Monitoring-Based Key Revocation Schemes for Mobile Ad Hoc Networks

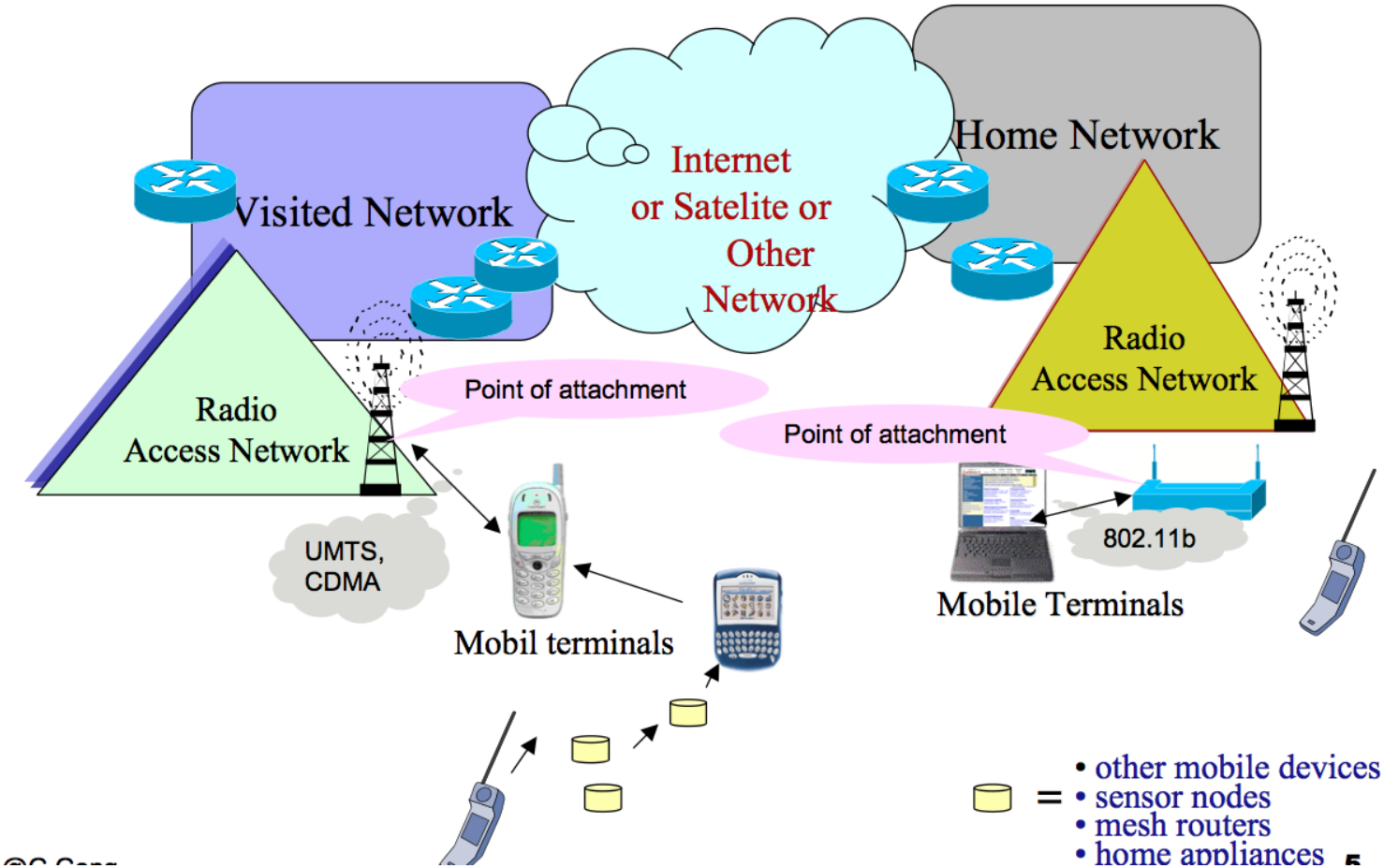
Guang Gong

Department of Electrical and Computer Engineering
University of Waterloo
CANADA
<http://comsec.uwaterloo.ca/~ggong>

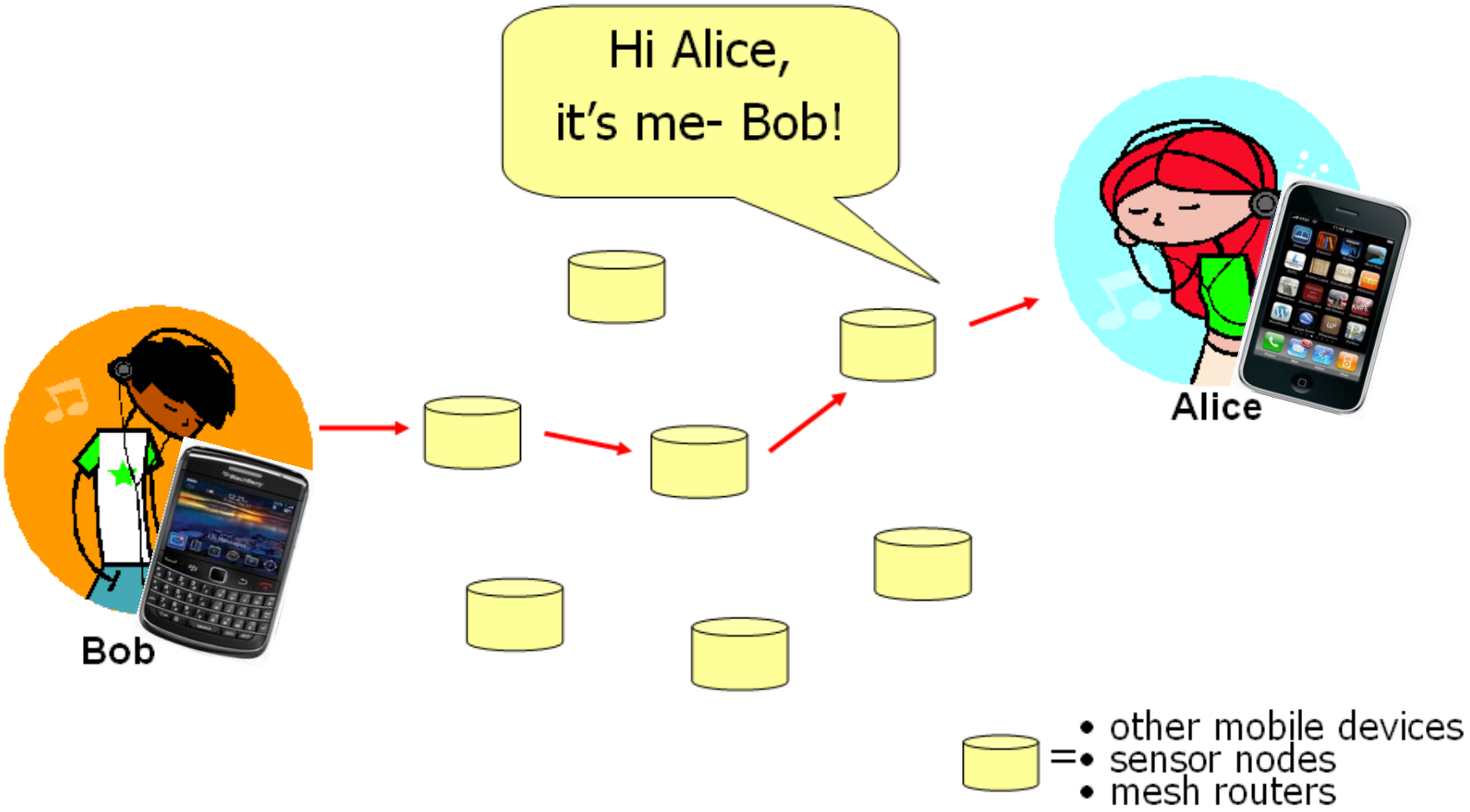
Outline

- **Security** requirements
- Solutions & **challenges** in MANETs
- **Review** of identity-based crypto schemes and existing key revocation schemes
- Two new **monitoring based** self-organized key revocation schemes
- **Implementation** on MICAz motes
- **Conclusions and remarks**

Model for Mobile Communication Security

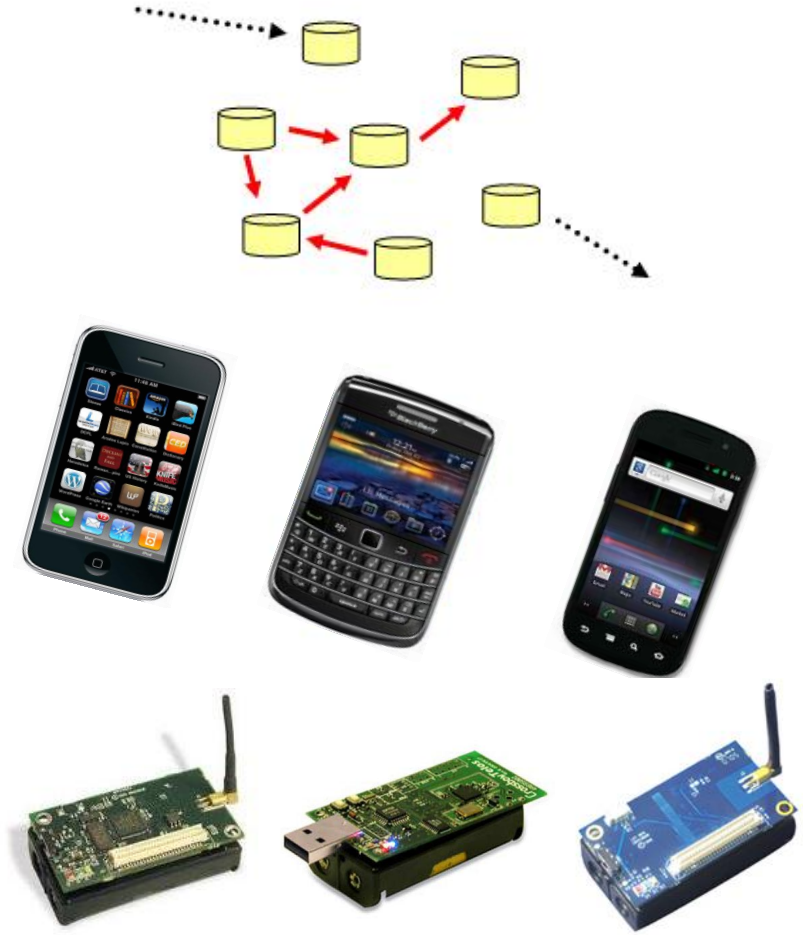


Communication Scenario in MANETs

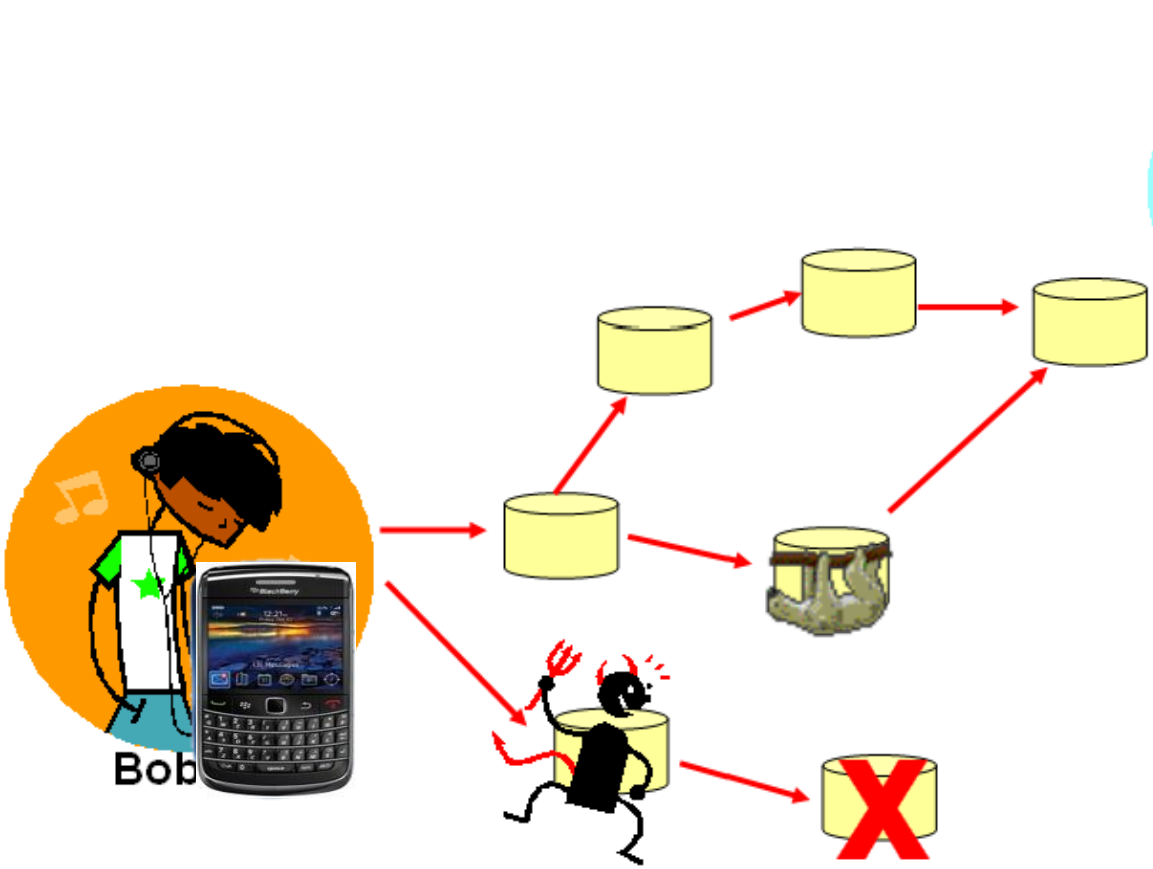


Challenges in MANETs

- 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

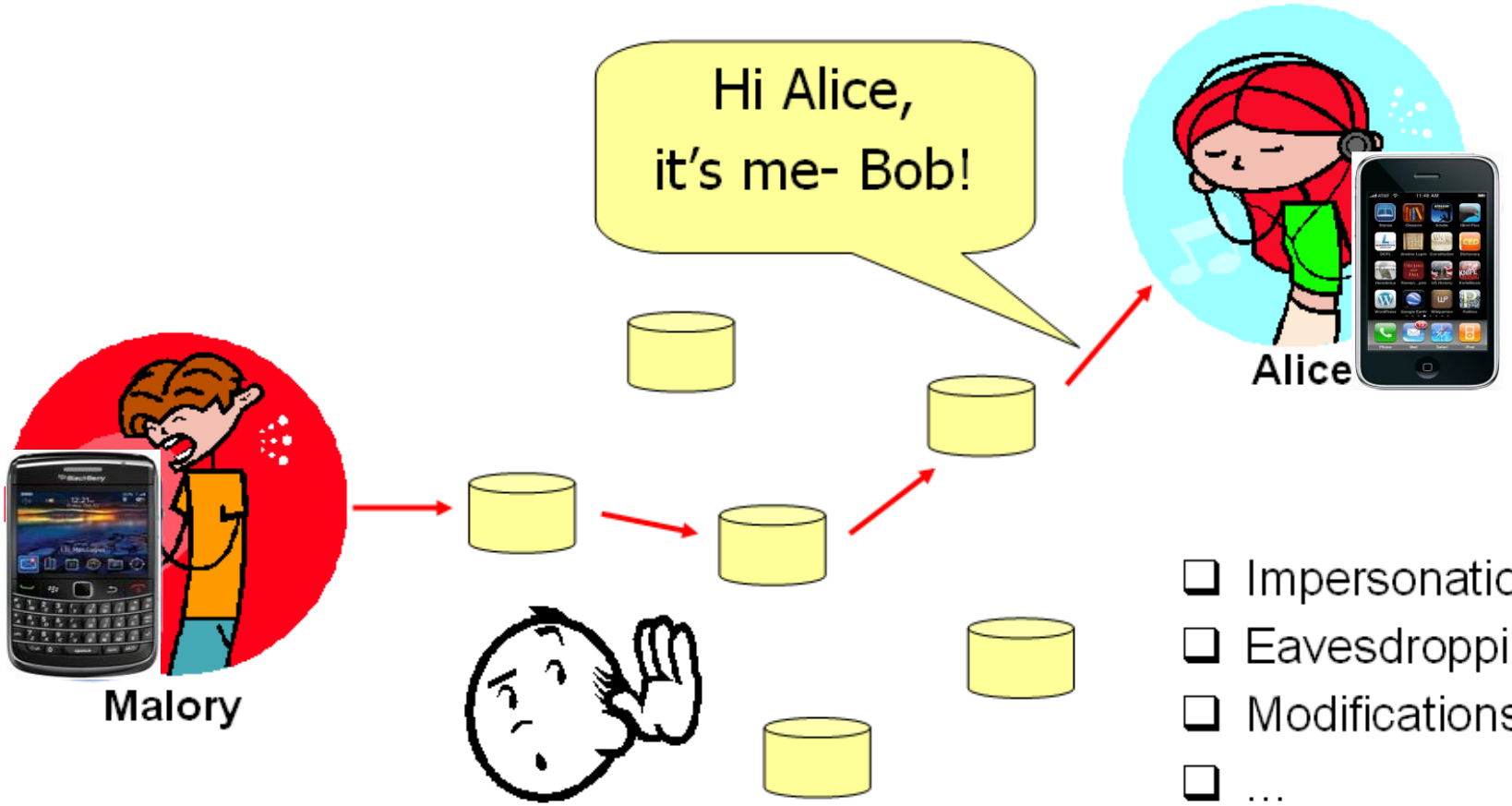


Routing Attacks



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

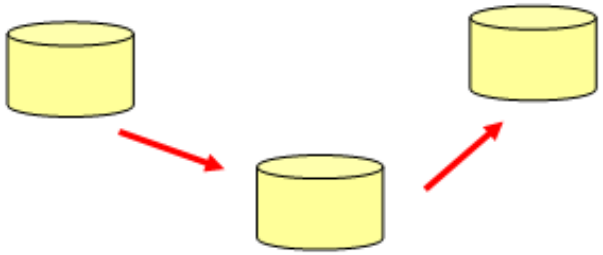
Communication Attacks



- 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-key** 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 a Key Generation Center (KGC) to generate and distribute **private** keys

We evaluate ID-based solutions! However, the solutions proposed here are applicable to both PKI and d symmetric-key systems.

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
- [BF'01] First ID-based encryption scheme
  - Boneh-Franklin scheme uses bilinear mappings
  - set up
    - 2 groups $\mathbb{G}_1, \mathbb{G}_2$ of order q
    - bilinear map $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_2$
    - arbitrary generator $P \in \mathbb{G}_1$
    - hash function $H_1 : \{0,1\}^* \rightarrow \mathbb{G}_1^*$
  - KGC
    - master key $s \in \mathbb{Z}_q^*$
    - 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

$$Q_i = H_1(ID_i \parallel \textbf{'expiry date'})$$

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

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

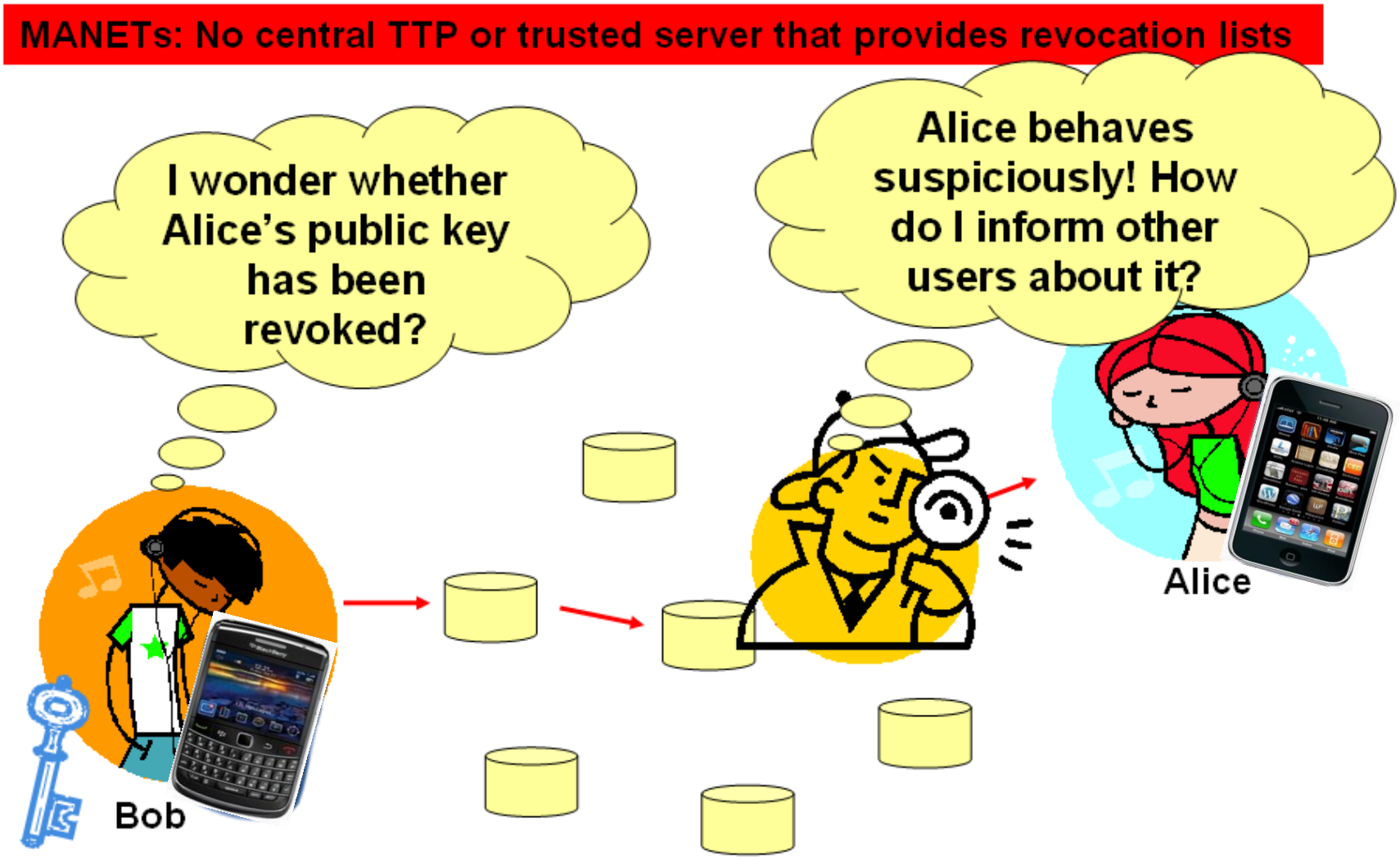
Problems of ID-Based Schemes

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

2. **Key revocation**
   - revocation is 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



Conventional Revocation Schemes

- Certificate Revocation Lists (CRLs)
  - distributed by a central trusted server or TTP to all users
- △CRLs
  - 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 (1)

- **CBC-Based Schemes**
  - **Threshold** based approach [Zhou & Hass '99, Luo et al. '02&'04]
  - **Self-organized** certificate revocation (weighted accusation scheme) [Crépeau et al. '03&'06]
  - **Suicide** for certificate revocation [Clulow & Moore '06&'07]
- **IBC-Based Schemes**
  - **Threshold** based approach [Deng et al. '04, Saxena et al. '04, Zhang et al. '06]

Revocation Schemes for MANETs (2)

- **Game-Theoretical Scheme** [Raya et al.′08]
  - Suitable for **ephemeral** MANETs where contact times between nodes are **short** and neighbors change **frequently** (e.g., VANETs)
  - Reputations are **hard** to build in **ephemeral** MANETS
- **Incentive Based Scheme** [Reidt et al.′09]
  - Encourage rational nodes to sacrifice **short-time** personal utility in favor of **longer term** gains.
  - Inherits the **attractive properties** of suicide-based revocation (i.e., immediacy & abuse resistance)
  - **Reward** a node for a justified suicide by employing a periodically available **Trusted Authority** (TA)

Binary Decision and Multi-level Decisions on Nodes' Behavior

- **Binary decision**: classification of nodes' behavior in all previous schemes: **good** or **bad**.
  - Advantages: simple and easy to implement.
  - Disadvantages:
    - The **binary** behavior differentiation omits the actual **cause** and the **degree** of misbehavior.
    - Some misbehavior may just happen **accidently** and last only for a **short time** (misbehavior due to temporary network congestion, etc.).
- **Multi-level decisions**: classifying nodes behavior into multi-categories of misbehavior.
  - This is a more reasonable **solution**: **collecting more information** about nodes that misbehave accidently instead of evicting them immediately.

Proposed Key Revocation Schemes with Binary and Multi-level Decisions

We consider two scenarios

Binary decisions of misbehavior

$\Downarrow$

Majority voting trust model

Multi-level decision for multi-categories of misbehavior

$\Downarrow$

Dirichlet multinomial model

Pre-Conditions

- **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
- **System assumptions**
  1. bidirectional communication links
  2. each node has a monitoring scheme implemented
  3. each node has a unique identity
  4. each node knows identities and hop-distance of its one-hop neighbors
  5. nodes obtain keys from off-line KGC before joining network

Scheme 1: Key Revocation with Binary Decision

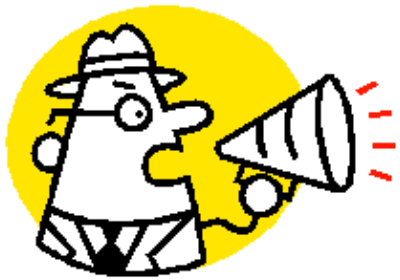
Key Renewal and Key Format

- **Renew key** if previous key is
  - revoked
  - compromised
  - expired

- **New keys issued for same identity**
  - $Q_i = H_1(ID_i \parallel t_i \parallel v_i)$
  - 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 consisting of accusation values $a^i_{j,i}$

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

  - N_i: a set of the members of 1-hop neighbors
  - $a^i_{j,i} = 0$, ID_i marks ID_j as trustworthy
  - $a^i_{j,i} = 1$, 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

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

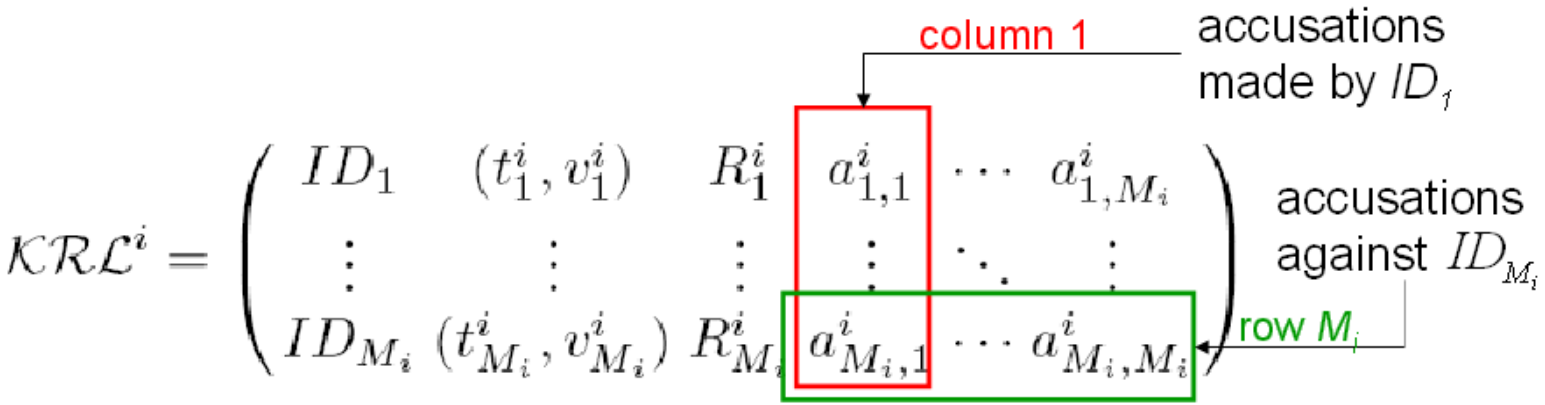
- **Harakiri** messages ***hm***
  - upon noticing that private key d_i is compromised, ID_i broadcasts

    $hm_i = (ID_i, d_i, Q_i, t_i, v_i, \text{“revoke"}, hopcount)$

- **Messages** send to 1-hop neighborhood
  - verify authenticity and forward
  - repeated m times

Accusation Scheme

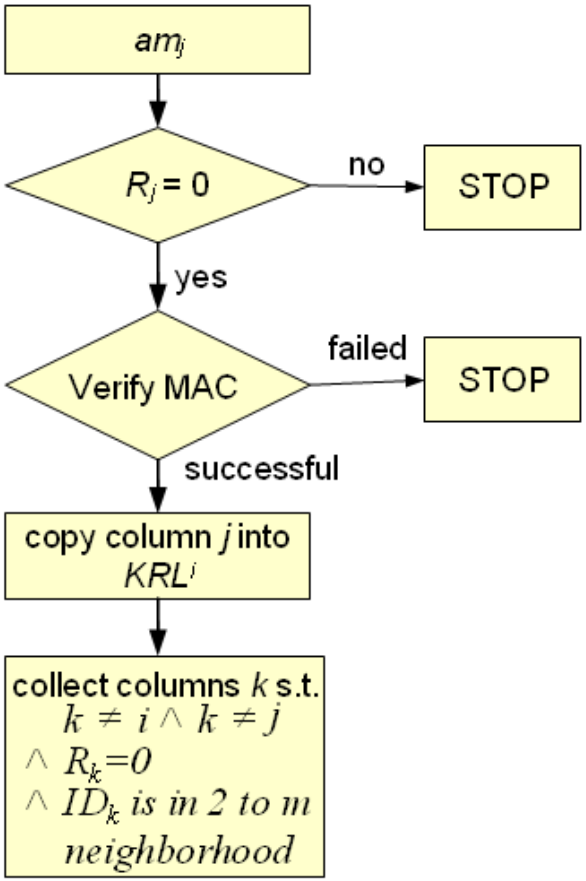
Every node ID_i generates key revocation list KRL^i from its own ***am*** and received ***am & hm***



- M_i number of nodes in m-hop neighborhood
- node i considers the public key Q_j of node j as revoked if revocation value $R_j^i = 1$: $R_j^i = 1$ **if** t_j^i **expired or** $a_{j,i}^i = 1$ **or** $a_{j,j}^i = 1$ **or** $\sum_{k=1}^{M_i} a_{j,k}^i > \delta$
- δ is the threshold for revoking a key

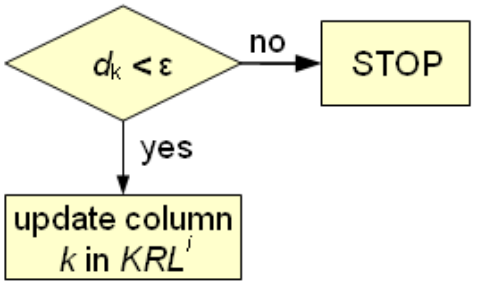
Update Key Revocation List (KRL)

ID_i **repeats** for all received accusation messages am_j



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

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

Recap Revocation Scheme

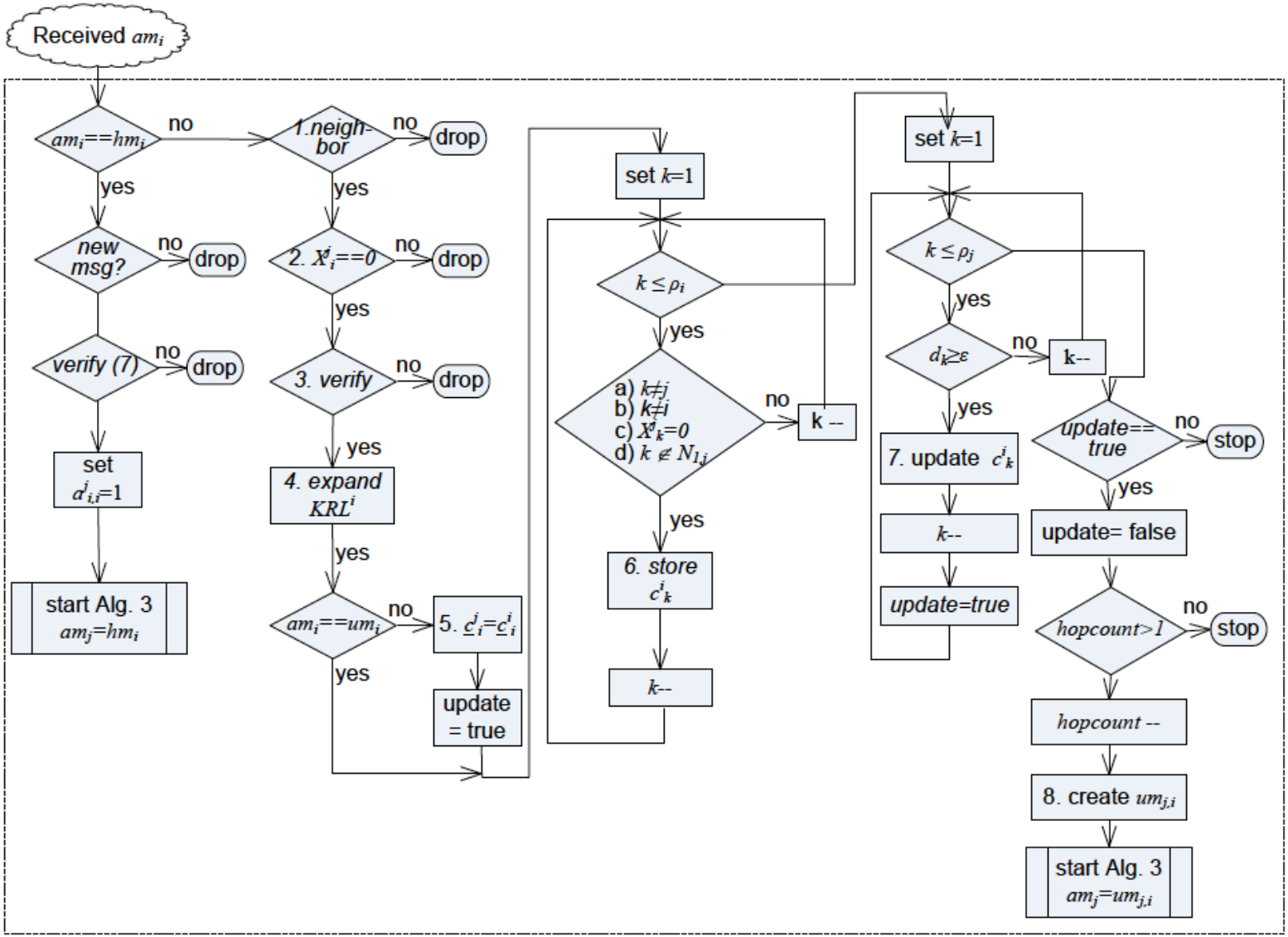
Neighborhood Watch (NW)

Propagation

Accusation Scheme

Harakiri

Flowchart Revocation Algorithm for Update KRL



Security Analysis (1): Outsider Attacks

- Routing attacks prevented by using **secure routing protocols**
- Eavesdropping prevented by using **secure AKE protocols**
- Message authentication and integrity are protected with **pre-shared keys**
- **battery exhaustion attack** prevented by only accepting accusation messages from trusted one-hop neighbors
- If an adversary **spoofs the identity** of a trusted one-hop neighbor, the attack would be detected when verifying the authenticity of the first message.

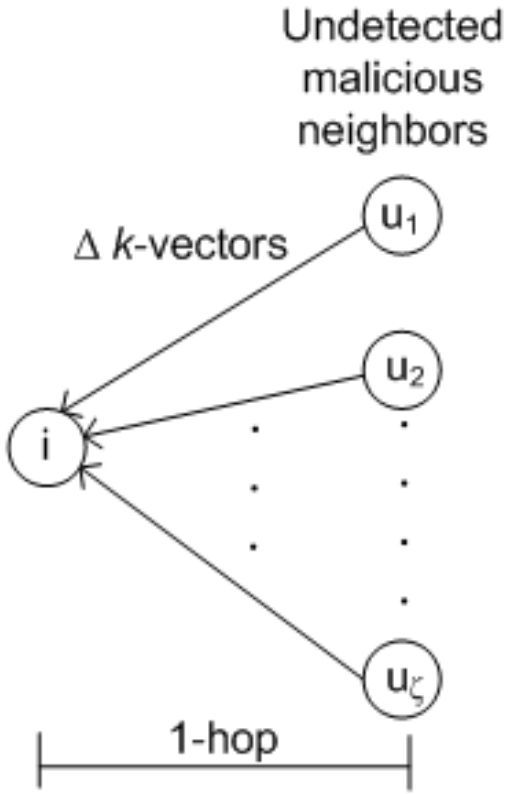
Security Analysis (2): Non-colluding Insiders

- **Sybil Attacks**
  - Malicious nodes could try to bypass security parameter δ by fabricating δ different identities, so called sybil attack.
  - **Sybil attacks requiring keying material** are prevented by using **ID-based public keys** of a fixed format, i.e. upon identifying to the KGC, a node can only obtain one possible valid private key for a specific expiry date.
  - **Sybil attack that does not require keying material** is prevented by choice of security parameters δ and ε.
- **Roaming Adversaries**: By selecting *m* sufficiently large and the expiry intervals small, roaming adversaries have to travel fast to escape the revocation of their keys.

Security Analysis (3): Colluding *l*-hop Neighbors

Colluding one-hop neighbors

- **Monitoring scheme**
  - **false negative rate** β
  - undetected malicious one-hop neighbors $n_u^i = \beta n_m^i$ (n_m^i is the number of i's malicious one-hop neighbors)
- **Altering direct** accusations
  - prevented if $\beta < \frac{\delta}{\sigma_i}$ (σ_i is the sum of i's honest one-hop neighbors and malicious one-hop neighbors)
- **Altering reported** accusations
  - prevented if $\beta < \frac{1}{\sigma_i}(\lfloor \frac{\varepsilon}{2} + 1 \rfloor)$



Scheme 2: Key Revocation in MANETs based on Dirichlet Multinomial Model

- **Model**
  - Suppose that the behavior of network nodes falls into one of **three possible categories**: good, suspicious and malicious behavior.
  - Assume that the observed data are gathered by a **multinomial experiment** and therefore follows a **multinomial distribution**.
  - Use the 3**-dimension Dirichlet distribution** as the **prior distribution** of the unknown probabilities.
  - After obtaining the observation data, compute the **posterior probability expectation** of unknown parameters and make the corresponding response.

Dirichlet-Multinomial

- The **multinomial Dirichlet density function** over Θ is

$$f(\vec{p} \mid \vec{r}, \vec{a}) = \frac{\Gamma\left(\sum_{i=1}^{k}(r(\theta_i) + \mathcal{C}a(\theta_i))\right)}{\prod_{i=1}^{k}\Gamma\left(r(\theta_i) + \mathcal{C}a(\theta_i)\right)} \prod_{i=1}^{k} p(\theta_i)^{(r(\theta_i)+\mathcal{C}a(\theta_i)-1)},$$

- The **prior constant** $\mathcal{C}$ can be set to $\mathcal{C} = 2$ when a uniform distribution over binary state spaces is assumed.
- $r(\theta_i) + \mathcal{C}a(\theta_i)$ is called the **evidence vector**. $r(\theta_i)$ is the information obtained from the observations and $\mathcal{C}a(\theta_i)$ is the prior uncertainty.
- The **probability expectation** of any of the k random variables can be computed as: $\mathbb{E}(p(\theta_i) \mid \vec{r}, \vec{a}) = \frac{r(\theta_i)+\mathcal{C}a(\theta_i)}{\mathcal{C}+\sum_{i=1}^{k} r(\theta_i)}$.

A New Approach for Key Revocation with Multi-level Decisions in MANETs

Bayesian Model of Node Behavior Analysis:

- Network nodes' behavior falls into one of **three possible categories**.
- The observed data are gathered by a **multinomial experiment**.
- **3-dimension Dirichlet distribution** is used as the **prior distribution** of the unknown probabilities.
- The **posterior probability expectation** of unknown parameters is computed to make the corresponding response.

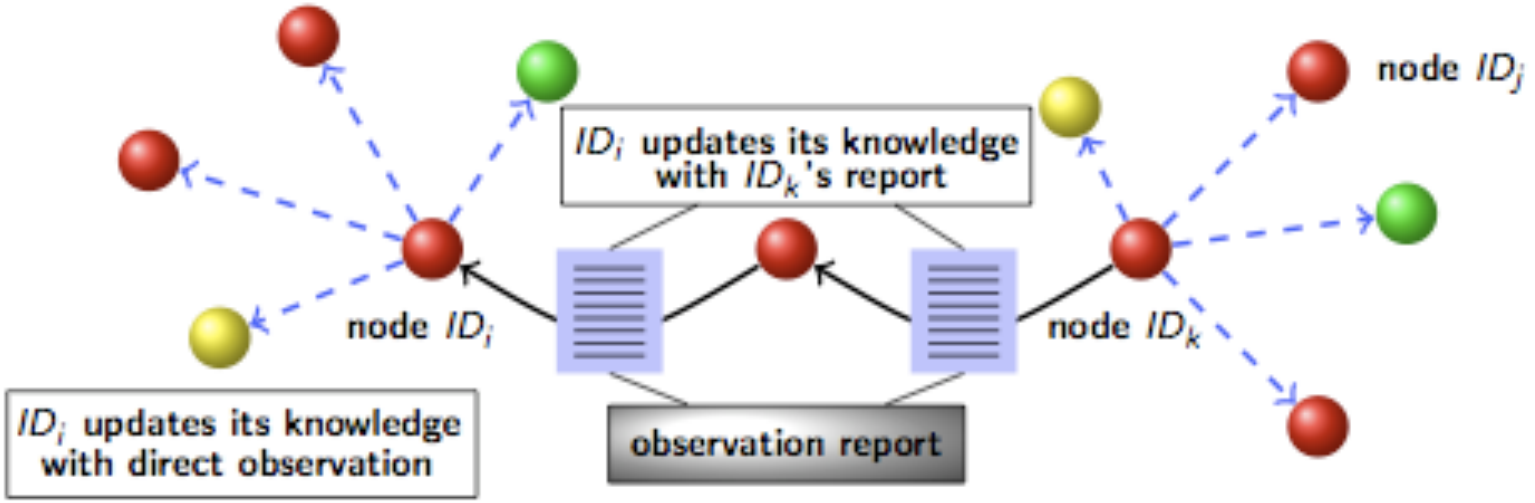


Figure: ID_i updates its knowledge about other nodes' behavior based on its direct observation and ID_k's report

Overview of Protocol

Step 1. Network Initialization

- Generation of system parameters
- Registration of network nodes
- Classification of node behavior

Step 2. Neighborhood Watch

- Monitor neighbors' behavior and generate observation matrix
- Update key status of nodes with direct observations

Step 3. Authenticated Information Dissemination

- Disseminate nodes' direct observations to all m-hop neighbors in an authenticated way by using a keyed-hash function

Step 4. Filter of False Statements

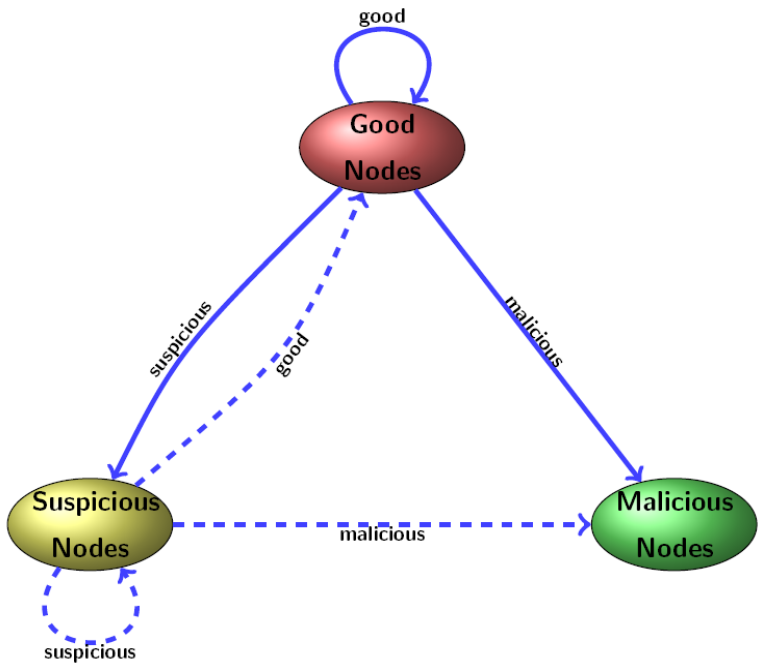
- Filter out potentially false statements statistically
- Update key status of nodes based on Dempster-Shafer theory

Step 5. Multilevel Response for Malicious Nodes

- Revoke keys of nodes showing malicious behavior
- Cease communication with nodes showing suspicious behavior and keep observing their behavior for further decision

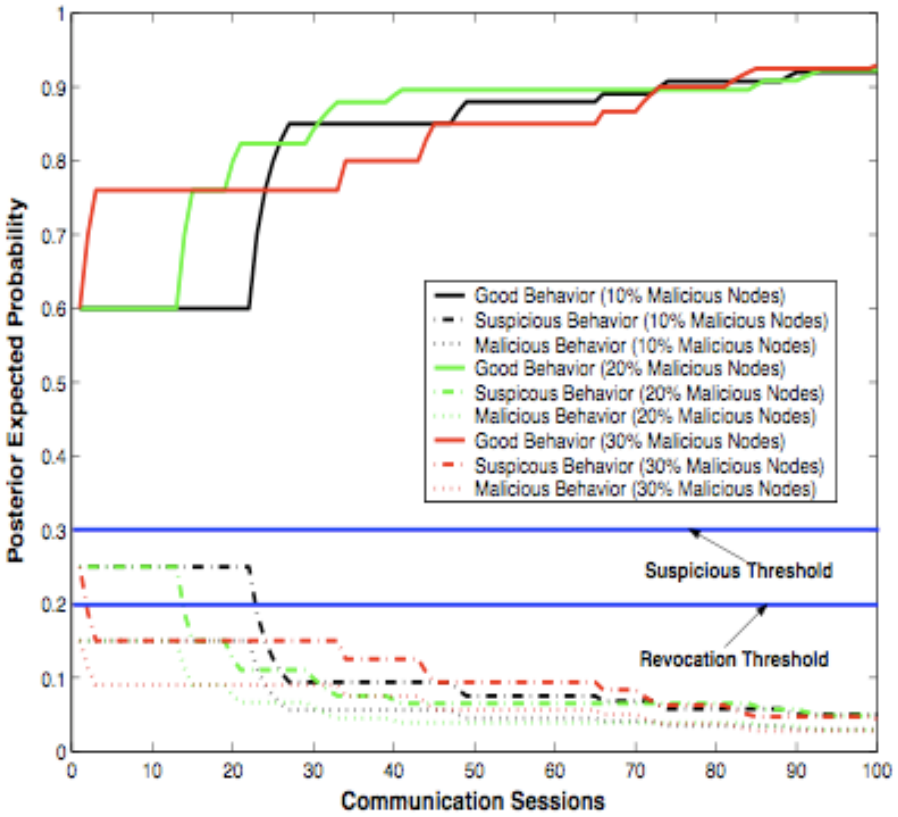
Classification of node behavior

- State space $\Theta = \{\theta_g, \theta_s, \theta_m\}$: θ_g, **good**; θ_s, **suspicious** ; and θ_m, **malicious**
- Three behavior sets: $\mathbb{B}_g$, **good behavior**; $\mathbb{B}_s$, **suspicious behavior**; and $\mathbb{B}_m$, **malicious behavior**
- Node behavior analysis: **3-dimension Dirichlet distribution Dir($\alpha_g, \alpha_m, \alpha_s$)**

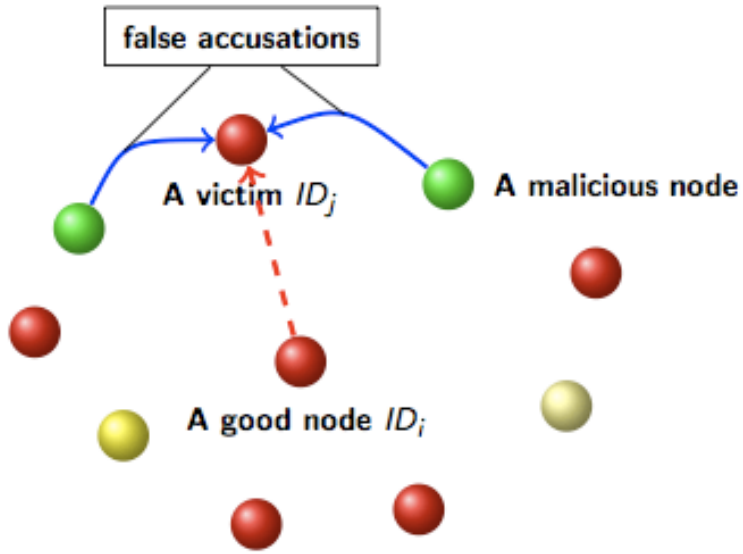


Protocol Simulation and Analysis

False Statement Attacks by Collusive Adversaries (I)

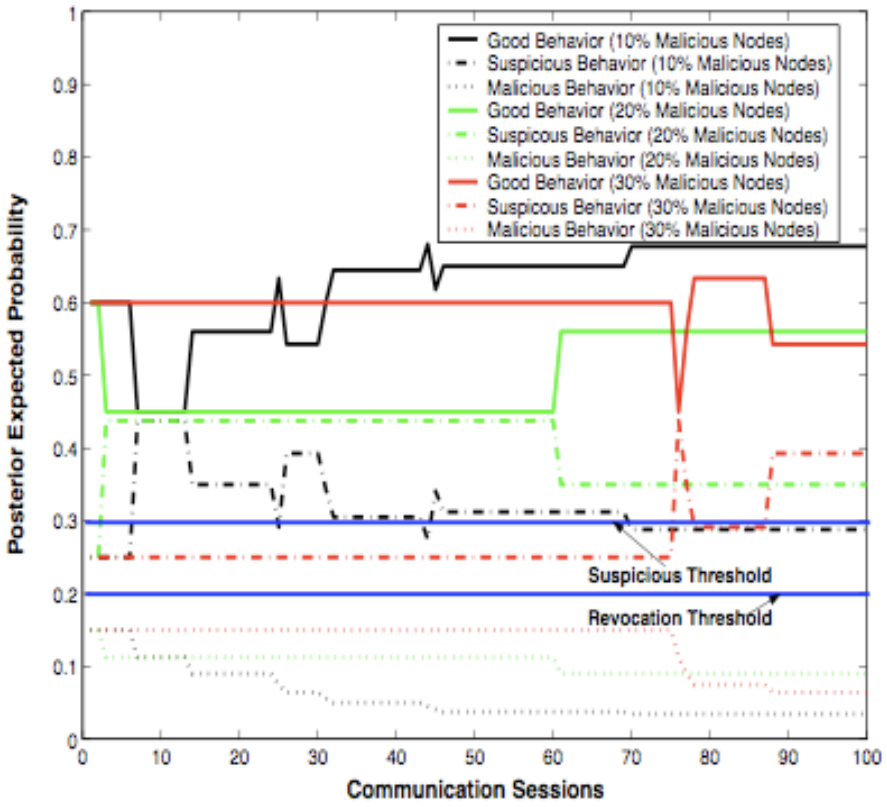


(a) A good node's opinion about the key status of the other good node selected by collusive adversaries

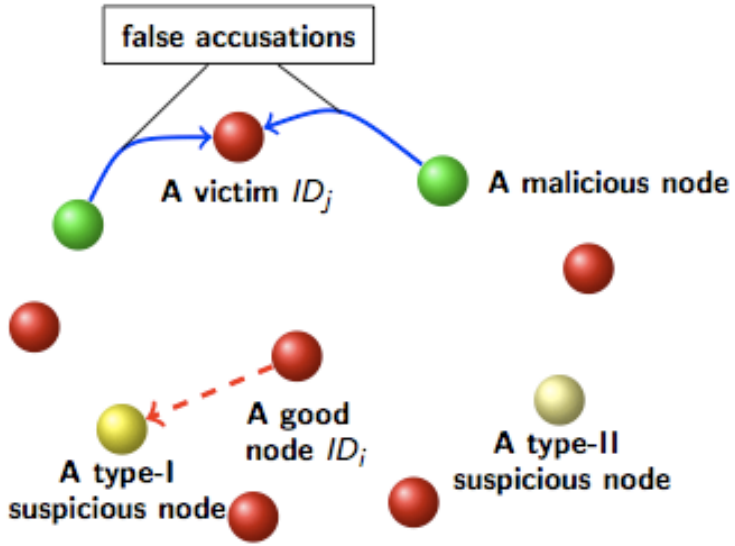


The left figure shows that false accusations from collusive adversaries cannot affect a good node ID_i's opinion about the victim ID_j's behavior.

False Statement Attacks by Collusive Adversaries (II)



(b) A good node's opinion about the key status of a type-I suspicious node



- A type-I suspicious node shows suspicious behavior followed by good behavior.
- The left figure shows that a type-I suspicious node can be trusted again by a good node ID_i after it behaves normally.

Summary for Scheme 1

Features of the proposed **self-organized** key revocation scheme with binary decision 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 (δ, ε, m)
- Efficient due to use of **pre-shared asymmetric keys** with MACs and propagation to m-hop neighborhood
- Designed **ID-based key format** allows key renewal

Summary of Scheme 2

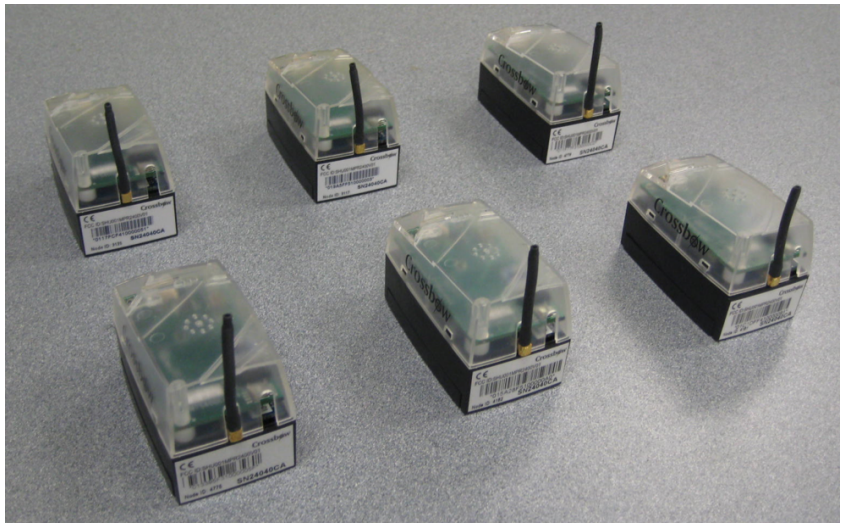
- A novel **self-organized** key revocation scheme based on the **Dirichlet multinomial model** and **identity-based cryptography**
- A **theoretically sound basis** for nodes analyzing and predicting peers' behavior based on their own observations and other nodes' reports
- **Three** categories of nodes' behavior: **good** behavior, **suspicious** behavior, and **malicious** behavior
- **Multilevel response** according to the severity of malicious behavior.
- Good **attack-resistant** properties with appropriate selection of design parameters.

Extensions of the Two Basic Revocation Schemes

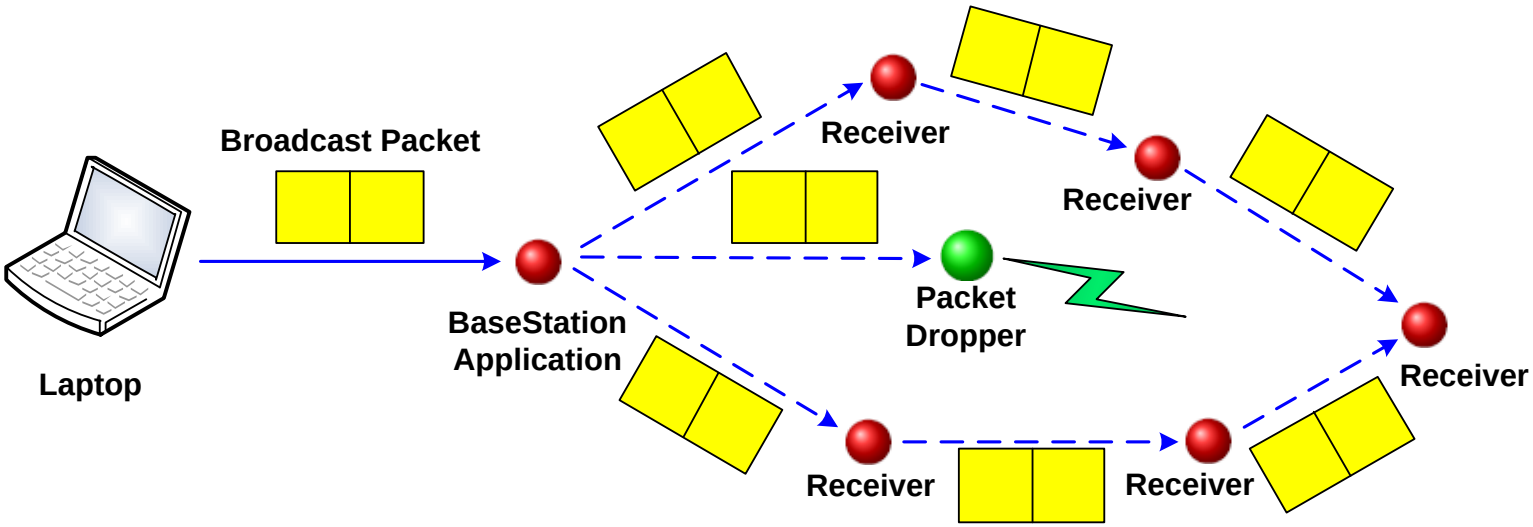
1. **Distributed** On-line KGC
2. Regaining Trust
3. Sleeping Nodes
4. **Confidential** Accusations
5. Dedicated Key Pairs:
6. Crypto Agility: adopt to **PKI or symmetric-key** schemes
7. Adapting Scheme to Hostile Environments
8. **Adaptive** Monitoring Schemes and Security Parameters
9. Network-wide **Revocations**
10. Adversary Models

Experiment Platform

- Sensor node: **MICAz** mote
  - a **low-power** 8-bit microcontroller **ATmega128L**
  - 128 KBytes program flash memory
  - 512 KBytes measurement flash
  - 4 KBytes configuration EEPROM
  - Maximum clock frequency: 8 MHz
  - **ZigBee** transceiver **CC2420** (Data rate: 250 kbps; Packet size: up to 128 bytes (with a payload of 102 bytes))
  - Operation system: **TinyOS**



Experiment Setup (in progress)



- The testbed consists of **one laptop sender** and **seven MICAz motes**.
- The laptop connects to an MICAz mote through a **programming board** and periodically generate a broadcat message.

Experiment Setup Cont. (in progress)

- One of the MICAz motes (the green one) is configured to **drop** the broadcast packet.
- Other motes **record** the behavior of the green one and perform the **key revocation**.
- The **pairwise keys** among sensor nodes are computed using **bilinear pairing** during the **neighborhood discovery** phase.
- The **message authentication code** (MAC) is calculated using a **keyed hash function**.

Implementation of Bilinear Pairing on MICAz Motes (1)

Bilinear pairings for binary elliptic curves:

- A **supersingular** binary curve: $y^2 + y = x^3 + x + b$
- The **order** of this curve is $N = 2^m + 1 \pm 2^{\frac{m+1}{2}}$
- The **embedding degree** is $k = 4$ (i.e., the least integer s.t. N divides $2^{km} - 1$)
- Choosing $T = 2^m - N$ and a prime r dividing N, Barreto *et al.* defined the **reduced η_T pairing**:

$$\begin{aligned} \eta_T(\cdot,\cdot) &: E(\mathbb{F}_{2^m})[r] \times E(\mathbb{F}_{2^m})[r] \to \mathbb{F}^*_{2^{4m}} \\ \eta_T(P,Q) &= f_{T',P'}(\psi(Q))^{\frac{2^{4m}-1}{N}}, \end{aligned}$$

where $T' = \pm T$ and $P' = \pm P$. The function f is a **Miller function** and ψ is the **distortion map** $\psi(x, y) = (x^2 + s, y + sx + t)$.

Implementation of Bilinear Pairing on MICAz Motes (2)

- **Field** representation: $\mathbb{F}_{2^{271}} = \mathbb{F}_2[x]/x^{271} + x^{207} + x^{175} + x^{111} + 1$
- Pairing-friendly **supersingular** curve $E : y^2 + y = x^3 + x$
- Let $q = 2^{271}$. The extension field $\mathbb{F}_{q^4}$ is represented using **tower extensions** $\mathbb{F}_q \to \mathbb{F}_{q^2} \to \mathbb{F}_{q^4}$:
  - $\mathbb{F}_{q^2} = \mathbb{F}_q[s]/(s^2 + s + 1)$,
  - $\mathbb{F}_{q^4} = \mathbb{F}_{q^2}[t]/(t^2 + t + s)$.

  A **basis** for $\mathbb{F}_{q^4}$ over $\mathbb{F}_q$ is $\{1, s, t, st\}$.
- The reduced η_T pairing can be computed within 2.5**s** on MICAz motes.

Pairing Computation on Wireless Sensor Nodes

Table: η_T pairing on different wireless sensor nodes

Implementation	Sensor Nodes	Timing (s)
Szczechowiak *et al.*'08	MICAz	10.96
Ishiguro *et al.*'08		5.80
Szczechowiak *et al.*'09		2.66
Fan & Gong'09		**2.5**
Oliveira *et al.*'10		1.90
Szczechowiak *et al.*'08	Tmote Sky	5.25
Szczechowiak *et al.*'09		1.71
Oliveira *et al.*'10		1.27

The contents of the talk are taken from the following 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), ser. LNCS 4104, pp. 224-237, 2006.

X. Fan and G. Gong.
Key Revocation Based on Dirichlet Multinomial Model for Mobile Ad Hoc Networks,
the Proceedings of the Fourth IEEE LCN Workshop on Network Security (WNS 2008), Montreal, October 17, 2008.

K. Hoeper and G. Gong.
Monitoring-Based Key Revocation Schemes for Mobile Ad Hoc Networks: Design and Security Analysis,
Technical Report of Centre for Applied Cryptographic Research (CACR), CACR 2009-15, 2009.

Other Work on MANETs:

Z. Li and G. Gong,
Computationally Efficient Mutual Entity Authentication in Wireless Sensor Networks,
Journal of Ad Hoc Networks, Vol. 9, No. 2, pp. 204-215, 2011.

A. Tassanaviboon and G. Gong.
A Framework Toward a Self-Organizing and Self-Healing Certificate Authority Group in a Content Addressable Network,
The 6th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob 2010), pp. 614-621, 2010.

X. Fan and G. Gong.
Reputation Based Key Revocation for Mobile Ad Hoc Networks, in preparation.