - *The number of non-traffic bytes a node transmits per time unit*
- High traffic delivery ratio
  - *The fraction of traffic packets that a node accepts in all the packets it receives from its neighbors*

Future Work

- The potential work
  - How to against *Hello Attack (Bogus JOIN message)*
  - How to against wormhole attack
    - *TIK[3]?*
  - Find a synchronization-free solution with lightweight computation

Reference

- [1] S.Zhu,S.Xu,S.Setia and S.Jajodia, LHAP:A Lightweight Hop-by-Hop Authentication Protocol for Ad-hoc Networks, *To appear in ICDCS 2003 International Workshop on Mobile and Wireless Network (MWN 2003),* May 2003.
- [2]A. Perrig, R. Canetti, D. Song, and D. Tygar. Efficient and Secure Source Authentication for Multicast. *Proc. of NDSS 2001*
- [3]Y.Hu, A.Perrig and D.Johnson, Packet Leaches: A defense against Wormhole Attacks in Wireless Networks, *In Proceedings of IEEE INFOCOM 2003*, March 30-April 3, 2003, San Francisco, Califonia, USA