Key Revocation for Identity-Based Schemes in Mobile Ad Hoc Networks

Guang Gong

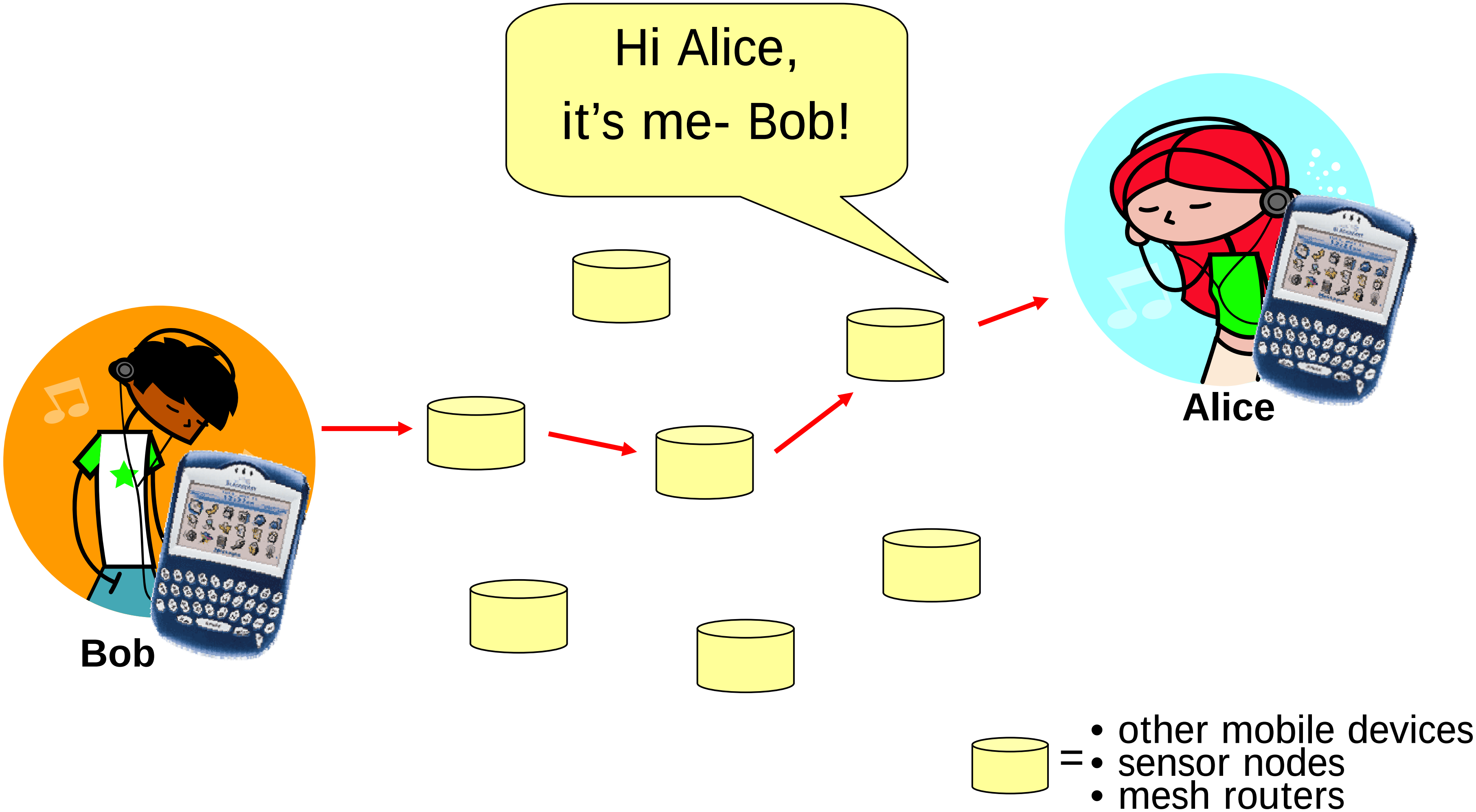
Department of Electrical & Computer Engineering
University of Waterloo, CANADA

Joint work with Katrin Hoeper

Outline

- Security requirements
- Solutions & challenges in MANETs
- Review identity-based crypto schemes
- Existing schemes
- Proposed key revocation & renewal scheme
- Security analysis
- Conclusions

Communication Scenario in MANET



=
- other mobile devices
- sensor nodes
- mesh routers

Challenges in MANETs

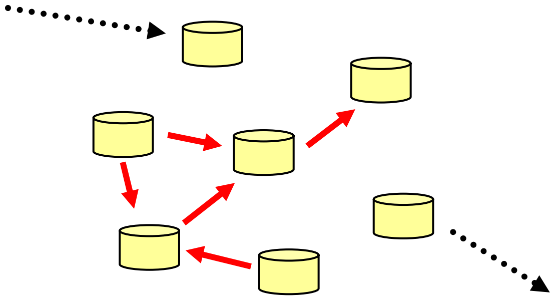
❑Properties of MANETs

♦self-organizing

♦no central trusted third party (TTP)

♦dynamic

♦wireless channels



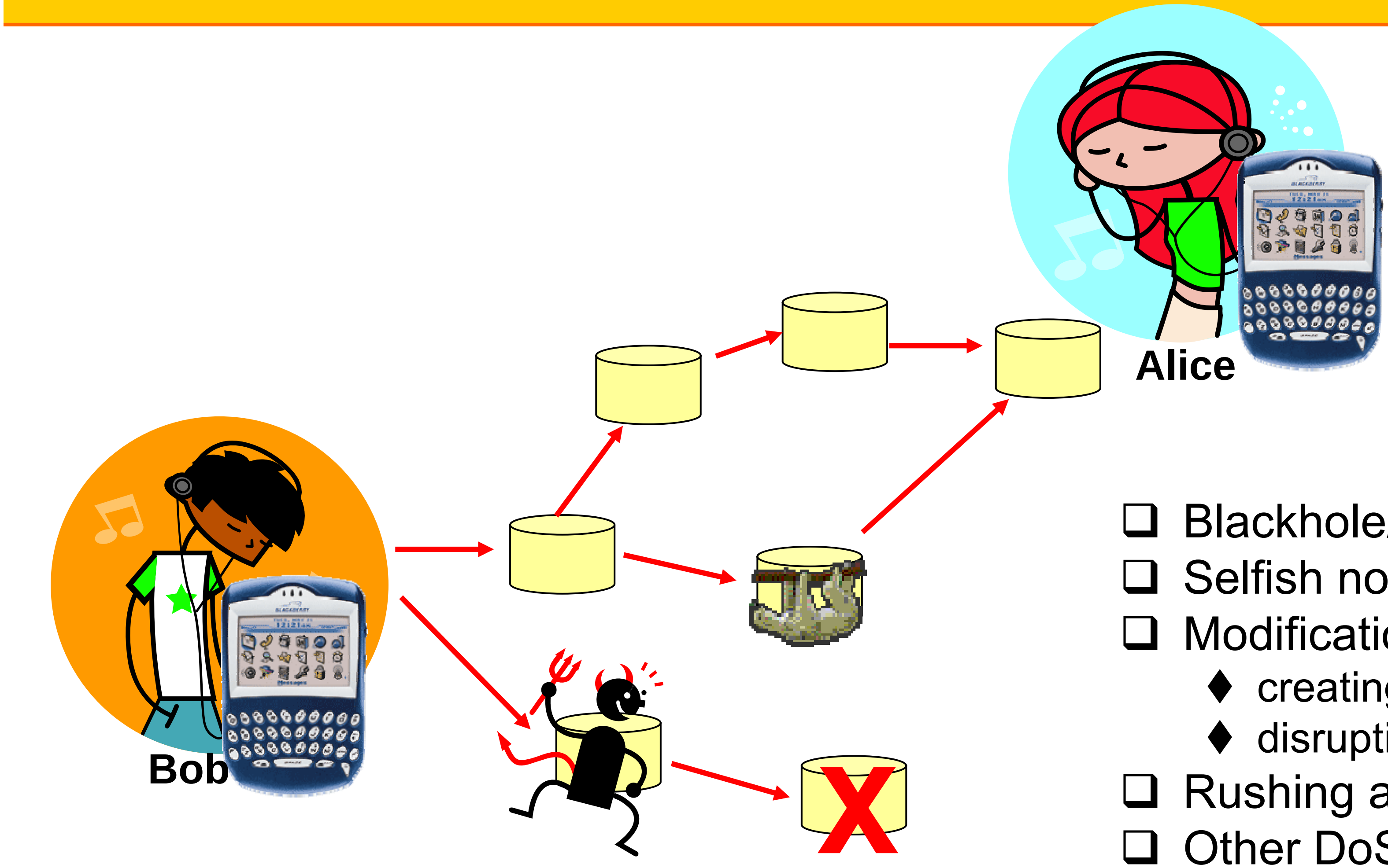
❑Properties of devices

♦constrained devices

□ CPU, memory, battery

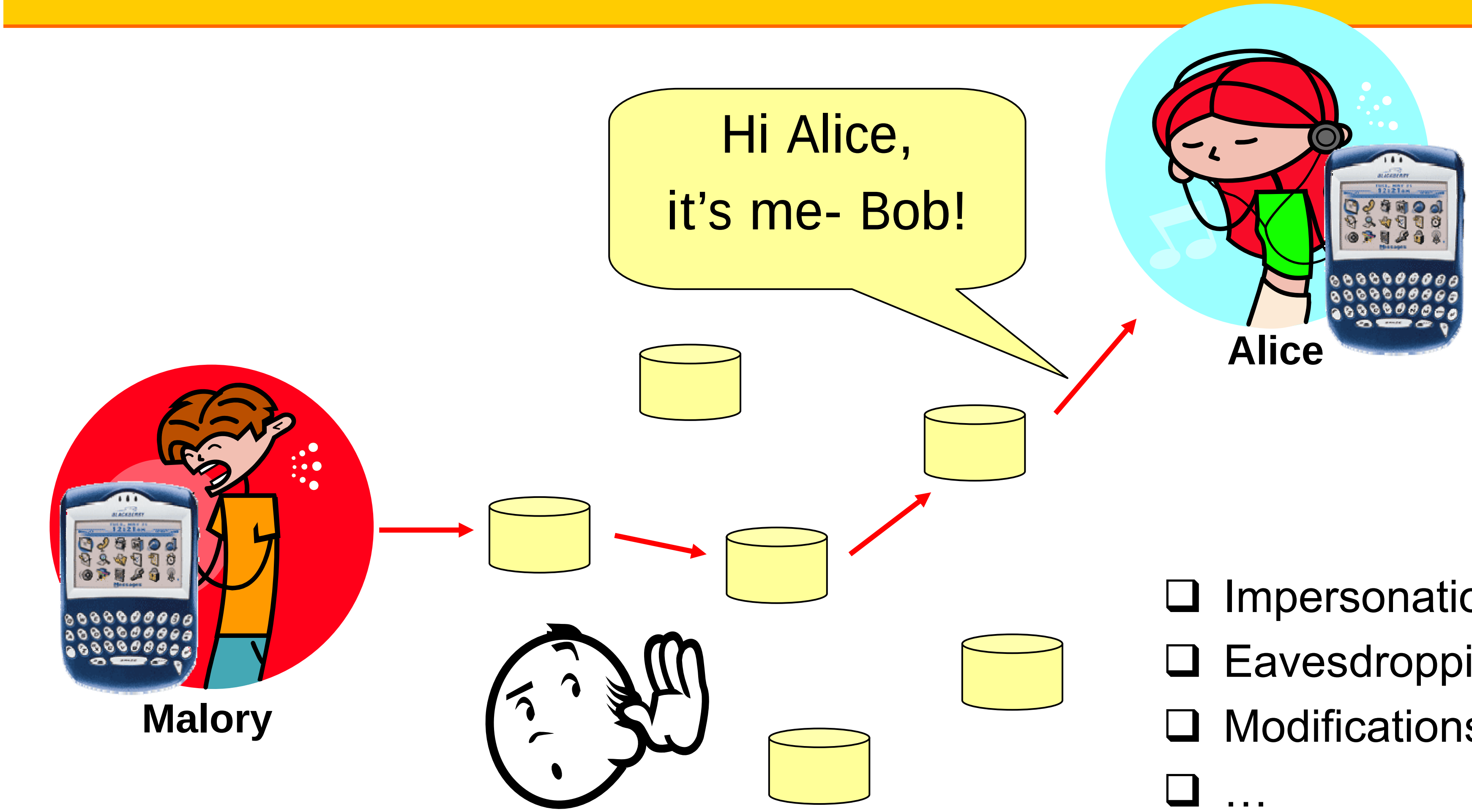
♦limited physical protection

Routing Attacks



- ❑ Blackhole/wormhole
- ❑ Selfish nodes
- ❑ Modification attacks
  - ♦ creating loops
  - ♦ disruption attacks
- ❑ Rushing attacks
- ❑ Other DoS attacks

Communication Attacks

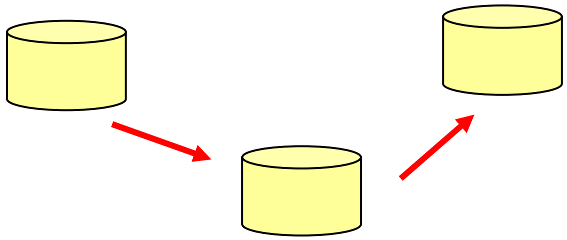


- Impersonation
- Eavesdropping
- Modifications
- …

Security Requirements

❑Routing *(hop to hop)*

- ♦source authentication
- ♦message integrity



❑Communication *(end to end)*

- ♦entity authentication
- ♦message integrity
- ♦confidentiality

Existing Security Solutions

- □Symmetric schemes
  - ♦require secure key distribution

- □Public key infrastructures (PKIs)
  - ♦require Certificate Authority (CA) to issue & distribute public key certificates

- □Identity-based crypto (IBC) schemes
  - ♦require Key Generation Center (KGC) to generate and distribute private keys

✡ We evaluate ID-based solutions!

Review: ID-Based Schemes

- [Shamir`84] First identity-based signature scheme
  - idea: use common information, “identity” (ID), as public keys
  - key generation center (KGC) computes and distributes private keys

Review: ID-Based Schemes (cont'd)

❑[BF`01] First ID-based encryption scheme

- ♦Boneh-Franklin scheme uses bilinear mappings
- ♦set up
  - □2 groups G_1, G_2 of order q
  - □bilinear map $\hat{e}: G_1 x\ G_1 \rightarrow G_2$
  - □arbitrary generator $P \in G_1$
  - □hash function $H_1: \{0,1\}^* \rightarrow G_1{}^*$
- ♦KGC
  - □master key $s \in Z_q{}^*$
  - □public key $P_{pub} = sP$

user ID_i

public key $Q_i = H_1(ID_i)$

private key $d_i = sQ_i$

Features of ID-Based Schemes

❑Efficient key management

- ♦no public key certificates
- ♦no key exchange prior communication
- ♦implicit public key validation

$$Q_i = H_1(ID_i \| \text{'expiry date'})$$

- ♦additionally in pairing based schemes
  - □non-interactive pre-shared pairwise keys

$$K_{i,j} = \hat{e}(d_i, Q_j) = \hat{e}(d_j, Q_i) \quad (1)$$

Problems of ID-Based Schemes

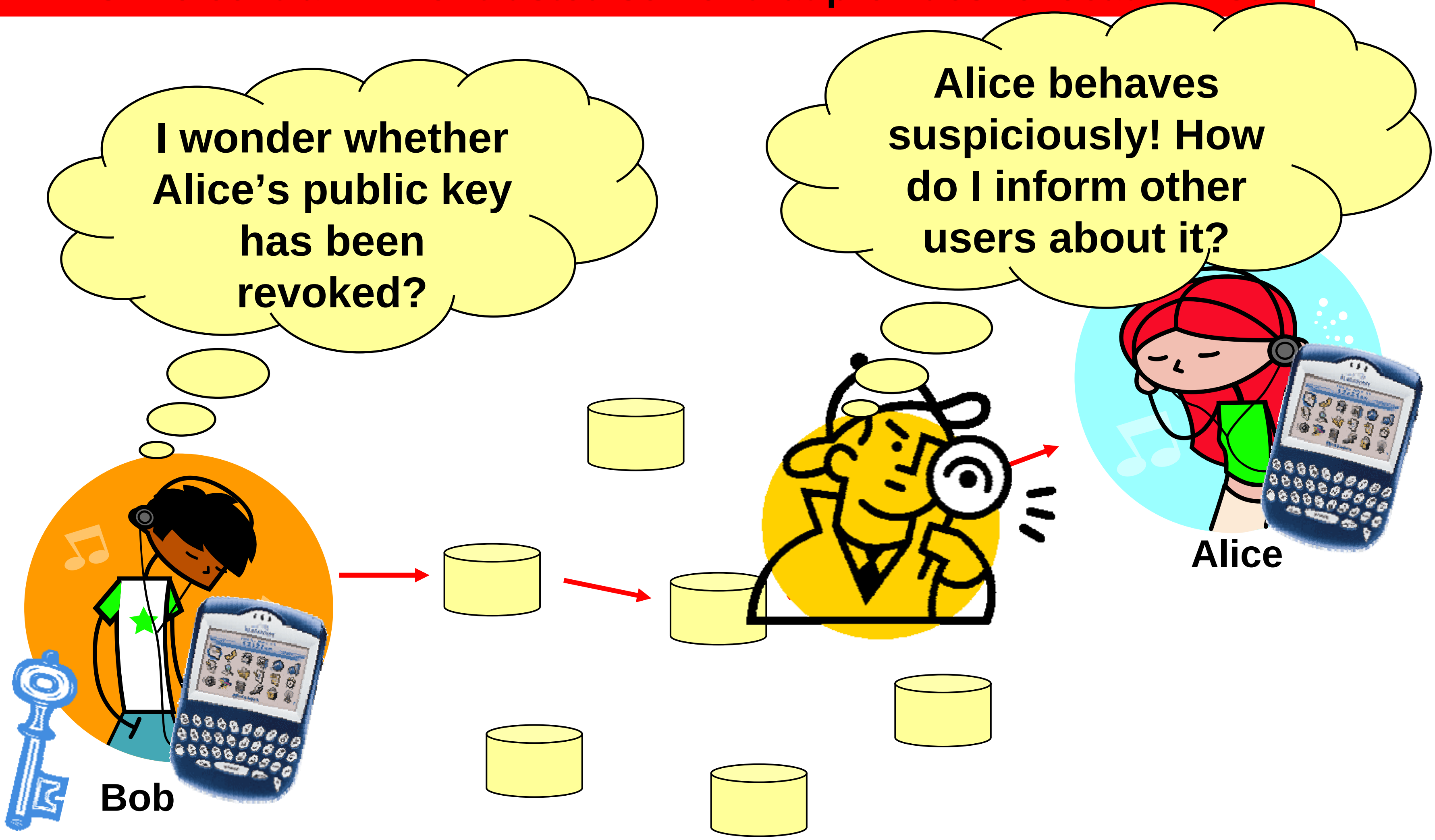
1. Key escrow
   - inherent property of all ID-based schemes
   - KGC knows all private & pairwise keys

2. Key revocation
   - revocation crucial due to likelihood of compromises
   - no central TTP available to maintain revocation lists
   - current schemes do not provide such mechanisms

3. Key renewal
   - after revocation new ID-based keys need to be issued for the same identity

Revocation Problem

MANETs: No central TTP or trusted server that provides revocation lists


I wonder whether Alice’s public key has been revoked?
Alice behaves suspiciously! How do I inform other users about it?
Alice
Bob

Conventional Revocation Schemes

❑ Certificate Revocation Lists (CRLs)

- ♦ distributed by a central trusted server or TTP to all users

❑ ΔCRLs

- ♦ TTP distributes only CRL updates to reduce bandwidth

❑ Online Certificate Status Protocol (OCSP)

- ♦ users query current certificate status from CA

❑ Micali’s Novomodo scheme

- ♦ new elements of hash chain are published by CA if certificate is still valid, more efficient than OCSP

♦ all these solutions work only for PKIs and require a fixed infrastructure, e.g. an on-line CA, TTP or trusted server

✡ solutions are not applicable to MANETs!

Revocation Schemes for MANETs

❑ [Luo et al.`02]

- ♦ users send signed accusations to all users
- ♦ δ accusation against the same user revoke his key
- ♦ problems: no details provided; no possibility for users to revoke their own keys; joining users need to verify many signatures

❑ [Crépeau et al.`03]

- ♦ accusation scheme with δ-threshold
- ♦ problems: accusations not secured; requires broadcasts to entire network

✡Still no secure sophisticated revocation scheme for MANETs

✡Still no revocation schemes for ID-based schemes yet!

Proposed Scheme

- System set up:
  1. based on BF scheme
  2. preshared key $K_{i,j}$ provides message authentication, e.g., $f(x)$ where $f(x)$ is a hash function
- Assumptions for our key renewal and revocation scheme:
  1. bidirectional communication links
  2. nodes are in promiscuous mode
  3. each node has a unique identity
  4. nodes know identities of their one-hop neighbors
  5. nodes know their *m*-hop neighborhood
  6. nodes obtain keys from off-line KGC before joining network

Key Renewal

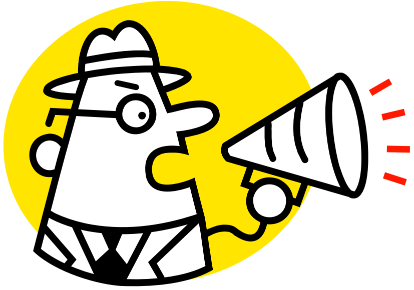
- Renew key if previous key is
  - revoked
  - compromised
  - expired
- New keys issued for same identity
  - $Q_i = H_1(ID_i \| t_i \| v_i)$
  - t_i: expiry date of public key Q_i
  - v_i: version number of Q_i
  - user needs to re-authenticate to external KGC

Key Revocation

□ Revocations need to be on-line

□ Revoke key if

1. nodes behave suspiciously
   - □ observe & tell others
   - □ send accusation message *am*
   - □ δ accusations for revoking key
2. own key is compromised
   - □ tell others
   - □ send harakiri message *hm*



Neighborhood Watch

- ❑All nodes observe their 1-hop neighborhood N_i
  - ♦each node ID_i maintains accusation matrix AM^i containing accusation values $a^i_{j,i}$

$$AM^i = \begin{pmatrix} ID_1 & (t^i_1, v^i_1) & a^i_{1,i} \\ \vdots & \vdots & \vdots \\ ID_{N_i} & (t^i_{N_i}, v^i_{N_i}) & a^i_{N_i,i} \end{pmatrix}$$

N_i: number of 1-hop neighbors

- □ $a^i_{j,l}$ = 0, ID_i marks ID_j as trustworthy
- □ $a^i_{j,l}$ = 1, ID_i marks ID_j as malicious, only reset if a new valid key Q_j’ is received
- □ update AM^i every time malicious behavior is observed

Propagation

- Accusation messages *am*
  - after AM^i or KRL^i update, ID_i propagates update am_i

$$am_{i,j} = (f_{K_{i,j}}(ID_i, am_i), ID_i, am_i)) \text{ to all } ID_j \in N_i$$

- Harakiri messages *hm*
  - upon noticing that private key d_i is compromised, ID_i broadcasts $hm_i = (ID_i, d_{i,} Q_i, t_i, v_i, \text{"revoke"}, hopcount)$
- Messages send to 1-hop neighborhood
  - verify authenticity and forward
  - repeated *m* times

Accusation Scheme

- Every node ID_i generates key revocation list KRL^i from NW and received *am* & *hm*

column 1

accusations made by ID_1

$$\mathcal{KRL}^i = \begin{pmatrix} ID_1 & (t^i_1, v^i_1) & R^i_1 & a^i_{1,1} & \cdots & a^i_{1,M_i} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ ID_{M_i} & (t^i_{M_i}, v^i_{M_i}) & R^i_{M_i} & a^i_{M_i,1} & \cdots & a^i_{M_i,M_i} \end{pmatrix}$$

accusations against ID_{M_i}

row M_i

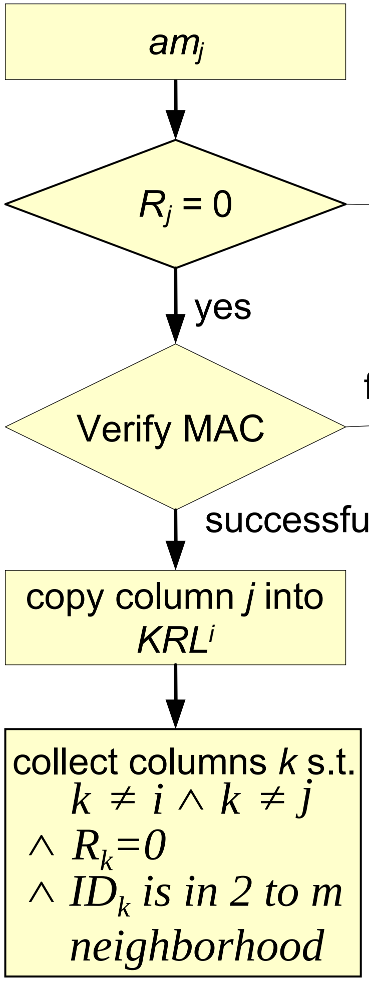
  - M_i number of nodes in *m*-hop neighborhood
  - Q^i_j considered revoked if revocation value $R^i{}_j = 1$

$$R^i_j = 1 \text{ if } t^i_j \text{ expired } \vee a^i_{j,i} = 1 \vee a^i_{j,j} = 1 \vee \sum_{k=1}^{M_i} a^i_{j,k} > \delta$$

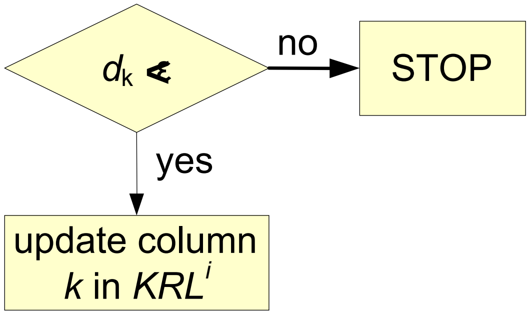
  - δ is the threshold for revoking a key

Update Key Revocation List

- ❑ ID_i repeats for all received accusation messages am_j


am_j
$R_j = 0$
no
STOP
yes
Verify MAC
failed
STOP
successful
copy column j into KRL^i
collect columns k s.t.
$k \neq i \wedge k \neq j$
$\wedge\ R_k=0$
$\wedge\ ID_k$ is in 2 to m neighborhood

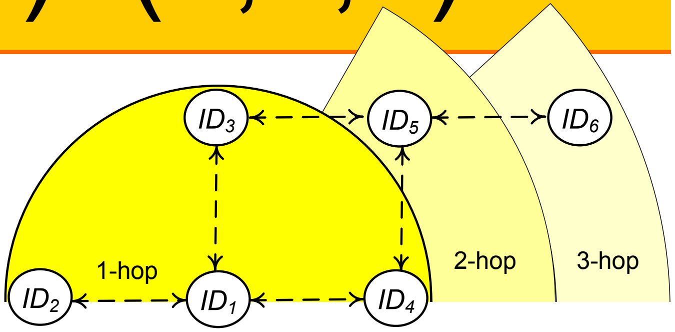
- ❑ After processing all received am_j
  - ♦ ID_i checks the number d_k of collected columns k
  - ♦ ε is threshold for updating columns of nodes that are 2 to m hops away



- ❑ ID_i updates column k in KRL^i

$$a^i_{l,k} = \begin{cases} 1 & \text{if} \sum_{j=1}^{d_k} a^j_{l,k} > \frac{d_k}{2} \\ 0 & \text{if} \sum_{j=1}^{d_k} a^j_{l,k} < \frac{d_k}{2} \\ a^i_{l,k} & \text{otherwise} \end{cases}$$

Toy Example: $(\delta,\varepsilon,m)=(3,2,2)$



- ❑ ID_1 receives am_2, am_3, am_4
  - ♦ discard am_2, save am_3 and am_4
  - ♦ copy column 3 from am_3 *and* column 4 from am_4 into KRL^1
  - ♦ collect vectors k
    - □ $k=(\cancel{1},\cancel{2},\cancel{3},\cancel{4},5,\cancel{6})$ from am_3
    - □ $k=(\cancel{1},\cancel{2},\cancel{3},\cancel{4},5,\cancel{6})$ from am_4

D_5 = 2, update column 5

<u>Before update</u>

$$KRL^1=\begin{pmatrix} ID_1 & 0 & 0 & 0 & 0 & 0 & 0 \\ ID_2 & 1 & 1 & 0 & 0 & 0 & 0 \\ ID_3 & 0 & 0 & 0 & 0 & 0 & 0 \\ ID_4 & 0 & 0 & 0 & 0 & 0 & 0 \\ ID_5 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

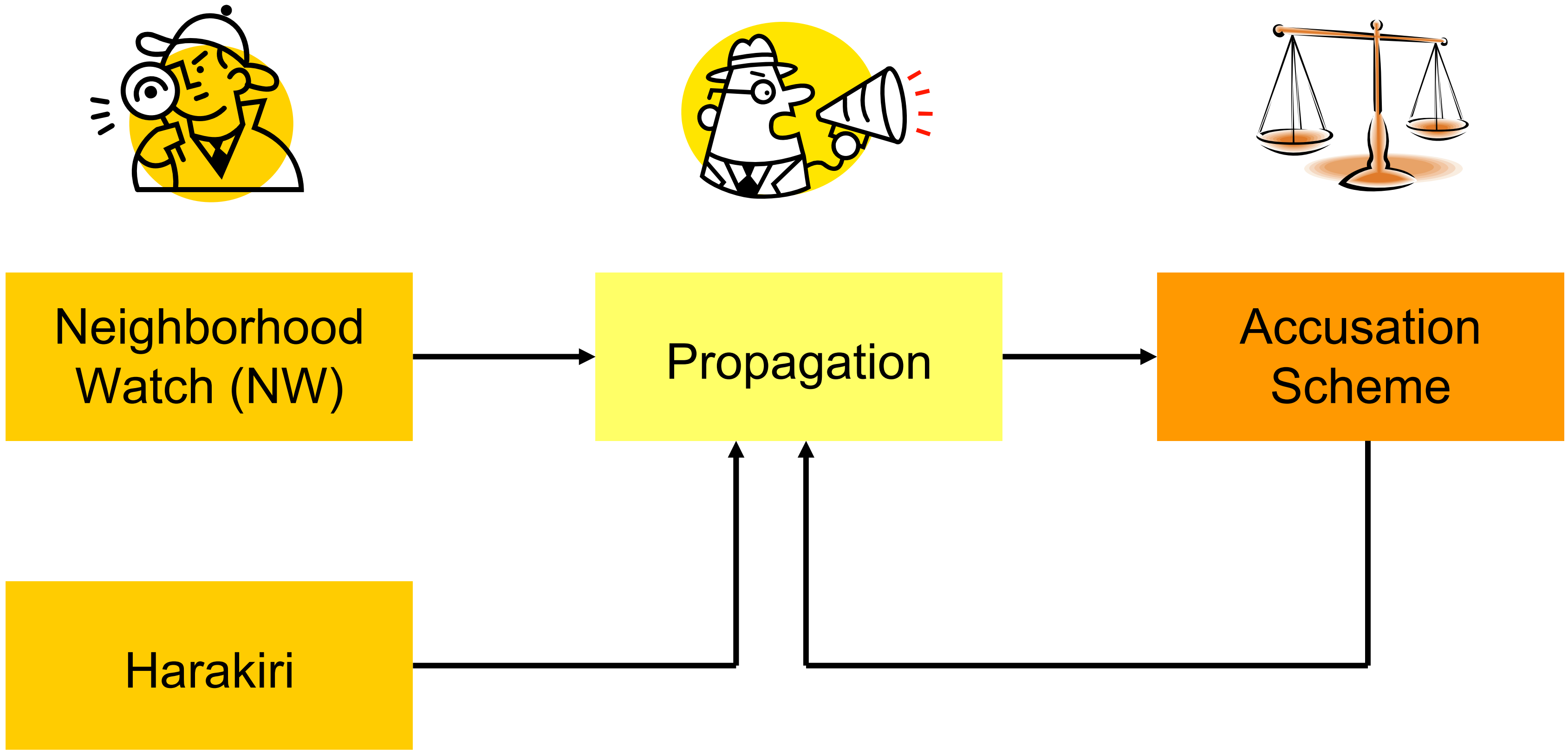
$$KRL^3=\begin{pmatrix} ID_1 & 0 & 0 & 1 & 0 & 0 & 1 & - \\ ID_2 & 1 & 1 & 0 & 1 & 1 & - & - \\ ID_3 & 0 & 0 & 1 & 0 & 0 & 0 & - \\ ID_4 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ ID_5 & 1 & 0 & - & 1 & 1 & 0 & 1 \\ ID_6 & 1 & - & - & 1 & 1 & 0 & 0 \end{pmatrix}$$

$$KRL^4=\begin{pmatrix} ID_1 & 0 & 0 & 1 & 0 & 0 & 0 & - \\ ID_2 & 1 & 1 & 0 & 1 & 1 & - & - \\ ID_3 & 0 & 0 & 1 & 0 & 0 & 1 & - \\ ID_4 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ ID_5 & 1 & 0 & - & 1 & 1 & 0 & 1 \\ ID_6 & 1 & - & - & 1 & 1 & 1 & 0 \end{pmatrix}$$

<u>After update</u>

$$KRL^1=\begin{pmatrix} ID_1 & 0 & 0 & 0 & 0 & 0 & 0 \\ ID_2 & 1 & 1 & 0 & 1 & 1 & - \\ ID_3 & 0 & 0 & 0 & 0 & 0 & 0 \\ ID_4 & 0 & 0 & 0 & 0 & 0 & 1 \\ ID_5 & 0 & 0 & 0 & 1 & 1 & 0 \end{pmatrix}$$

Recap Revocation Scheme



Neighborhood Watch (NW)

Propagation

Accusation Scheme

Harakiri

Security Analysis I

❑Outsider attacks

- ♦routing attacks prevented by using secure routing protocols
- ♦eavesdropping and impersonation prevented by using secure AKE protocols
- ♦attacks on revocation and renewal scheme prevented by using MACs for message authentication

Security Analysis II

- Insider attacks
  - malicious insider can be identified and their keys be revoked by our neighborhood scheme
  - false revocations prevented for up to ✉ *-1* false accusations
  - more than $\frac{\varepsilon}{2}$ undetected one-hop neighbors have to collude for a false revocation of a single node that is 2 to *m* hops away
  - recognized key compromises are securely & quickly propagated throughout an *m*-hop network

Conclusions

We designed a self-organized key revocation scheme for ID-based schemes employed in MANETs

- ♦ proposed revocation scheme enables user to instantly verify whether a key is revoked and revoke their own keys
- ♦ revocation scalable in security & performance in terms of security parameters *(✉, ε, m)*
- ♦ efficient due to use of pre-shared symmetric keys with MACs and propagation to *m*-hop neighborhood
- ♦ our ID-based key format allows key renewal

Future Work

- ❑ Many extensions are possible
  - ♦ adopt solution to PKI schemes
  - ♦ maintain accusation values for all network nodes, i.e. m = N (remove Assumption 5)
  - ♦ include weighted accusation values (0..1) [Crépeau et al.`03] (Note. In this case, the accusation values do not represent the status of the keys.)
  - ♦ include sleeping mode for nodes
- ❑ Further performance & security analysis
  - ♦ sign & broadcast vs. MAC & m-hop
  - ♦ false positive & false negative accusations

References

- K. Hoeper and G. Gong, “Key Revocation for Identity-Based Schemes in Mobile Ad Hoc Networks”, Ad-Hoc, Mobile, and Wireless Networks (ADHOC-NOW 2006), August, 2006, Ottawa. *Lecture Notes in Computer Science*, vol. 4104, pp. 224-237, 2006.

- K. Hoeper and G. Gong, Bootstrapping Security in Mobile Ad Hoc Networks Using Identity-Based Schemes with Key Revocation, Technical Report, University of Waterloo, CACR 2006-04, 2006.