Secure Admission Control in Mobile Ad-Hoc Networks

Jeong H. Yi

jhyi@ics.uci.edu

Computer Science Department

University of California at Irvine



1

Outline

- Introduction
- Motivation
- Definition
- Analysis of existing schemes
- Design and implementation
- Performance evaluation
- Future work

2

Work Done: Existing Scheme Analysis

- *On the Utility of Distributed Cryptography in P2P and MANETs: The Case of Membership Control*
  - M. Narasimha, G. Tsudik, J. H. Yi
  - IEEE ICNP'03
  - Broke threshold RSA scheme
  - Proposed new threshold DSA scheme

3

Work Done: Implementation

- *Experimenting with Admission Control in P2P*
  - N. Saxena, G. Tsudik, J. H. Yi
  - WADIS'03
  - Designed and implemented "**Bouncer**" toolkit
- Related APIs
  - PS_APIs: implementation of plain RSA, May 2002
  - ASM_APIs: implementation of ASM, June 2002
  - TS-RSA_APIs: implementation of TS-RSA, July 2002
  - TS-DSA_APIs: implementation of TS-DSA, April 2003

Source code available at http://sconce.ics.uci.edu/gac

4

Work Done: Performance Evaluation

- *Admission Control in Peer-to-Peer: Design and Performance Evaluation*
  - N. Saxena, G. Tsudik, J. H. Yi
  - ACM SASN'03
  - Integrated "**Bouncer**" with Gnutella and Secure Spread
  - Measured performance of some existing schemes

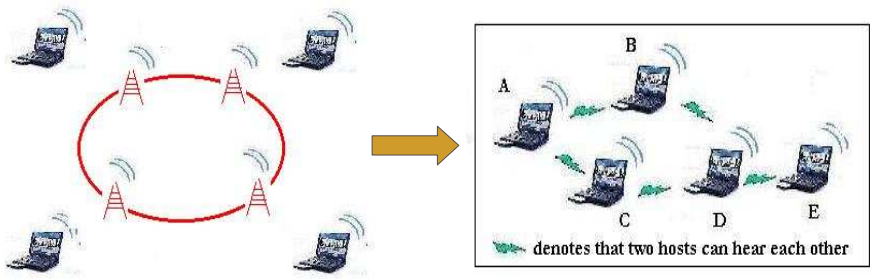
5

Mobile Ad Hoc Networks (MANETs)

- Mobile
  - Random and perhaps constantly changing
- Ad-hoc
  - Not engineered
- Networks
  - Elastic data applications which use networks to communicate

6

MANET Properties



- Infrastructure-less
- Distributed architecture
- Self-organizing
- Wireless connections

7

Many Applications

- Automotive Networks
- Personal Area Networks
  - Ubiquitous Computing
  - Wearable Computing
- Military Applications
- Emergency Operations
- Sensor Networks
- etc…

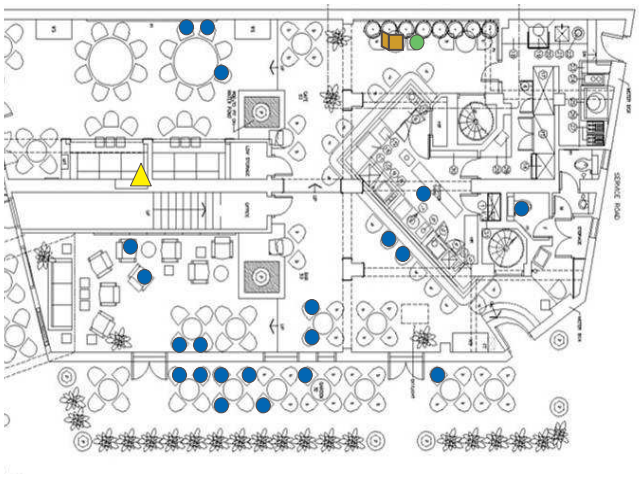
8

Campus Networks

- It is a nice warm day in the University Cafe…
- All the students

  are happy, drinking some coffee, discussing which project group to attend.
- When suddenly somebody switches on his laptop

  … and surfs the Internet while having a cup of coffee
- … obviously somewhere there is a W-LAN base station



9

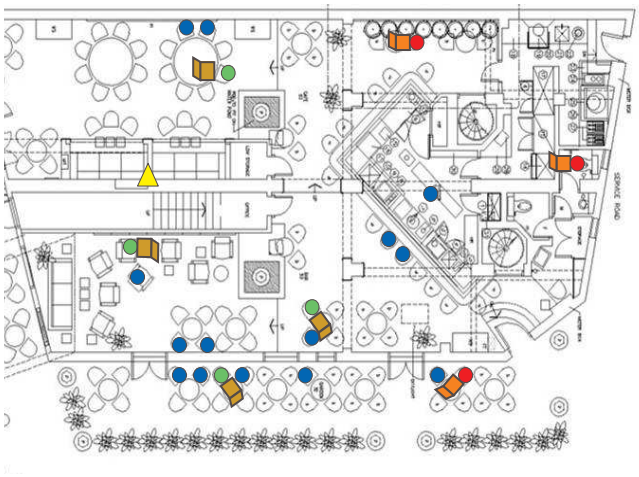
Campus Networks

- The next day …

  … more students

  … connect to W-LAN
- But some of them

  … have severe connection problems
- … **Something must be done**



10

Campus Networks

- So they move closer to the base station

... and closer

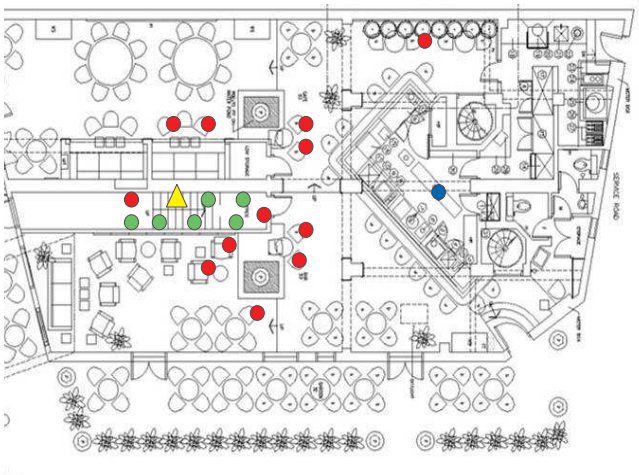
- The lucky ones establish a connection on the stairway



- The others



can not connect and waste some time ...



11

Campus Networks

- ... and so they live unhappily together until
- ... some day a project grou implements a

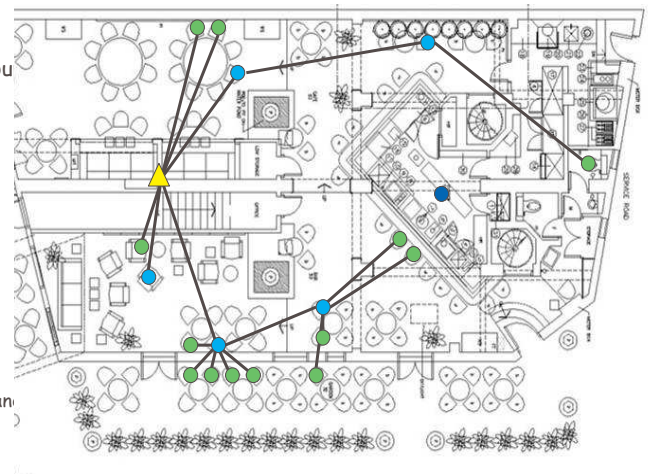
Mobile Ad-Hoc Network based on Wireless LAN

- ... and saves the day.
- Now some



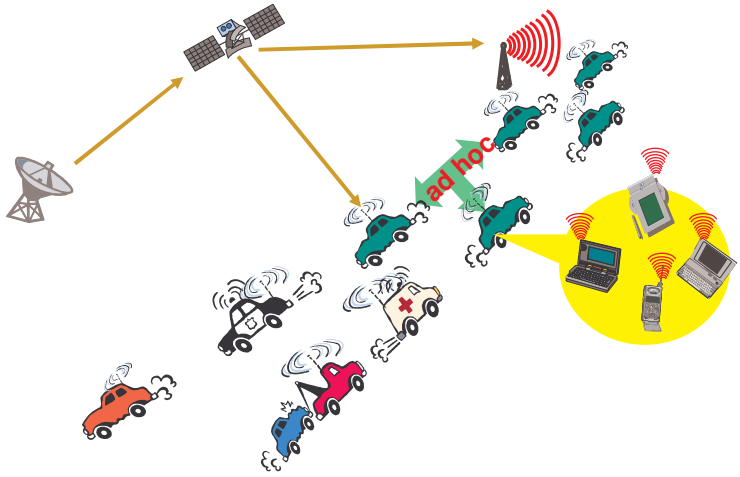
... act as client and router an shared their bandwidth to connect others





12

Automotive Networks



13

Ubiquitous Computing

- many devices per person, becoming interconnected



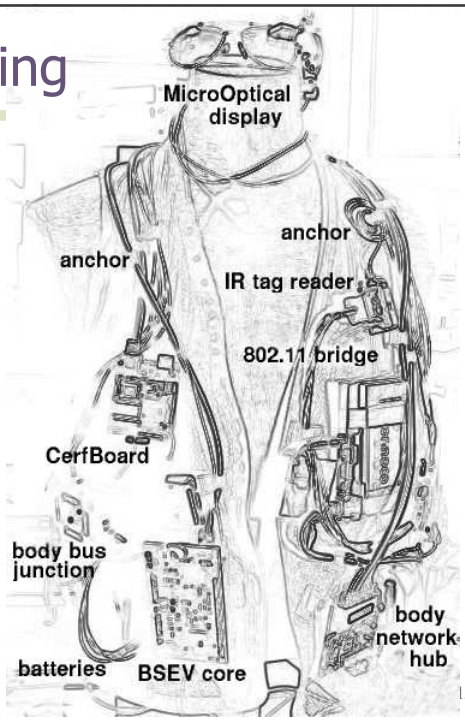
14

Wearable Computing

MIThril is a wearable computing project. Its goal is to build a computer system that you can wear, instead of a computer system that you carry

Source :
http://www.media.mit.edu/wearables/mithril/





15

State of The Art

- IBM ThinkPad 560X
  - 233 MHz Pentium
  - 64 MB DRAM
  - 340 MB HD





16

Bio-Digital Convergence

Wearable Computing



+



- **Always ON**
- **Portable while Operation**
- **Hands-free Use**
- **Sensors**
- **Proactive**

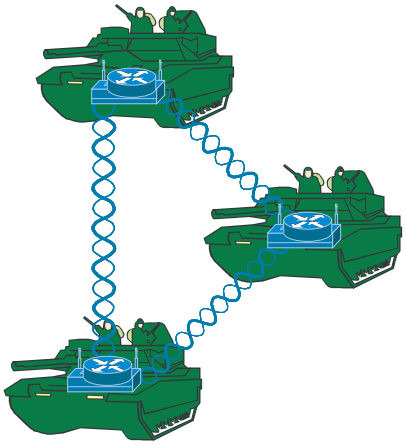
Computer/sensors embedded in the environment

Computers/sensors on **people**
Running all the time
Hands Free

17

Military Applications

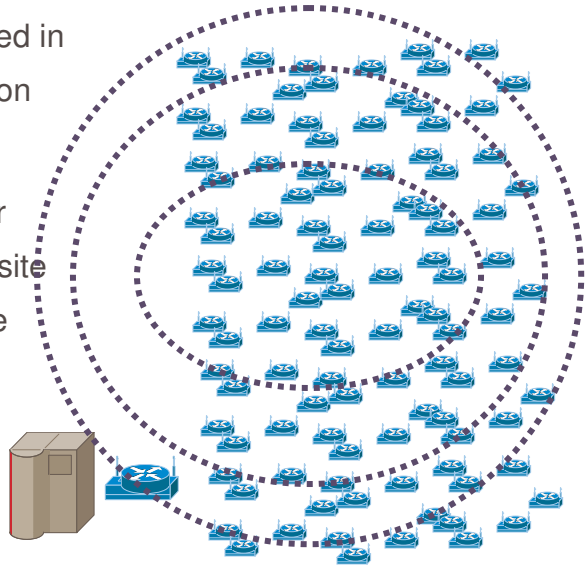
- Combat regiment in the field
  - Perhaps 4000-8000 objects in constant unpredictable motion…
- Intercommunication of forces
  - Proximity, function, plan of battle
- Special issues
  - Low probability of detection
  - Random association and topology



18

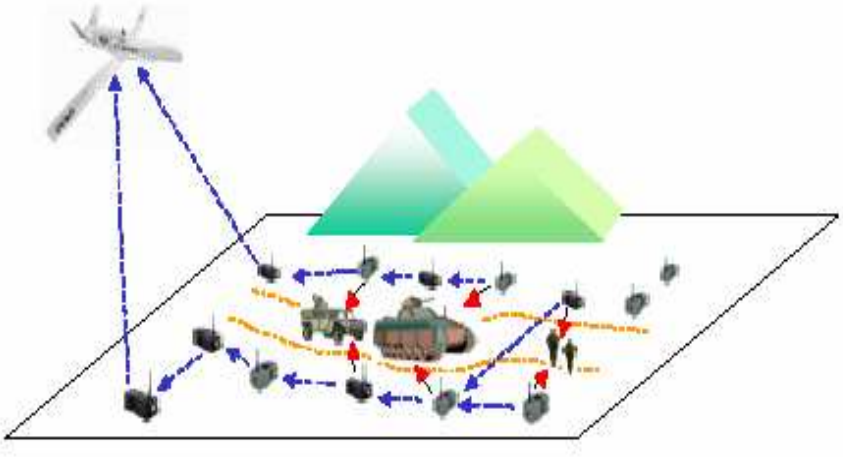
Sensor Networks

- Networks deployed in random distribution
- Low power
- Delivering sensor data to a central site for some purpose



19

Military Surveillance



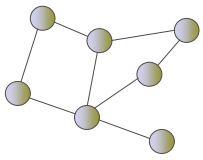
20

Outline

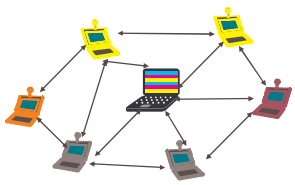
- Introduction
- **Motivation**
- Definition
- Analysis of existing schemes
- Design and implementation
- Performance evaluation
- Future work

21

Peer Group Settings



Decentralized P2P



MANETs

- No centralized control
- No hierarchy
- Fault-tolerant
- Dynamic membership

Distributed and scalable security services required

22

Node Misbehavior

- Selfish Nodes
  - Do not cooperate
  - Priority: battery saving
  - No intentional damage to other nodes.
- **Attacks:**
  - passive denial of service
  - black hole
  - idle status

- Malicious Nodes
  - Goal: damage to other nodes
  - Battery saving is not a priority
- **Attacks:**
  - *active* denial of service
  - traffic subversion
  - attacks exploiting the security mechanism

23

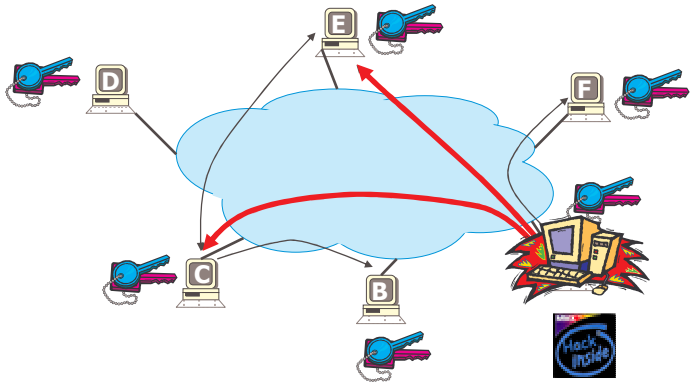
Peer Group Security: Prior Work

Secure communication:

- Key management
- Authentication
- Anonymity
- Secure routing

24

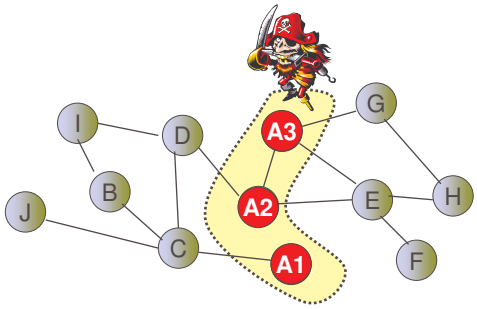
Key Management



25

Sybil attack

- Douceur [IPTPS'02]
- An adversary may create multiple identities



Lesson: Verify identities

26

Motivation

- Secure group communication does not address membership eligibility
- Without *secure admission control*, secure communication (e.g., key management) is useless



27

Outline

- Introduction
- Motivation
- **Definition**
- Analysis of existing schemes
- Design and implementation
- Performance evaluation
- Future work

28

Terminology

- Group Charter
  - defines admission policies



- Group Membership Certificate (GMC)
  - proves membership



- Group Authority (GAUTH)
  - Bootstrapping entity



29

Admission Control Models

- **Admission via Public ACL**
  - Not suitable for *dynamic* peer group



- **Admission by Centralized Authority**
  - Violates *peer* nature
  - Single point of failure



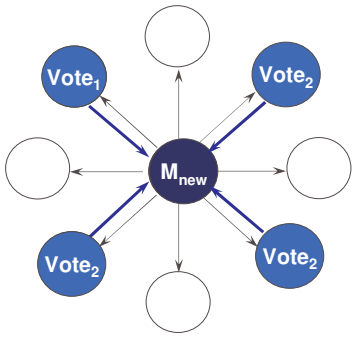
- **Our Focus: Admission by Members**



30

Admission Control

- New member (M_{new}) wants to join the group
- A quorum of t current members need to issue M_{new} a group membership certificate (GMC)
- If no quorum found, membership is denied



- Step 1: Join request
- Step 2: Join commit (Vote)
- Step 3: GMC issuance

31

Threshold Types

- Fixed Threshold
  - Expressed as minimum # of votes (e. g., 5)
  - What if *group size* < threshold?
- Dynamic Threshold
  - Expressed as percentage of # of current members (e.g., 30%)
  - Threshold = percentage * *group size*
  - Keeping an updated group size is important.



Ø *Group Authority (GAUTH), as bootstrapping node, is only trusted to keep account of group size.*

32

Relevant Cryptographic Techniques

- **Plain Signatures (PS)**
  - RSA, DSA, etc.
- **Accountable Subgroup Multi-signatures (ASM)**
  - e.g., Ohta, et al. [CCS'01]
  - Based on Schnorr signature scheme
- **Threshold RSA Signatures (TS-RSA)**
  - e.g., Kong, et al. [ICNP'01]
  - Dealer is required for initialization
- **Threshold DSA Signatures (TS-DSA)**
  - Extension of scheme by Gennaro, et al. [Eurocrypt'96]
  - # of group members (n) can be increased

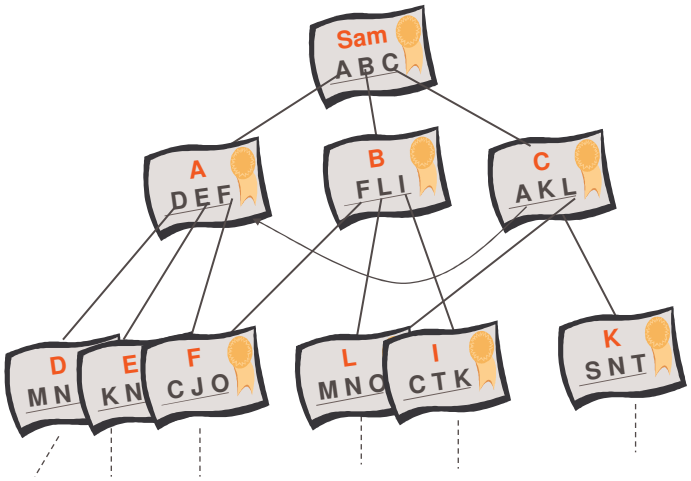
33

Feature Summary

	PS	ASM	TS-RSA	TS-DSA
Dealer involved			√	
Simultaneous on-line presence		√	√	√
Accountability	√	√		
Unlinkability			√	√
Verifiability of secret share	NA	NA		√
Lineage problem	√	√		

34

Membership Authentication: Lineage Problem



35

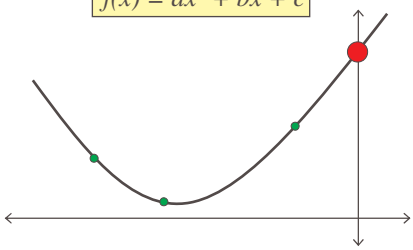
Outline

- Introduction
- Motivation
- Definition
- **Analysis of existing schemes**
  1. **Threshold Secret Sharing**
  2. Threshold RSA signatures (TS-RSA)
  3. Threshold DSA signatures (TS-DSA)
- Design and implementation
- Performance evaluation
- Future work

36

Lagrange Interpolation

$f(x) = ax^2 + bx + c$



- Given *t* points in the plane, there is only one polynomial of degree *t-1* that intersects all *t* points
- *t-1 points do not suffice for interpolation*

37

Shamir's Secret Sharing

- Dealing Secret Shares
  - Dealer randomly selects polynomial *f(x)* of degree *t-1*

$$f(x) = S + a_1 x + a_2 x^2 + \ldots + a_{t-1} x^{t-1} \pmod{q}$$

$$ss_i = f(id_i) \pmod{q}$$

  - Note: $f(0) = S$
  - Dealer distributes secret shares to users
- Secret Recovery

$$S = \sum_{i=1}^{t} ss_i l_i(0) \pmod{q} \qquad l_i(x) = \prod_{j=1, j\neq i}^{t} \frac{x - id_j}{id_i - id_j} \pmod{q}$$

- Distributed Share Computation

$$ss_{new} = \sum_{i=1}^{t} ss_i l_i(id_{new}) \pmod{q}$$

What if users are malicious?

38

Verifiable Secret Sharing (VSS)

- P. Feldman [FOCS'87]
- Select f(x) over Z_q as in Shamir's

$$f(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_{t-1} x^{t-1} \pmod{q}$$

- Setup
- Exponent is in **mod q**
- q, p : large prime
- q | p-1
- Secret share verification

$$g^{ss_i} \pmod{q} = \prod_{j=0}^{t-1} (W_j)^{(id_i)^j} \pmod{p}$$

$$\left(g^{f(id_i)} = g^{a_0 + a_1 (id_i) + \Lambda\, a_{t-1} (id_i)^{t-1}} (\mathrm{mod} p) \right)$$

39

Outline

- Introduction
- Motivation
- Definition
- **Analysis of existing schemes**
  1. Threshold Secret Sharing
  2. **Threshold RSA signatures (TS-RSA)**
  3. Threshold DSA signatures (TS-DSA)
- Design and implementation
- Performance evaluation
- Future work

40

RSA Signature scheme

- Setup
  - Let $N=pq$, where p, q are large primes
  - $d = e^{-1} \bmod \Phi(N)$, where $\Phi(N)=(p-1)(q-1)$
  - d: secret key, (e, N): public keys
- Signature generation
  - $c = m^d \pmod N$
- Verification
  - $m \overset{?}{=} c^e \pmod N$

41

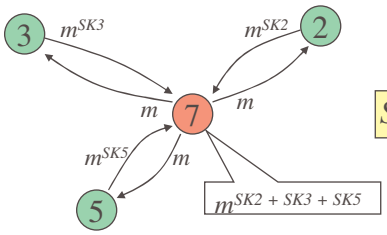
Threshold RSA (TS-RSA)

- J.Kong, et al. [
- Setup
  - Generate RSA key
  - Dealer randomly selects polynomial $f(x)$ of degre

$$f(x) = \boldsymbol{d} + a_1 x + a_2 x^2 + \ldots + a_{t-1} x^{t-1} \pmod N$$

- d is never reconstructed.
- mod N (composite)

- Signature generation



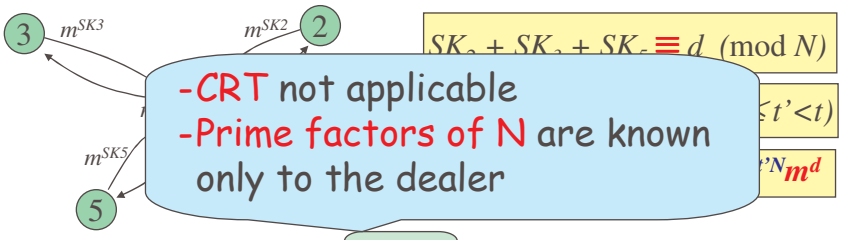
$$SK_i = ss_i l_i(0) \pmod N$$

$$SK_2 + SK_3 + SK_5 \equiv d \pmod N$$

$$m^d \equiv \prod_{i=1}^{t} m^{SK_i} \pmod N$$

42

TS-RSA: t-bounded offsetting

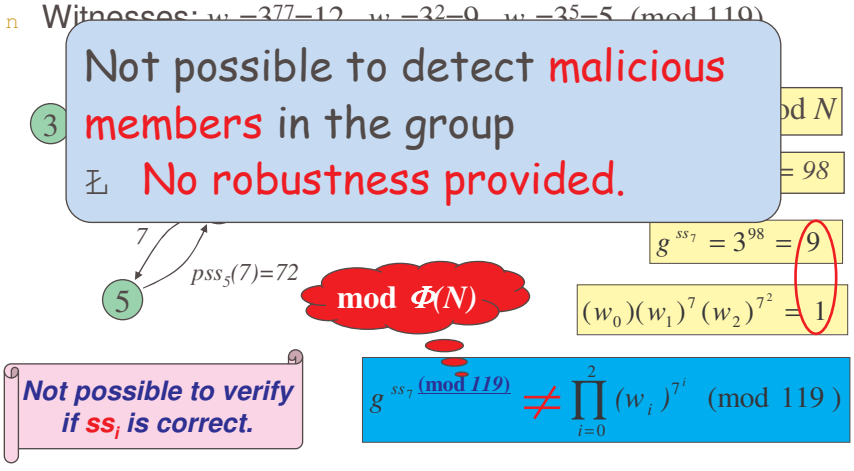


22 msec

```
Y = m^(t'N+d);
offset= m^-N mod N;
for (i=0; i <= t; i++)   {
  if (Y^e = m  mod N)
       break;
       Y = Y * offset mod N;
}
return Y   (= m^d  mod N)
```


TS-RSA: VSS failure

- Example: $f(x) = 77 + 2x + 5x^2 \pmod{119}$, $g=3$
- Witnesses: $w_1 = 3^{77} = 12$, $w_2 = 3^{2^2} = 9$, $w_3 = 3^{5^2} = 5 \pmod{119}$



Not possible to verify if ss_i is correct.

TS-RSA: Summary

- No verifiability of secret shares
  - Gennaro [Crypto'96] and Shoup [Eurocrypt'00]: schemes to provide verifiability
  - Boneh & Franklin [Crypto'97]: distributed RSA key generation
    - very high communication and/or computation overhead
    - impractical in group setting such as MANETs
- Trusted dealer involved at initialization

45

Outline

- Introduction
- Motivation
- Definition
- **Analysis of existing schemes**
  1. Threshold Secret Sharing
  2. Threshold RSA signatures (TS-RSA)
  3. **Threshold DSA signatures (TS-DSA)**
- Design and implementation
- Performance evaluation
- Future work

46

DSA Signature scheme

- Setup
  - Generate p, q, such that $q \mid p-1$
  - $g \in Z_p^*$ such that $g^q = 1 \bmod p$
  - $x \in Z_{q-1}^*$, $y = g^x \bmod p$
  - secret key: x, public keys: (p,q,g,y)
- Signature generation
  - generate *random* $k \in Z_{q-1}^*$
  - compute $r = (g^{k^{-1}} \bmod p) \bmod q$
  - compute $s = k(m+xr) \bmod q$
  - signature: (r, s)
- Verification
  - compute $v = (g^{ms^{-1}} y^{rs^{-1}} \bmod p) \bmod q$
  - compare (r, v)

47

Threshold DSA (TS-DSA)

- We extended threshold DSS scheme proposed by Gennaro, et al. [Eurocrypt'96]
  - group size (n) can be increased.
  - threshold (t) can be changed.
- No dealer involved
- VSS holds

48

TS-DSA: Setup

- Self-initialization by founding members
  - uses Joint Secret Sharing (JSS), T.P.Pedersen [Eurocrypt'91]

$$f(z) = \sum \begin{cases} f_1(z) = f_{10} + f_{11}z + \Lambda + f_{1,t-1}z^{t-1} \pmod q \rightarrow \text{User}_1 \\ f_2(z) = f_{20} + f_{21}z + \Lambda + f_{2,t-1}z^{t-1} \pmod q \rightarrow \text{User}_2 \\ \text{M} \\ f_n(z) = f_{n0} + f_{n1}x + \Lambda + f_{n,t-1}z^{t-1} \pmod q \rightarrow \text{User}_n \end{cases}$$

$$x = f(0) = \sum f_i(0)$$

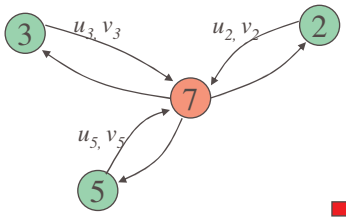
Nobody knows x.

- Each user computes $f_i(id_j)$ (j=1..n, j != i), and sends it to others.
- Each user computes his own secret share

$$ss_i = f(id_i) = \sum_{j=1}^{n} f_j(id_i)$$

TS-DSA: Signature Generation

- DSA signature: (*r*, *s*)



O(t²) comm. O(t) exp.

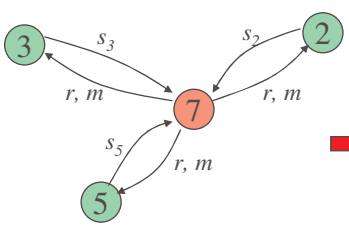
$$u_j = k_j a_j \bmod q \qquad v_j = g^{a_j} \bmod p$$

$$U = \sum_{j=1}^{t} u_j l_j(0) \bmod q \quad [= ka \bmod q]$$

$$V = \prod_{j=1}^{t} (v_j)^{l_j(0)} \bmod p \quad [= g^a \bmod p]$$

extra exp.

$$r = (V^{U^{-1}} \bmod p) \bmod q \quad [= g^{k^{-1}} \bmod p \bmod q]$$



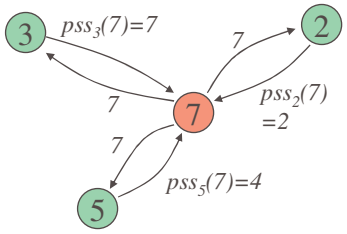
(2t-1)-degree

$$s_j = k_j(m + x_j r) \bmod q$$

$$s = \sum_{j=1}^{t} s_j l_j(0) \bmod q$$

TS-DSA: VSS success

- Example: $f(x) = 7 + 2x + 5x^2 \pmod{11}$, $g=9$, $q=11$, $p=23$
- Witnesses: $w_0=9^7=4$, $w_1=9^2=12$, $w_2=9^5=8 \pmod{23}$



$pss_i(j) = ss_i l_i(j) \bmod p$

$ss_7 = pss_2(7) + pss_3(7) + pss_5(7) = 2$

$g^{ss_7} = 9^2 = 12$

$(w_0)(w_1)^7(w_2)^{7^2} = 12$

$$g^{ss_7 \pmod{11}} = \prod_{i=0}^{2} (w_i)^{7^i} \pmod{23}$$

51

TS-DSA: Summary

- Pros:
  - VSS guaranteed
  - Key generation fully distributed
- Cons:
  - Robust only if fewer than $\lfloor (t+1)/2 \rfloor$ malicious users
  - Extra $O(t^2)$ communications between signers for random secret *k*

52

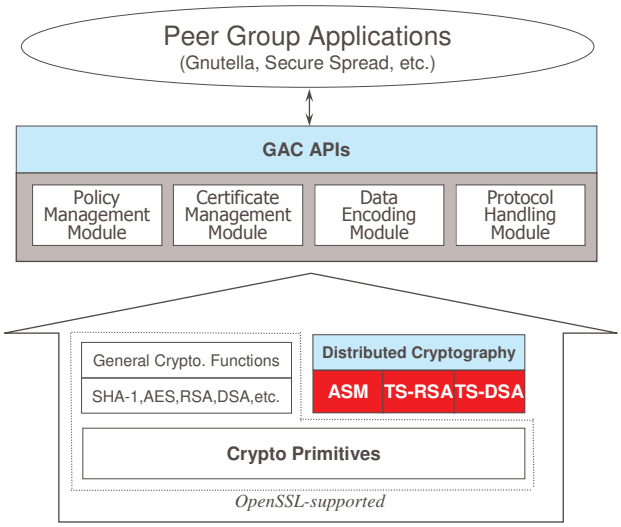
Outline

- Introduction
- Motivation
- Definition
- Analysis of existing schemes
- **Design and implementation**
- Performance evaluation
- Future work

53

System Design - "Bouncer" toolkit





54

Dynamic Threshold Update

```
Function GAC_Dynamic_Threshold_Update();

Input parameters:
    X509* GChart,          \* group charter *\
    int N_old,             \* old group size *\
    int N_cur,             \* current group size *\
    int T_cur              \* current threshold *\

Body:
    int diff;
    int offset;
    int Win;               \* Window buffer size *\
    int T_new              \* new threshold *\

     T_new=T_cur;
     Win=WIN_TIMES*GChart.threshold.fixed;
     diff = N_cur - N_old;
     if (diff >= Win) {
         offset = ⌊diff / Win⌋;
         N_old = N_old + (offset*Win);
         T_new = ⌊(GChart.threshold.dynamic /
                   100) * N_old⌋;
         if (T_new > T_cur)
              T_cur=T_new;
     }
     return T_new;
```

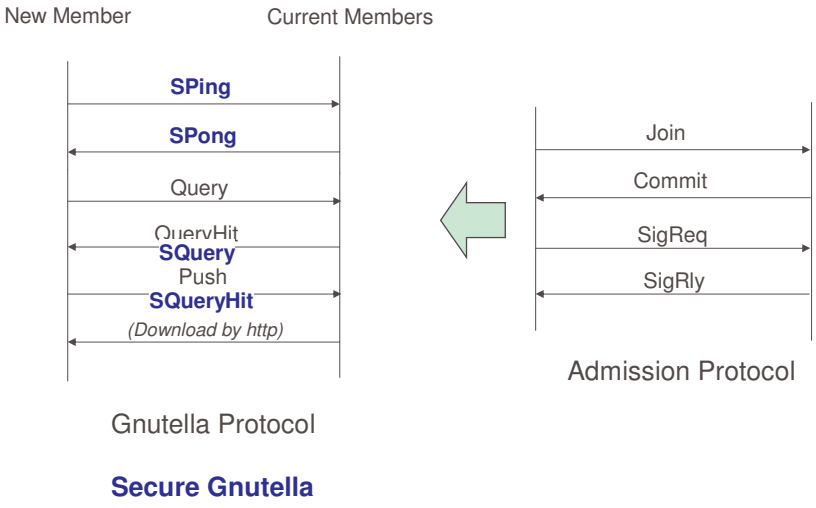
55

GAC APIs

- Plain RSA APIs
  - GAC_PACKET *PS_Join_Reqest();
  - GAC_PACKET *PS_Join_Commit();
  - GAC_PACKET *PS_GMC_Request(); /* optional */
  - GAC_PACKET *PS_GMC_Reply(); /* optional */
- TS-RSA APIs
  - GAC_PACKET *TSS_Join_Request();
  - GAC_PACKET *TSS_Join_Commit();
  - GAC_PACKET *TSS_Sign_Request();
  - GAC_PACKET *TSS_Part_Sign();
  - GAC_PACKET *TSS_GMC_Request(); /* optional */
  - GAC_PACKET *TSS_GMC_Reply(); /* optional */
- TS-DSA APIs
  - GAC_PACKET *TSD_Join_Request();
  - GAC_PACKET *TSD_Join_Commit();
  - GAC_PACKET *TSD_Chal_Req();
  - GAC_PACKET *TSD_Chal_Rly();
  - GAC_PACKET *TSD_Rnd_Req();
  - GAC_PACKET *TSD_Rnd_Rly();
  - GAC_PACKET *TSD_Sign_Request();
  - GAC_PACKET *TSD_Part_Sign();
  - GAC_PACKET *TSD_GMC_Request(); /* optional */
  - GAC_PACKET *TSD_GMC_Reply(); /* optional */
- ASM APIs
  - GAC_PACKET *ASM_Join_Request();
  - GAC_PACKET *ASM_Join_Commit();
  - GAC_PACKET *ASM_Sign_Request();
  - GAC_PACKET *ASM_Part_Sign();
  - GAC_PACKET *ASM_GMC_Request(); /* optional */
  - GAC_PACKET *ASM_GMC_Reply(); /* optional */

56

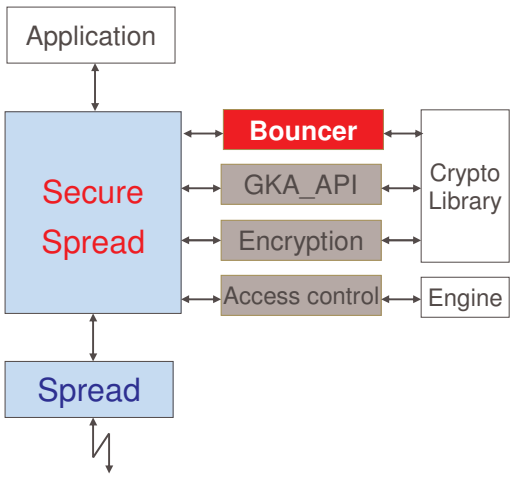
Integration with Gnutella



57

Integration with Secure Spread

- Spread: A wide area reliable group communication system
- Secure Spread: Integrates security services with Spread
  - Supports only static access control
    - daemon level ACL's
    - *flush* mechanism
  - *No notion of secure, dynamic, distributed admission.*
- Modified Spread APIs
  - SP_GAC_Join(); /* new */
  - SP_receive(); /* modified */



58

Outline

- Introduction
- Motivation
- Definition
- Analysis of existing schemes
- Design and implementation
- **Performance evaluation**
- Future work

59

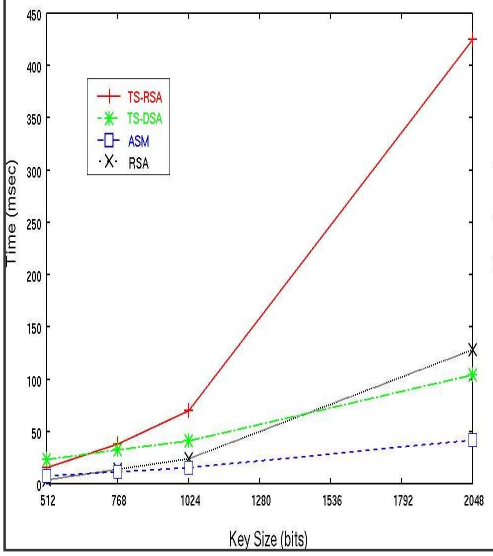
Experimental Setup

- **Gnutella Experiment:**
  - Integrated decentralized protocol with Gnut-0.4.21
  - Tested on a high-speed LAN
- **Secure Spread Experiment:**
  - Integrated centralized protocol with Secure SPREAD-2.1.0
  - Spread daemons on 10 machines at Johns Hopkins Univ.
  - A client at UCI
- Measurements
  - Fixed threshold
  - Dynamic threshold

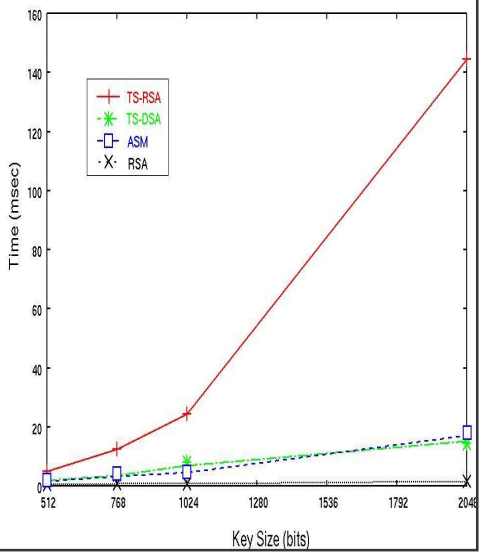
60

Computation Cost

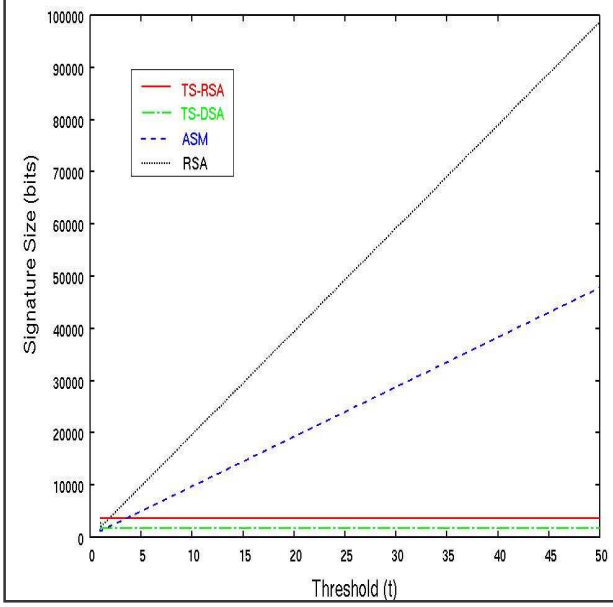
Signature generation



Signature verification



Signature Size

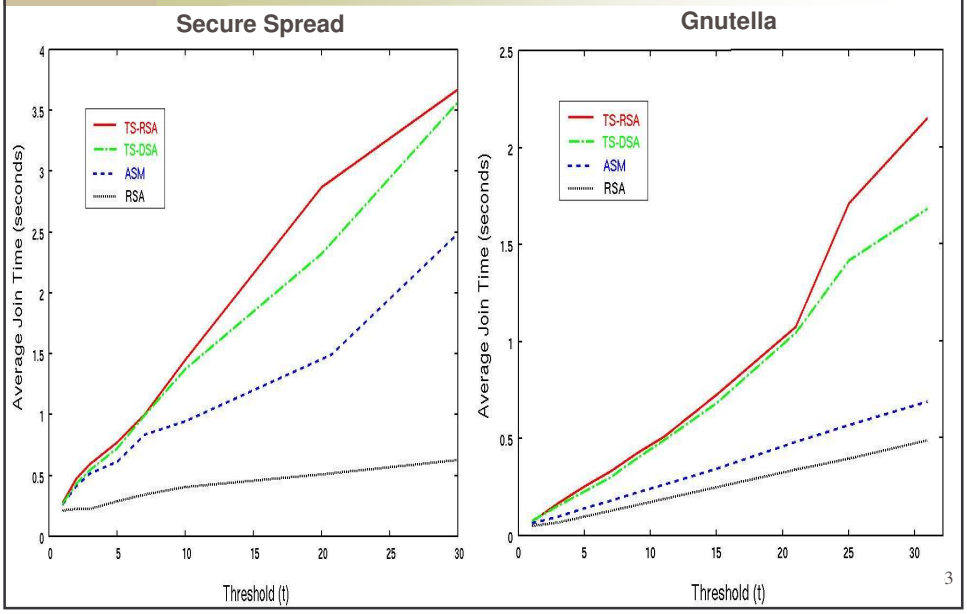


	Signature length
RSA	***t*** * (|K| + |id|)
ASM	|q| + |E| + ***t*** * |id|
TS-RSA	|K|
TS-DSA	2*|q|

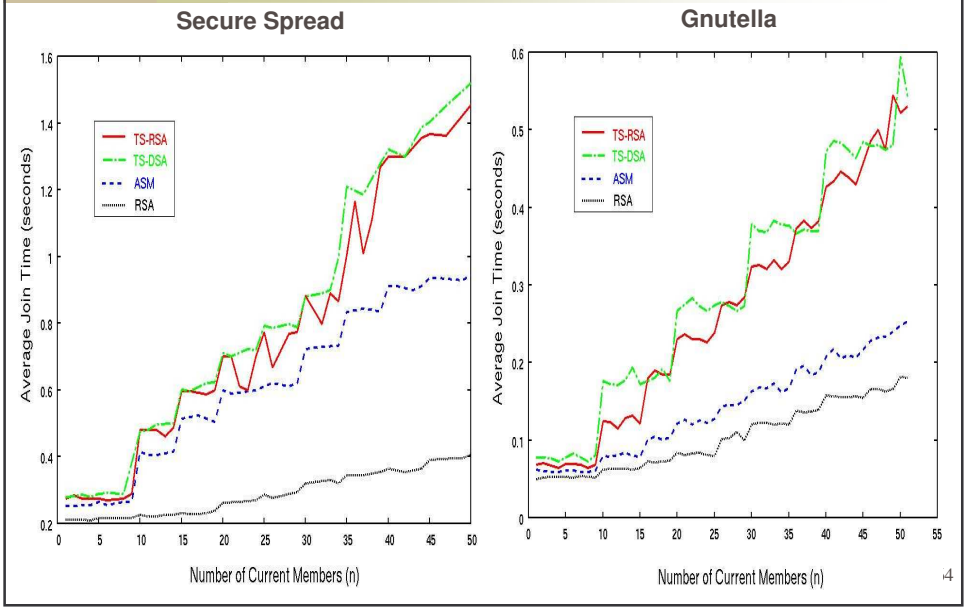
t: threshold
K: private key
id: signer's id
q: modulus q
E: challenge (hash size)

62

Fixed Threshold Experiments



Dynamic Threshold Experiments



Summary

- Designed several P2P admission control mechanisms
- Assessed practicality of distributed cryptography for dynamic peer groups.
  - Threshold signatures are currently ***NOT PRACTICAL*** in MANETs and sensor networks
  - Reasonable for Internet-based P2P systems that operate in (at least partially) synchronous mode
- Difficult to identify one scheme best-suited for all peer group admission scenarios.
- If admission is difficult, distributed membership revocation is even harder!

65

Future Work

- TS-RSA
  - Efficient RSA distributed modulus generation
  - VSS in Dynamic setting
- TS-DSA
  - Better communication efficiency?
- Aggregated Signatures?
- Bilinear mapping based approach
  - Security proof of the protocol
  - External membership proof process
- Other, more “systems” approaches?
- Revocation?

66

End

