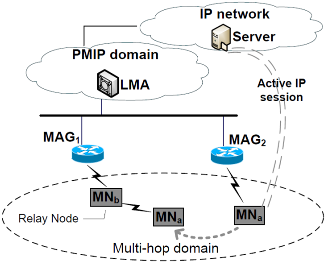
EM^3A: Efficient Mutual Multi-hop Mobile Authentication Scheme for PMIP Networks

Sanaa Taha

November 18, 2011

Multi-hop PMIP Networks

- Mobile wireless networks are envisioned to support multi-hop communications
- Intermediate nodes relay packets in infrastructure-connected mobile networks
- [1] proposes a scheme for IP mobility support in multi-hop PMIP vehicular networks

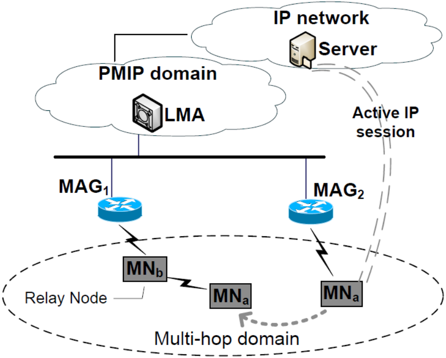


Problem Definition

- Existing authentication schemes use relay nodes (RNs) to only forward the authentication credentials between MN and MAG.
- DoS and fraud attacks can cause service disruptions and financial losses, due to resources exhaustion and high end-to-end delay.
- The Challenge is the difficulty of generating a security association between MN and RN.
- EM^3A works in conjunction with a proposed key establishment scheme

Network and Communication Model

- A MN must connect directly to a MAG in order to obtain a valid IP prefix in the PMIP domain.



Threat and Trust Models

- Internal adversaries : legitimate users who exploit their legitimacy to harm other users
  - Impersonation attack
  - Colluders
- External adversaries : unauthorized users who aim at identifying the secret key and breaking the authentication scheme.
  - Replay attack
  - Man-In-The- Middle
  - Denial of Service

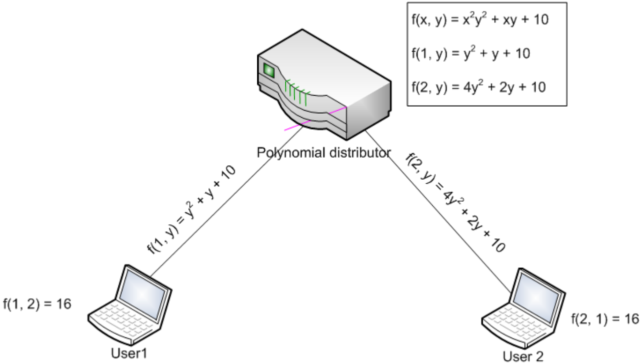
Threat and Trust Models

- Assumptions:
  - Both LMA and MAGs are trusted parties for MNs.
  - After authenticating them, legitimate nodes in the PMIP domain faithfully follow the routing protocol when they are selected to provide their relay services for another MN in their surroundings.
  - Each MAG has a unique identity and the LMA maintains a list of those identities and distributes them to all legitimate users in the PMIP domain.

Symmetric Polynomials

A symmetric polynomial

is any polynomial of two or more variables that has the interchangeability property, i.e., $f(x, y) = f(y, x)$.



Symmetric Polynomials with Mobile Heterogeneous Networks

- A decentralized key generation schemes are proposed in [2],[3] to generate a shared secret key between two arbitrary MNs.
- These schemes achieve t-secrecy level, high MN's revocation overhead, and high Communication Overhead

t-Secrecy

A scheme with t-secrecy property can be broken if $t+1$ users collude to reveal the secret polynomial $f(x, y)$

1- Key Establishment Phase

- Each MAG in the domain generates a four-variables symmetric polynomial $f(w,x,y,z)$, network polynomial, and then sends this polynomial to the LMA.
- Domain Polynomial:

$$F(w,x,y,z) = \sum_{i=1}^{l} f_i(w,x,y,z), 2 \leq l \leq n$$

- The LMA evaluates $F(w,x,y,z)$ for each MAGs identity, ID_{MAG},and then securely sends each individual MAG its own evaluated polynomial
- $F(ID_{MAGi},x,y,z),\ i = 1,2,....,n$

2- MN Registration Phase

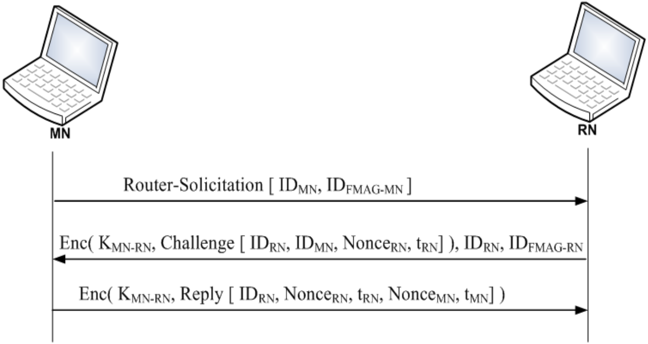
- MN authenticates itself to the MAG to which it is directly connected.
- MAG $\rightarrow$ MN :

$$F(ID_{MAG}, ID_{MN}, y, z)$$

- LMA $\rightarrow$ MN : The list of current MAGs identities
- $MN_a \leftrightarrow MN_b$:

$$F(ID_{FMAGa}, ID_a, ID_{FMAGb}, ID_b) = F(ID_{FMAGb}, ID_b, ID_{FMAGa}, ID_a)$$

3- Authentication Phase



Mobile Node Revocation

- LMA replaces $ID_{FMAG-MN}$, with another unique identity, ID_{NFMAG}, and sends the new identity to all legitimate nodes in the domain.
- Each legitimate node updates its stored MAGs list by replacing the old identity with the new one.
- LMA $\rightarrow$ MN_j :

$$F(ID_{NMAG}, ID_{MNj}, y, z)$$

- Only MNs that share the same $ID_{FMAG-MN}$ need to change their evaluated polynomials and keys.

Internal Adversary

- Impersonation Attacks:

$$K_{a-b} = F(ID_{FMAGa}, ID_a, ID_{FMAGb}, ID_b)$$

- Collusion Attacks: increase secrecy level

$$s = \sum_{k=2}^{n} \binom{n}{k} \times t$$
$$s = t \times [2^n - (1 + n)]$$
$$s \simeq t \times 2^n$$

- The number of colluders that can break the scheme increases from $t + 1$ to $(t \times 2^n) + 1$

External Adversary

- DoS attacks: should know a valid shared key, K_{MNi-RN}, in order for the RN to forward its RS message.
- Replay Attacks: Time stamps and nonces
- MITM Attacks: Challenge and Reply messages.

Computation Overhead

Scheme	Computation overhead	Time(ms)
AMA [4]	$T_s + T_v \times Pr_{check}$	2.55
GMSP [5]	$T_s + T_v + T_c$	2.60
Multi-hop MIP [6]	$T_c + T_{EAP}$	.0194
ALPHA [7]	$T_c + T_{disclose}$	7.5094
EM^3A	$2 \times T_c$	.0194

T: time needed to perform an operation
RSA 1024, and AES schemes
MN-RN RTT : $5ms$

Communication Overhead

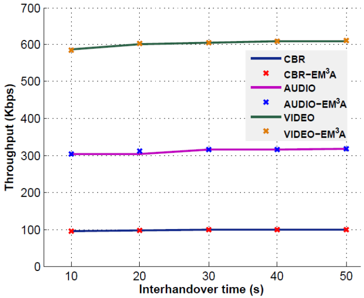
Scheme	Communication Overhead
AMA [4]	B_{cert}
GMSP [5]	B_{cert}
Multi-hop MIP [6]	$B_{EAP} + B_{key-exchange}$
ALPHA [7]	$B_{ACK} + B_{disclose}$
EM^3A	$B_{FMAGs-list} + B_{challenge}$

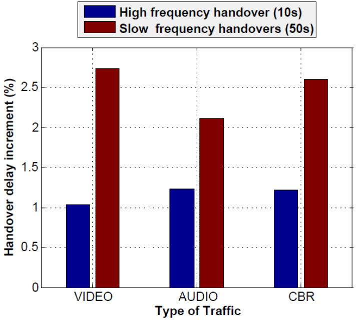
B: bytes needed to Send information

Simulation Parameters

PHY Layer	2.4GHz, 5.5Mbps, 100mW Tx power, -110dBm sensitivity
MAC Layer	802.11 ad hoc mode, 150m radio range
Traffic type/rates	UDP / VBR video (mean 600Kbps), VBR audio (mean 320Kbps), CBR best effort 100Kbps
Session time	$\sim$3min

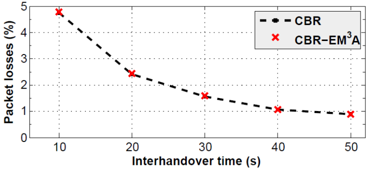
Simulation Results

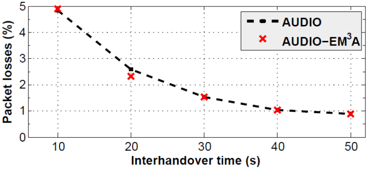


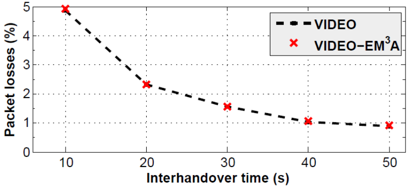


Delay increases by $\sim 1.1\%$ and $\sim 2.5\%$

Simulation Results







Packet losses increases by $\sim 0.03\%$ and $\sim 0\%$

Conclusions and future work

- An efficient authentication scheme, EM^3A, has been proposed.
- Both mobile node and relay node guarantee the legitimacy of each other.
- A novel proposed symmetric polynomial-based key establishment scheme
- EM^3A thwarts internal and external authentication adversaries.
- EM^3A achieves higher secrecy level and lower computation and communication overheads.
- EM^3A results in a low delay and allows for seamless communications even in highly mobile/highly traffic demanding scenarios.
- EM^3A could be extended to use for general multi-hop enabled PMIP networks such as mesh networks.

Thank you

Questions?

M. Asefi, S. Cespedes, X. Shen, and J. W. Mark, "A Seamless Quality-Driven Multi-Hop Data Delivery Scheme for Video Streaming in Urban VANET Scenarios," in *Proc. of IEEE ICC 2011*, pp. 1–5.

A. Gupta, A. Mukherjee, B. Xie, and D. P. Agrawal, "Decentralized Key Generation Scheme for Cellular-based Heterogeneous Wireless Ad hoc Networks," *J. Parallel Distrib. Comput.*, vol. 67, pp. 981–991, 2007.

K. Pillai and M. Sebastain, "A Hierarchical and Decentralized Key Establishment Scheme for End-to-End Security in Heterogeneous Networks," in *Proc. of EEE IMSAA 2009*, pp. 1 –6.

N. Ristanovic, P. Papadimitratos, G. Theodorakopoulos, J.-P. Hubaux, and J.-Y. Le Boudec, "Adaptive Message Authentication for Multi-hop Networks," in *Proc. of Eighth*

International Conference on Wireless On-Demand Network Systems and Services (WONS) 2011, pp. 96 –103.

B. Xie, A. Srinivasan, and D. Agrawal, "GMSP: A Generalized Multi-hop Security Protocol for Heterogeneous Multi-hop Wireless Network," in *Proc. of IEEE WCNC 2006*, vol. 2, pp. 634 –639.

A. Al Shidhani and V. C. M. Leung, "Secure and Efficient Multi-Hop Mobile IP Registration Scheme for MANET-Internet Integrated Architecture," in *Proc. of IEEE WCNC 2010*, pp. 1 –6.

T. Heer, S. Götz, O. G. Morchon, and K. Wehrle, "Alpha: an adaptive and lightweight protocol for hop-by-hop authentication," in *Proc. of ACM CoNEXT '08*, pp. 23:1–23:12.