

Security Topics in Networking and Distributed Systems

CS 590D

Lecture 17: Authenticated Wireless Routing Protocols

Department of Computer Sciences
Purdue University

References

- Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks, Yih-Chun Hu, Adrian Perrig, and David B. Johnson. MobiCom 2002.
- A Secure Routing Protocol for Ad Hoc Networks, K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, and E. Belding-Royer, ICNP 2002.



Security Issues

- Attacks related to the RREQ
 - Drop the route request
 - Change the path on the packet and forward it
 - Generate false route request messages to burden the network
 - Spoof IP address and send requests
- Result: Nodes can add to a path and make it less probable that the “shortest path” is through them, or can shorten paths to make it more likely they are on paths
- Later, use this to either avoid forwarding traffic, or for traffic analysis, dropping packets

Security Issues

- Attacks related to RERR
 - Generate false route error messages
 - Drop route error messages
 - Spoof IP address and send error message for a valid route
- Attacker can continually tear down routes with false error messages, or by not reporting the error, packets will be lost.

Security Issues

- Attacks related to route replies
 - Suppress route replies
 - Send route replies with node as destination
 - Send false route replies, modify replies , false topology
 - Send higher sequence numbers

Security Issues

- Wormhole (tunneling) 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.

Security Issues

- 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

Security Issues

- Misbehaving nodes
 - Ad hoc networks maximize total network throughput by using all available nodes for routing and forwarding.
 - A node may misbehave by agreeing to forward the packet and then failing to do so because it is selfish, malicious or errors
 - How do you distinguish between the above 3 types?

The Need for Authentication

- Many of the attacks previously presented are possible because of lack of authentication and integrity
- End-to-end authentication vs hop-by-hop:
 - **End-to-end**: the destination is the one verifying the origin, no verification that the packet traveled indeed on the shortest path
 - **Hop-by-hop**: the destination and the intermediate nodes verify any previous sender, as well as origin

Providing Authentication

- Digital Signatures: requires PKI, expensive, provides also non-repudiation
- HMAC: requires a shared key, fast, does not provide non-repudiation
- Hash Chains; fast, requires additional storage, the anchor of the chain must be distributed in an authenticated manner (requires PKI)
- Tesla is a variant of hash chains

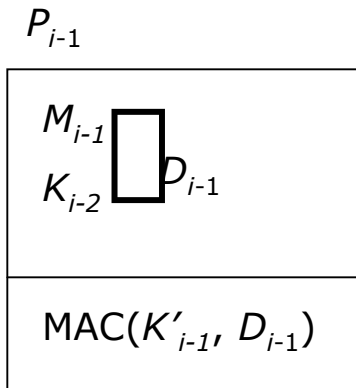
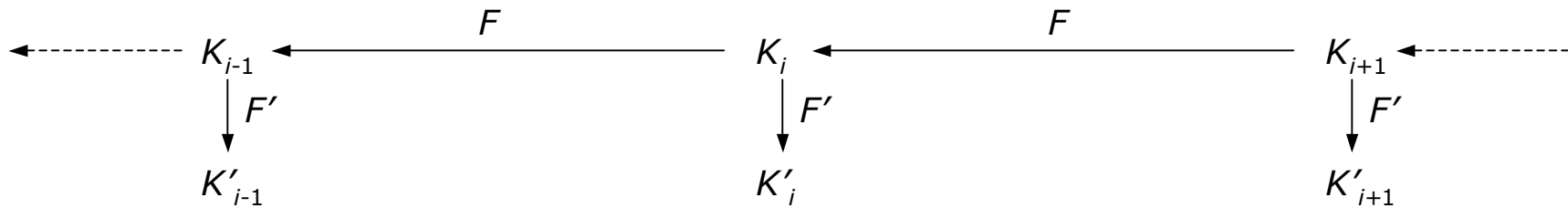
TESLA

- Broadcast authentication protocol: delayed key disclosure, requires clock synchronization
- One-way key chain: Each sender chooses random initial key K_N , generates one-way key chain as $K_i = H^{N-i}(K_N)$
- Schedule for disclosing keys: Each sender pre-determines the schedule, if i is the interval, then disclose K_i at $T_i = T_0 + i \cdot t$

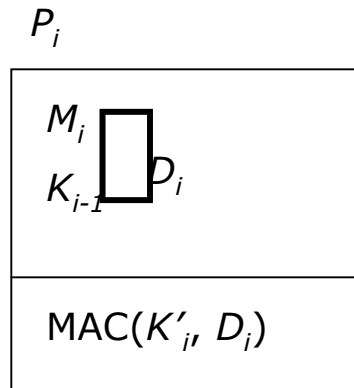
TESLA (cont.)

- Receiver can determine which key is disclosed based on loose time synchronization(ϵ)
- Sender selects K_i which will not be disclosed until $t + 2\epsilon$ time passes and add MAC using K_i
- Discard the packet if security condition fails
- TESLA security condition: K_i used to authenticate a packet cannot have been disclosed yet
- Requires buffering packets

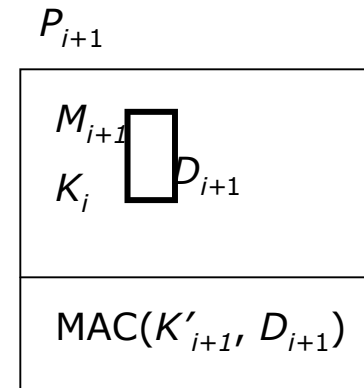
TESLA in Action



Authenticated

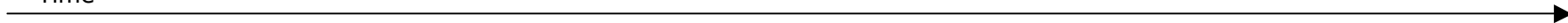


Authenticated



Can be authenticated after reception of P_{i+2}

Time



Ariadne

- Provides authentication for a simplified version of DSR (no optimizations)
- Uses a combination of shared keys, PKI and Tesla for authentication
- Authenticated nodes are trusted

Ariadne Assumptions

- Pairwise shared secret keys: set up $n(n+1) / 2$ keys for n nodes
- TESLA: set up shared secret keys between communicating nodes, distribute one authentic public TESLA key for each node
- Digital signatures: distribute one authentic public key for each node
- Each node has authentic element from Route Discovery chain(similar with TESLA)

Route Discovery

- Destination verifies the source of requests RREQ, source provides authentication by including a MAC with a shared key between source and destination
- Source authenticates nodes in Route Reply
- Target authenticates nodes in Route Request and return only legitimate paths (TESLA, digital signatures, standard MACs)
- Per-hop hashing: one-way hash functions to verify that no hop was omitted.

Route Maintenance

- A node generates a route error message ERR when delivery to next hop fails after a limited number of attempts
- To prevent unauthorized node from sending ERR messages, sender authenticates the ERR messages

ARAN (Authenticated Routing for Ad Hoc Networks)

- Provides: authentication, integrity, non-repudiation
- Uses certificates
- Some suggestion on how to do revocation
- States that no guarantee can be provided if a path is indeed the shortest path without using external mechanisms (for example timestamps).

ARAN

- Each intermediate node verifies previous signatures and replaces with its own (and certificate).
- Assumptions: intermediate nodes behave correctly, they check the signatures and replace with their own;
- Authenticated nodes are trusted

Route Maintenance

- ERR messages are signed and include the IP of the node issuing the message
- Includes protection against replay (timestamp)

Key Management

- Both Ariadne and ARAN require some form of key management
- Ariadne uses KDC to bootstrap the shared keys and the TESLA keys
- ARAN uses short-lived certificates which require the presence of a CA and revocation mechanisms
- How appropriate are the above solutions for ad hoc wireless networks?
- Other solutions: distributed CA, PGP-like public key infrastructure

Distributed CA

- Centralized CA model not appropriate for ad hoc wireless networks: revocation requires on-line PKI, single point of failure, vulnerability to node compromise
- Distributed CA Model, tolerates t faulty nodes
- Threshold signatures: signing needs coalition of $t+1$ correct nodes, while secret sharing prevents t malicious nodes from reconstructing CA private key
- *Zhou and Haas, Securing Ad Hoc Networks*

PGP Web of Trust

- Nodes issue certificates as in PGP
- Each node stores the certificates that it issued (**out-bound** certificates) and the certificates that other nodes issued for it (**in-bound** certificates)
- Each node builds up its own **out-bound** and **in-bound** subgraphs
- To establish secure communication, two nodes merge their subgraphs and check if they intersect
- *Hubaux, Capkun and Buttyán: The Quest for Security in Mobile Ad Hoc Networks, MobiHoc 2001*

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...

