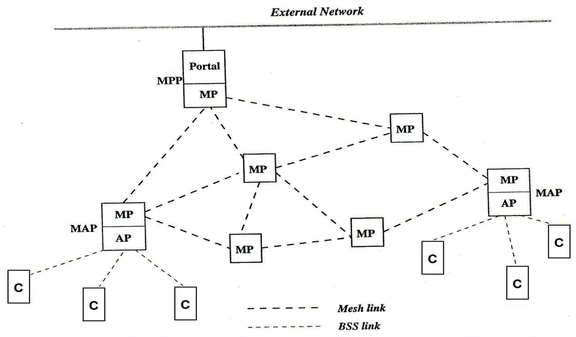
Fast Authentication for Mobile Devices in Wireless Mesh Networks

Celia Li and Uyen Trang Nguyen
Department of Computer Science and Engineering, York University
cli@cse.yorku.ca

Wireless Mesh Networks

- mesh points (MP). The MPs form a wireless *mesh backbone* to provide multi-hop connectivity from one mesh client (C) to another or to the Internet.
- mesh access points (MAP). A MAP is a mesh point that also works as an access point, i.e., connects mesh clients to the WMN.
- mesh point portal (MPP). A MPP is a mesh point that also works as a gateway connecting the WMN to the Internet.
- mesh clients (C). Mesh clients can be static (e.g., desktops, database servers) or mobile hosts (e.g., cell phone, PDAs).



Challenges of Authentication Protocols for WMNs

- Wireless channels have limited bandwidth and are error-prone.
- Wireless multi-hop routing drastically reduces network throughput.
- Shared broadcast medium is vulnerable to several types of attacks such as eavesdropping, jamming, and packet interception and modification.
- Distributed network architectures and operations make protocol design and implementation difficult.
- Mobile devices (e.g., cell phones, PDAs) have limited storage, computing capability and power supply. Mobility requires fast hand-off mechanisms.

Weaknesses of IEEE 802.11s Authentication

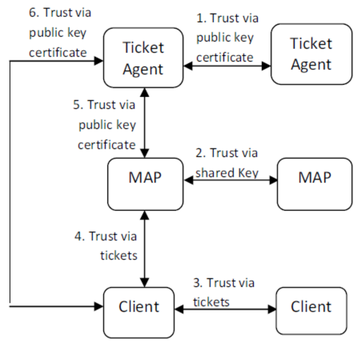
- IEEE 802.11s is a set of standards for WMNs.
- 802.11s authentication is a centralized scheme requiring a central authentication server, resulting in *long delay, low reliability, low scalability.*
- The current version of 802.11s does not specify any mechanisms/protocols that support fast hand-off.

Our Contributions [1]

- A new trust model for WMNs based upon which our proposed authentication protocols are designed.
- Ticket-based [2] authentication protocols that are efficient and resilient to attacks. No central authentication server is needed.
- Fast authentication from one access point to another during the hand-off process using tickets.

Trust Model

A trust model defines the trust relationships among network entities.



Tickets

A ticket [2] serves as a pass that a user submits to a system/network to allow it to verify the user's identity. We define three types of tickets:

- Client Ticket T_c

Client ID
Ticket Agent ID
Expiry Date
Client's Public Key
Signature Signed by Ticket Agent

- MAP Ticket T_R

Router ID
Ticket Agent ID
Expiry Date
Router's Public Key
Signature Signed by Ticket Agent

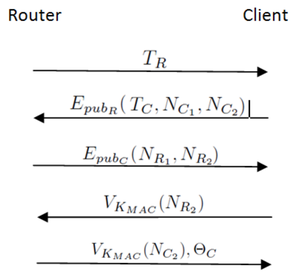
- Transfer Ticket θ_c

Router ID
Client ID
Ticket Agent ID
Expiry Date
MAC Algorithm
MAC Value

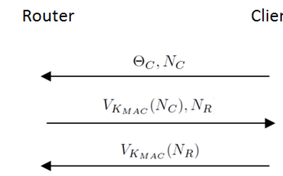
MAC: message authentication code

Fast Authentication Protocols

Login Authentication: executed when a client first logs in into the network.



Handover Authentication: executed when a client moves from one access point to another.



Notation	Description
C	Client
R	Mesh access point (MAP)
A	Ticket agent
I_x	ID number of entity x
Θ_C	Transfer ticket issued to a client
P_x	Public key issued to x
T_x	Ticket issued to x
τ_{exp}	Expiry date and time of a ticket
N_x	A nonce generated by x
Sig_x	Digital signature of entity x
MAC_{alg}	Type of MAC algorithm
$E_{pub_x}(m)$	Encryption of message m using x's public key
K_{MAC}	The key used to produce a message authentication code (Section 3.3.3)
$V_{K_{MAC}}(m)$	Message authentication code (MAC) resulting from the application of a MAC algorithm and a MAC key K_{MAC} on a message m

Performance Analysis

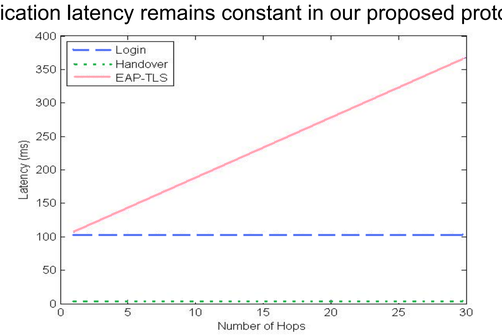
Computation and Communication Costs

Op.	Alg.	Time (ms)	Login	Handover	EAP-TLS
E_{pub}	RSA	1.42	1	0	1
D_{pub}	RSA	33.3	1	0	1
G_{sig}	ECDSA	11.6	1	0	1
V_{sig}	ECDSA	17.2	3	0	3
MAC	HMAC	0.015	1	6	1
Hash	SHA-1	0.009	1	0	3
Total computation cost			97.93ms	0.009ms	97.96ms
Number of messages			5	3	9
Authentication latency			97.93+5d	0.009+3d	97.96+9dh

EAP-TLS is the authentication protocol currently defined in IEEE 802.11s .

Authentication Latency

- EAP-TLS authentication latency increases as the hop count between the client and central authentication server increases.
- Authentication latency remains constant in our proposed protocols.



Conclusion

- We extend IEEE 802.11s standard to implement fast hand-off to support real-time applications such as voice-over-IP and audio/video conferencing.
- We propose a novel trust model that represents the trust relationships among the entities of a WMN, and new authentication protocols based on that model.
- A client and a mesh access point (MAP) mutually authenticate each other using one-hop communications. No central authentication server is required. Fast authentication for roaming from one MAP to another is supported by using tickets.
- Performance and security analyses show that our proposed authentication protocols are efficient and resilient to various kinds of attacks.

References:

[1] Celia Li and U.T. Nguyen, "Fast Authentication for Mobile Devices in WMNs", IEEE CCECE, Calgary, Canada, May 2010.

[2] A. A. Pizada and C. McDonald, "Kerberos Assisted Authentication in Mobile Ad-hoc networks," Conference on Australian Computer Science, Australia, 2004.