Bootstrapping Security in Mobile Ad Hoc Networks Using Identity-Based Schemes with Key Revocation

Katrin Hoeper and Guang Gong
2006

Presenter: Paul Miller
CS 6910-ACIS – Project 14A
Department of Computer Science
Western Michigan University
Instructor: Prof. Leszek T. Lilien, Fall 2006

Goals of the Paper

- PKI systems – (CA inside network)
  - key revocation requires thresholds [unsolved]
  - accusation schemes require enormous overhead
    - transmission of signed accusation tables from every node
    - or frequent broadcasts of accusation tables
  - CA outside – all nodes have to frequently check for revocations
- IBC systems – almost seemed unfinished
  - authors solved problems of key revocation
  - key renewal
  - accusations
  - non-static pre-shared keys

(Essentially, they wish to show they have concocted a useable solution.)

IBC History and Features

- Shamir 1984 first asked the question – signatures only
- Boneh and Franklin 2001 came up with BF Schemes
  - They suggested using a natural analog of the Diffie-Hellman assumption: ECC instead of discrete logs [7]: $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \mapsto \mathbb{G}_2$
  - (vanilla DH uses $g \in \mathbb{G}$ as a generator under mod-prime p)
  - They also suggested using Weil Pairing "for good"
- The main feature of IBC is the self authenticating public key: $Q_i = H_1(ID_i, expiry)$
- Of course they also require a Key Generating Center (KGC) to create private keys (d_i)
- All nodes can generate a pre-shared secret without interacting (as in DH) $K_{ij} = \hat{e}(d_i, Q_j) = \hat{e}(Q_i, d_j)$
- Note: The KGC knows all secrets and can compute all keys.

Features of MANET-IDAKE

- implicit non-interactive pre-authentication among all nodes
  - ID_i is built into the key Q_i!
  - Q_i is then self authenticating
- Since *expiry* is built into Q_i, no need to explicitly check expire like in PKI
- Each node automatically shares a key (K_{ij}) with each neighbor
- (PKIs can do this too, but recall that DH is interactive)
- The need for a KGC (key generation center) is a drawback
  - requires each node have an authentic channel to the KGC
  - each channel must be confidential
- key revocation was a problem but HG seem to have solved it.

IDAKE: Identities

- ID_i must be:
  - unchangeably bound for its lifetime
  - not transferable
  - unique
- email address?
- IP address?
- MAC address? (Media Access Control, not Message Authentication Code)
- open question?

IDAKE: Key Expirations

- PKI must frequently check for revocation (listeners @CA)
- In IBC, talkers do that work. HG: more efficient?
- early key revocation isn't really possible
  - can't issue new key for same date
  - can't issue for arbitrary date, ID_i params are "known"
  - If $Q_i = H_1(ID_i, expiry)$ then how do you ever revoke Q_i early?
  - Solution: $Q_i = H_1(ID_i, expiry, version)$
  - Malicious nodes could always $++version \ldots$ v_{max}

IDAKE: Key Revocation

Built in expirations aren't enough!

- key compromise (harakiri)
- malicious behavior (accusation)
- method to inform other nodes about revocations
- joining nodes need the db

IDAKE: Key Revocation: Neighborhood Watch

- supports harakiri, accusation, and informing new nodes
- doesn't broadcast to the entire network
- all nodes ID_i monitor their neighbors $t_j \in \mathcal{N}_i$
- $(t_j = ID_j$ and $j \in \{1, \ldots, N = |N_i|\})$
- the neighborhood watch keeps an accusation matrix:

$$\mathcal{AL}_i = \begin{pmatrix} t_1 & (date_1, v_1) & c_1 \\ \vdots & \vdots & \vdots \\ t_j & (date_j, v_j) & c_j \end{pmatrix}$$

- the flag $c_j \in \{0, 1\}$ indicates the status of Q_j (0 being trust)
- node t_i commits harakiri by sending

  $hm_i = (f_{K\,ij}(Q_i, ID_i, revoke), Q_i, ID_i, revoke)\ \forall t_j \in \mathcal{N}_i$

IDAKE: KR – NW Routing

- ID_i only forwards messages to/from t_j if $t_j \in \mathcal{N}_i$ and $c_j = 0$
- If ID_s wishes to talk to ID_r and $ID_r \ni \mathcal{N}_s$ they would have to talk to other nodes
- this creates a *path of trust*

IDAKE: Basic Setup (1/5)
The Six Basic Algorithms

- setup (choose public and private parameters [7])
  - q, $\mathbb{G}_1$, $\mathbb{G}_2$, P
  - $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \mapsto \mathbb{G}_2$
  - (affine, bi-linear, cyclic, abelian)
  - s – the secret
  - $P_{pub} = sP$ – not multiplication (groups)
  - H_1 is a hash $H_1 : \{0,1\} \rightarrow \mathbb{G}_1$
  - of the above, only s is kept secret
- extract (build a private key)
  - builds $Q_i = H_1(ID_i)$
  - $d_i = sQ_i$

IDAKE: Basic Setup (2/5)
The Six Basic Algorithms

- distribute – give all nodes (t_k) with their secret (d_i)
  - they can "physically" retrieve them
  - or it can distribute them using a "blinding technique like in [21]"
- compute shared key – (each node does this),
  $K_{ij} = \hat{e}(Q_i, d_j) = \hat{e}(Q_j, d_i)$
- key renewal – a new key pair (Q_i, d_i) is needed
  whenever Q_i is revoked/accused or d_i is compromised [not 7]

IDAKE: Basic Setup (3/5)
The Six Basic Algorithms: Key Revocation [not 7]

- neighborhood watch with accusations "[12,22]"

$$\mathcal{KRL}_i = \begin{pmatrix} t_1 & (date_1, v_1) & c_1 & a_{a,1} & \dots & a_{1,N} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ t_N & (date_N, v_N) & c_N & a_{N,1} & \dots & a_{N,N} \end{pmatrix}$$

- $\mathcal{M}_i$ is the "m-hop neighborhood" with $m > 1$, $N = |\mathcal{M}_i|$, and each row $t_j \in \mathcal{M}_i$
- accusations
  - $c_j = 1$ if $a_{j,i} = 1$ (this node accuses)
  - $c_j = 1$ if $a_{j,j} = 1$ (self revocation)
  - $c_j = 1$ if $(date_j, v_j)$ is expired
  - $c_j = 1$ if $A_j = \sum_{k=0}^{N} a_{j,k} > \delta$

IDAKE: Basic Setup (4/5)
The Six Basic Algorithms: Key Revocation part II

- the accusation message looks like hm_i above:
  $am_i = (f_{Kik}(ID_i, Q_j, t_j, accuse), ID_i, Q_j, t_j, accuse)$
  $\forall t_k \in \mathcal{N}_i$
- each neighbor sends the message to their neighbors
  ... and so on (m times) [??]
- during harakiri, t_i would send hm_i to its $\mathcal{M}_i$
  instead of $\mathcal{N}_i$ like above

IDAKE: Basic Setup (5/5)
The Six Basic Algorithms: Key Rev. DB (III)

- new nodes joining the network need to be updated
- $he_n = (ID_n, r_n, hello)$ where r_n is a "random nonce" prevent replay attacks.
- each node $t_i \in N_n$ sends a welcome message
  $wm_i = (f_{Kin}(ID_i, |\mathcal{KRL}_i|, \mathcal{KRL}_i, r_{n+1}),$
  $ID_i, |\mathcal{KRL}_i|, \mathcal{KRL}_i, r_{n+1})$
- ID_n should throw out welcome messages
  - where wm_i cannot be verified
  - Q_i is marked revoked in any other $\mathcal{KRL}_k$
  - $e_n \ll e_{av}$ ... e_n is the number of welcome messages and e_{av} is the average neighborhood size for the neighbors
  - or if $\mathcal{KRL}_i$ significantly differs from the majority.

IDAKE: Distributed KGC

- fully self organized MANET-IDAKE schemes are possible
- they would use ID-based (k, n)-thresholds like proposed in [13,20]

references

[*] Katrin Hoeper and Guang Gong. Bootstrapping Security in Mobile Ad Hoc Networks Using Identity-Based Schemes with Key Revocation. Department of Electrical and Computer Engineering, University of Waterloo, http://www.cacr.math.uwaterloo.ca/techreports/2006/cacr2006-04.pdf 1/25 2006.

[I happened to have read this previously. -Paul]

[7] D. Boneh and M. Franlink. Identity-Based Encryption from the Weil Pairing, *Advances in Cryptology - CRYPTO '2001*, LNCS 2139, pp. 213-229, 2001.

[I did not read these, but use their numbers in the ppt. -Paul]

[10] R. Canetti and H. Krawczyk. Analysis of Key-Exchange Protocols and their Use for Building Secure Channels, *Advances in Cryptology - EUROCRYPT '01*, LNCS 2045, pp. 453-474, 2001.

[12] C. Crepeau and C.R. Davis A Certificate Revocation Scheme for Wireless Ad Hoc Networks. *Proceedings of ACM Workshop on Security of Ad Ho and Sensor Networks (SASN '03)*, ACM Press, isbn 1-58113-783-4, pp.54-61, 2003

[22] H. Luo, P. Zerfos, J. Kong, S. Lu, and L. Zhang. Self-Securing Ad Hoc Wireless Networks, *Seventh IEEE Symposium on Computers and Communications (ISCC '02)*, 2002.

Colophon

This document was produced using Microsoft PowerPoint, mainly, but all text was rendered and formatted using MiKTeX and embedded in PowerPoint using TeX4PPT.

TeX is the simplest way to make math look as pretty as it does on the previous pages and is very popular for writing mathemtatical documents.

The background was rendered in POV-Ray and contains a great deal more detail than is readily visible in this PowerPoint document. The spheres represent water molecules and the angle between the hydrogens and size-proportion to the oxygen is mostly correct.

Full sources for the background and any assistance with TeX can be found by contacting `pemiller@cs.wmich.edu`.