Security Concepts for Wireless Sensor Network

(Vorlesung: SS05- Sensornetze)

University of Mannheim

24 June, 2005

Gastvortrag:
Dirk Westhoff
NEC Europe Ltd. Network Laboratories
Heidelberg, Germany

Empowered by Innovation NEC

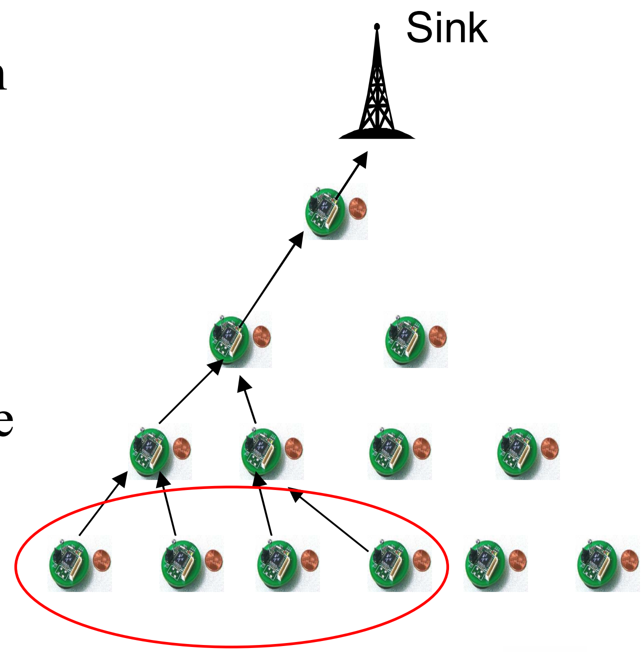
Requirements (func. + security)

functional

- **Data aggregation:**
  data transmission with a good balance between accuracy and energy efficiency to the sink

protection aims

- **Integrity/Authentication**:
  pair-wise data originator authentication or re-recognition for sensed data to ensure that only data from trusted sensors are considered for the data aggregation process
- **Plausibility**:
  plausibility check at the sink node to validate that the aggregated values are reasonable
- **Concealment**:
  Aggregated data need to be concealed end-to-end. Due to the aggregation during multi-hop transmission, concealed end-to-end transmission is not a trivial task.



aggregation area:

e.g. with aggregation function snapshot

- movement
- average
- min-max

Security Concepts*…

Key pre-distribution

1) key managemant scheme for WSNs **(…)** [EsGl02]
key rings for pairwise encryption…

2) topology aware group keying **(TAGK)** [WeGiAc05]
subset of keys per routable region…

3) a lot more…

Integrity/Authentication

4) Time Efficient Stream Loss Tolerant Authentication **(mTESLA)** [Pe et al. 02]
robust and efficient broadcast authentication…

5) Lamport's hash-chains, Merkle's hash tree [Lam78] [Mer??]
chaining of hash functions…

6) Zero Common Knowledge **(ZCK)** [WeWe03a]
extremely cost-efficient pairwise authentication (re-recognition)…

7) Identity Certified Authentication **(IC)** [WeWe03b]
shifting re-recognition to authentication…

8) more e.g. keyed hash chains, res. duckling, pub. key e.g. ECC?

**only for WSN (not for AdHoc)*

Security Concepts*…

Concealment

9) standard or “quasi”-standard RC5 (TinySec), AES-CCS-64 (IEEE 802.15.4)

hop-by-hop encryption with different keying models

10) Concealed Data Aggregation **(CDA)** [GiWeSc04]

E2E encryption in presence of aggregating intermediate nodes…

11) efficient aggregation of encrypted data **(…)** [CaMyTs05]

E2E encryption with diff. key per node + ID-list

Plausibility

12) Secure Information Aggregation **(SIA)** [PrSoPe03]

plausibility evaluation at the access router…

13) energy-accuracy trade-off in WSNs (…) [BuGaSr03]

…

Secure long-term Storage

14) tiny persistent encrypted data storage **(tinyPEDS)** [GiWeMy06]

distributed encrypted long-term storage within WSN…

**only for WSN (not for AdHoc)*

Agenda

- Requirements & Destination Platform
- E2E encryption for reverse multicast traffic
  "CDA: Concealed Data Aggregation"
- Key Pre-Distribution for CDA
  "Topology aware group keying"
- Re-recognition and authentication
  "Zero Common Knowledge"

Empowered by Innovation NEC

Reference Platform

Sensor Node, e.g.

- **Crossbow's MICA mote**
- **Speed: 4 MHz**
- **Flash 128Kbytes**
- **SRAM 4 Kbytes**
- **EEPROM 4Kbytes**
- **2xAA batteries**
- **Energy Ratio: Send/Receive/Compute/Sleep (100:100:10:1)…**
- **TinyOS (event driven), TinySec, TOSSIM, NesC**
- **Critical: Node lifetime and system lifetime:**

Major Metric: WSN's lifetime…

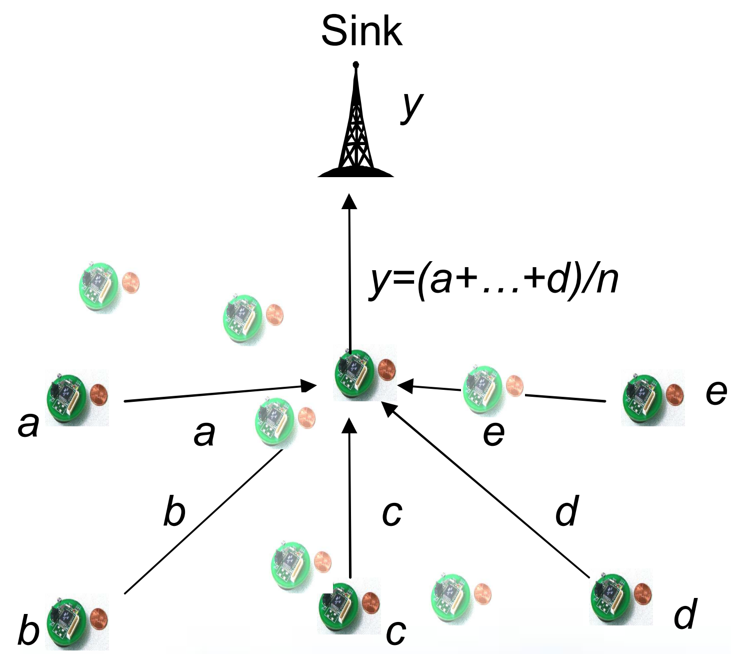
CDA: Concealed Data Aggregation

CDA Problem to be solved…

- **…Merging data aggregation and E2E - encryption**
- data need to be aggregated on its way to the sink node -> saves energy
- data aggregation function is context sensitive

Current proposals: data aggregation + hop-by-hop encryption, e.g. RC5 (single group key)

Our proposal: data aggregation + end-to-end encryption



aggregation function “average” of n sensor nodes

PROS:

- saves energy consuming encryption operations in the backbone…
- no lack of security at aggregating backbone nodes…
- most flexible for aggregator node election process over different epochs

CDA: Concealed Data Aggregation

CDA…

- additive and multiplicative PH

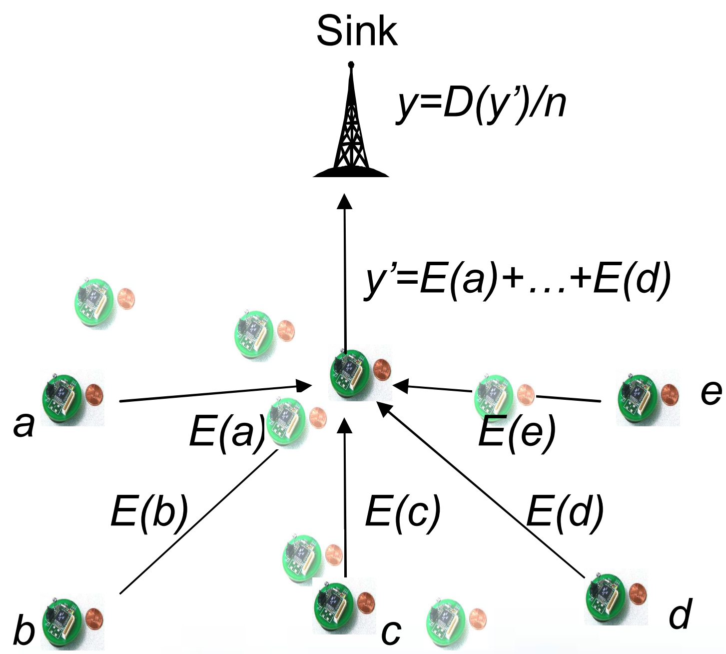
$$a+b=D_k(E_k(a)+E_k(b))$$
$$a*b=D_k(E_k(a)*E_k(b))$$

with rings (Q,+,x) and (R,+,x) and

$$E: K \times Q \to R$$
$$D: K \times R \to Q$$

a,b from *Q*, *k* from *K*

- E.g. by PH from Domingo-Ferrer
- aggregation functions
  - **average** and **movement detection**
  - no min/max => [WiOpt'03]
- suits also for aggregator hierarchies



aggregation function "average"
of n sensor nodes

CDA: Concealed Data Aggregation

PHs…(symmetric vs. asymmetric)

- symmetric, e.g. by Domingo-Ferrer [ISC'02]
  => unsecure for major parameter settings…
- asymmetric, e.g. by Okamota Uchiyama [EUROCRYPT'98]
  => provably secure but encryption and decryption 2 times slower than ECDSA

Threat Analysis…

- extended Dolev-Yao threat model…
- passive and active attacks…

	security cryptoscheme	capture resistance	overall security
Hop-by-hop (RC5, AES)	↗	↘	↘
CDA (sym. PH)	→	→	→
CDA (asym. PH)	↗	↗	↗

CDA: Concealed Data Aggregation

A symmetric and additive Reference PH…

Settings:

1) integer $d \geq 2$

2) large integer g.

/* g should have *i)* many small divisors and at the same time there should be *ii)* many integers less than g that can be inverted modulo g.*/

3) secret key: $k=(r,g')$.

/* $r \in \mathbf{Z}_g$ is chosen such that *i)* $r^{-1} \bmod g$ exists, ii) $\log_{g'} g$ is an integer with small g'.
- set of *cleartext:* $\mathbf{Z}_{g'}$
- set of *ciphertext:* $(\mathbf{Z}_g)^d$. */

Encryption: Randomly split cleartext $a \in \mathbf{Z}_{g'}$ into a secret $a_1, \ldots, a_d \in \mathbf{Z}_{g'}$ such that

1) $a=\sum^d_{j=1} a_j \bmod g'$ and $a_j \in \mathbf{Z}_{g'}$.

2) $E_k(a)=(a_1 r \bmod g,\ a_2 r^2 \bmod g, \ldots,\ a_d r^d \bmod g)$.

Decryption: Compute the j-th coordinate by

1) $r^{-j} \bmod g$ to retrieve $a_j \bmod g$.

2) In order to obtain a compute

$$D_k(E_k(a)) = \sum^d_{j=1} a_j \bmod g'.$$

Addition:

1) The ciphertext operation + is done componentwise.

CDA: Concealed Data Aggregation

Example:

CDA for "average" with reference PH

e.g. public parameters: d=2, g=28

key: r=3, g'=7

Sensor nodes:

S1: $E_{(3,7)}(1)=E_{(3,7)}(4,4)=(12,8)$

S2: $E_{(3,7)}(2)=E_{(3,7)}(7,2)=(21,18)$

S3: $E_{(3,7)}(1)=E_{(3,7)}(6,2)=(18,18)$

S4: $E_{(3,7)}(0)=E_{(3,7)}(6,2)= (9,8)$

S5: $E_{(3,7)}(1)=E_{(3,7)}(3,12)= (9,24)$

Aggregator node:

(12+21+18+9+9 mod 28,

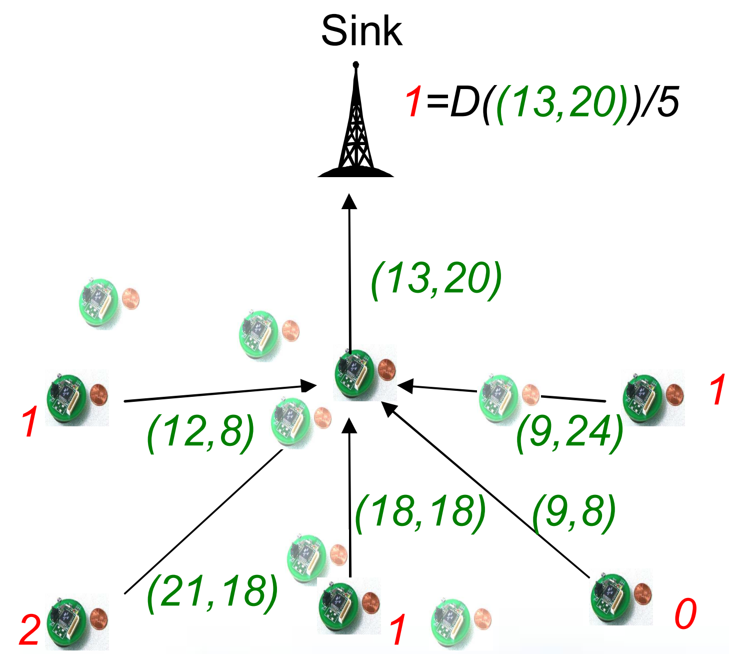
8+18+18+8+24 mod 28) =(13,20)

Sink node:

$D_{(3,7)}(13,20)$ = (13x19 mod 28, 20x19^2 mod 28) mod 7

= (23,24) mod 7 = 5

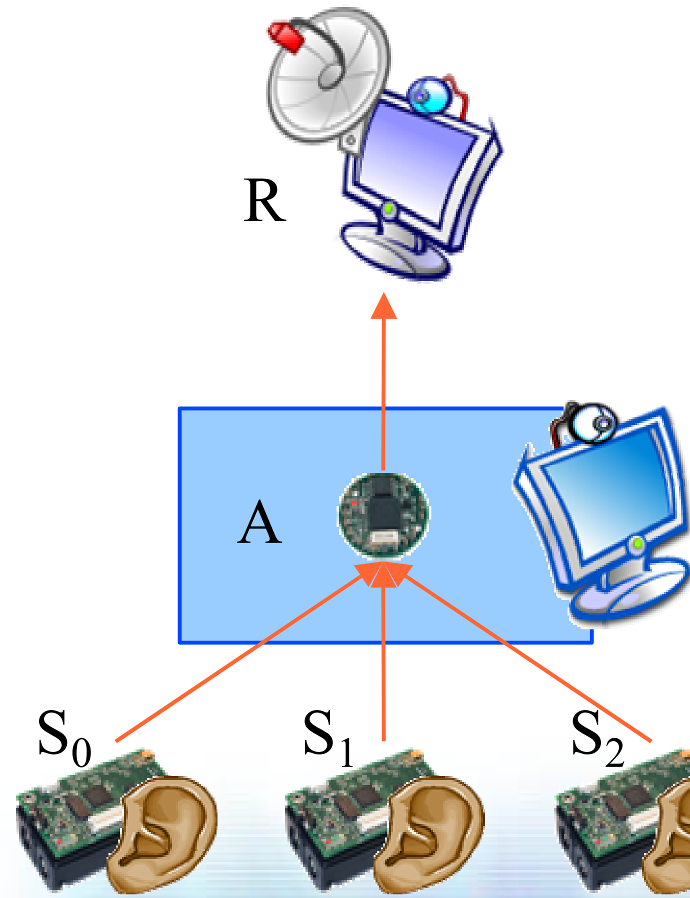
finally 5/5=1 (five nodes have been involved)



CDA: Performance and Demonstrator…

Demonstrator (Movement Detection)

- 3 sensor nodes sensing sound
- Visual interfaces at A and R



Performance…

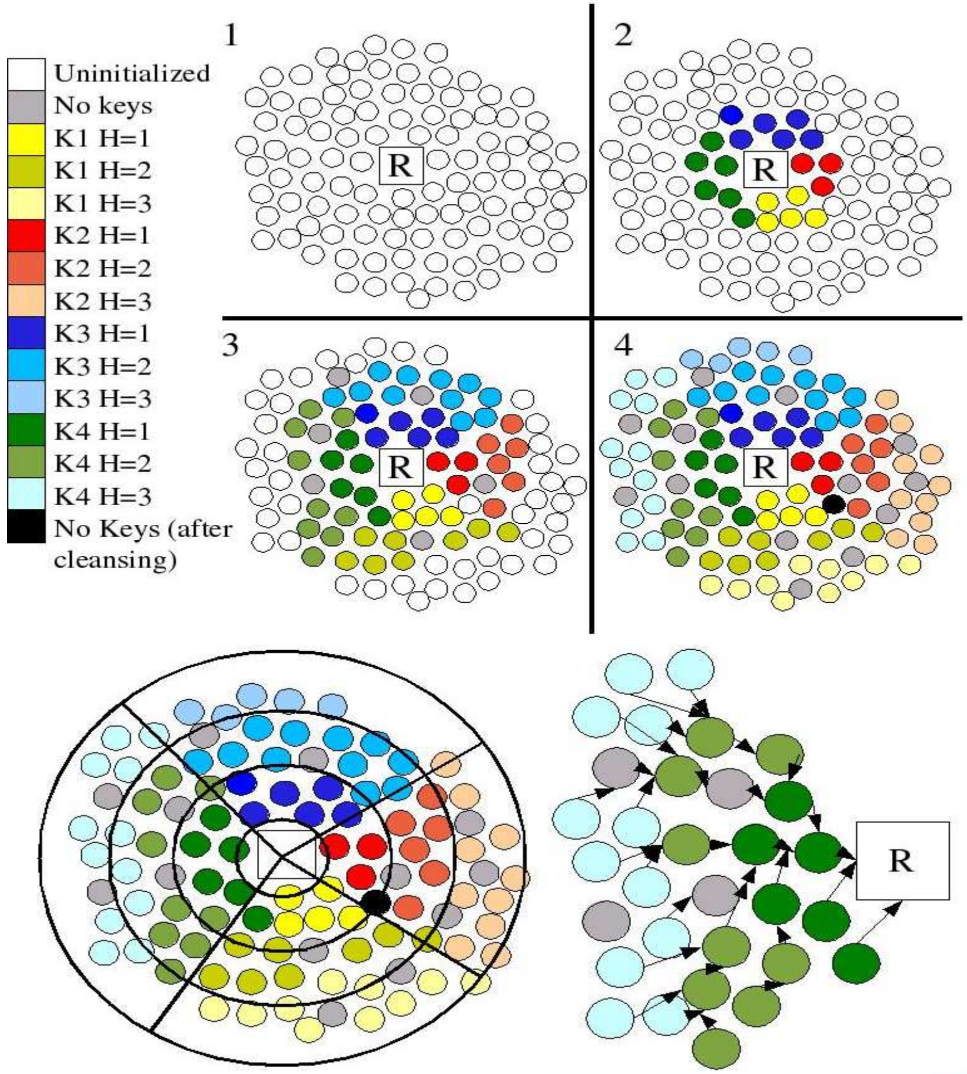
	encrypt [cc]	add [cc]	decrypt [cc]
	at Si	at A	at R
RC5	236	4	236
DF d=2	1951	1452	2330
DF d=3	3481	2178	3136
DF d=4	4277	2904	3942

But…

- ❖ CDA beats H-by-H with >6-9 sensor nodes per aggregator node
- ❖ CDA ensures flexible aggregator node election

Empowered by Innovation NEC

Pre Key-distribution for CDA…



"Topology Aware Group Keying"

Pre-Configuration

- same key pool and key Id-list at each node (manufacturer)

Roll Out

- randomly but equally distributed with sink in the centre

Bootstrapping

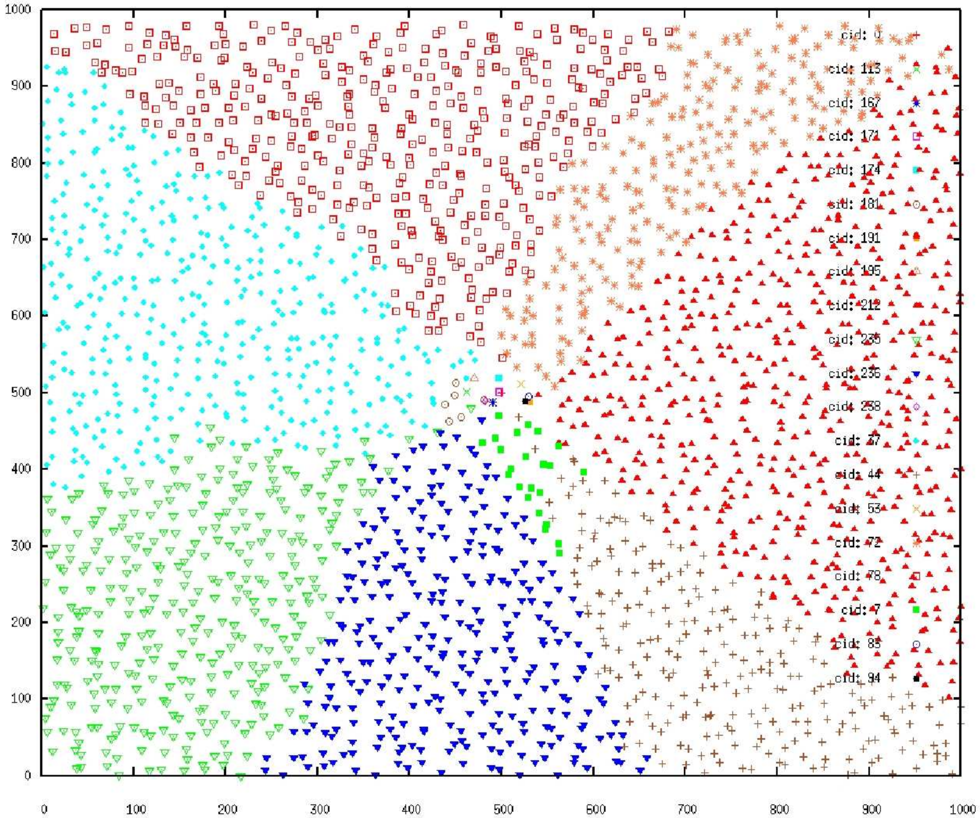
- Subset of key-pool per RR
- Each node stores 0/1 key

Cleansing

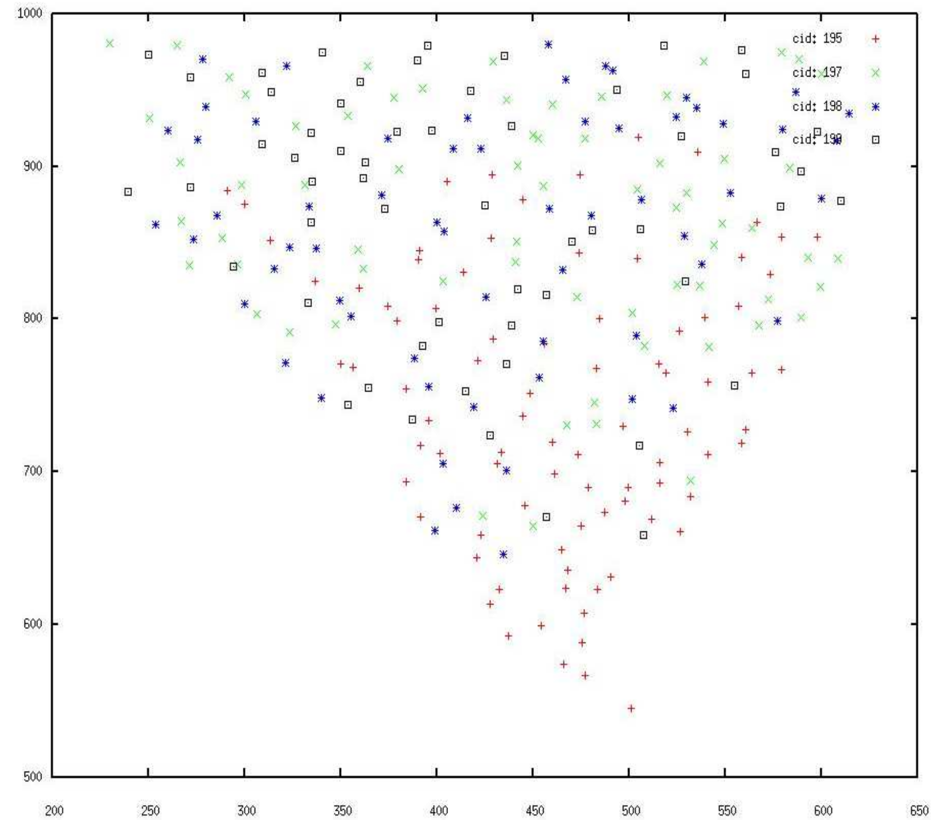
- nodes that have not been reachable delete key pool

Pre Key-distribution for CDA…

WSN: 8 RRs, 7 nearly same size



Per RR 3-5 keys, per epoch one

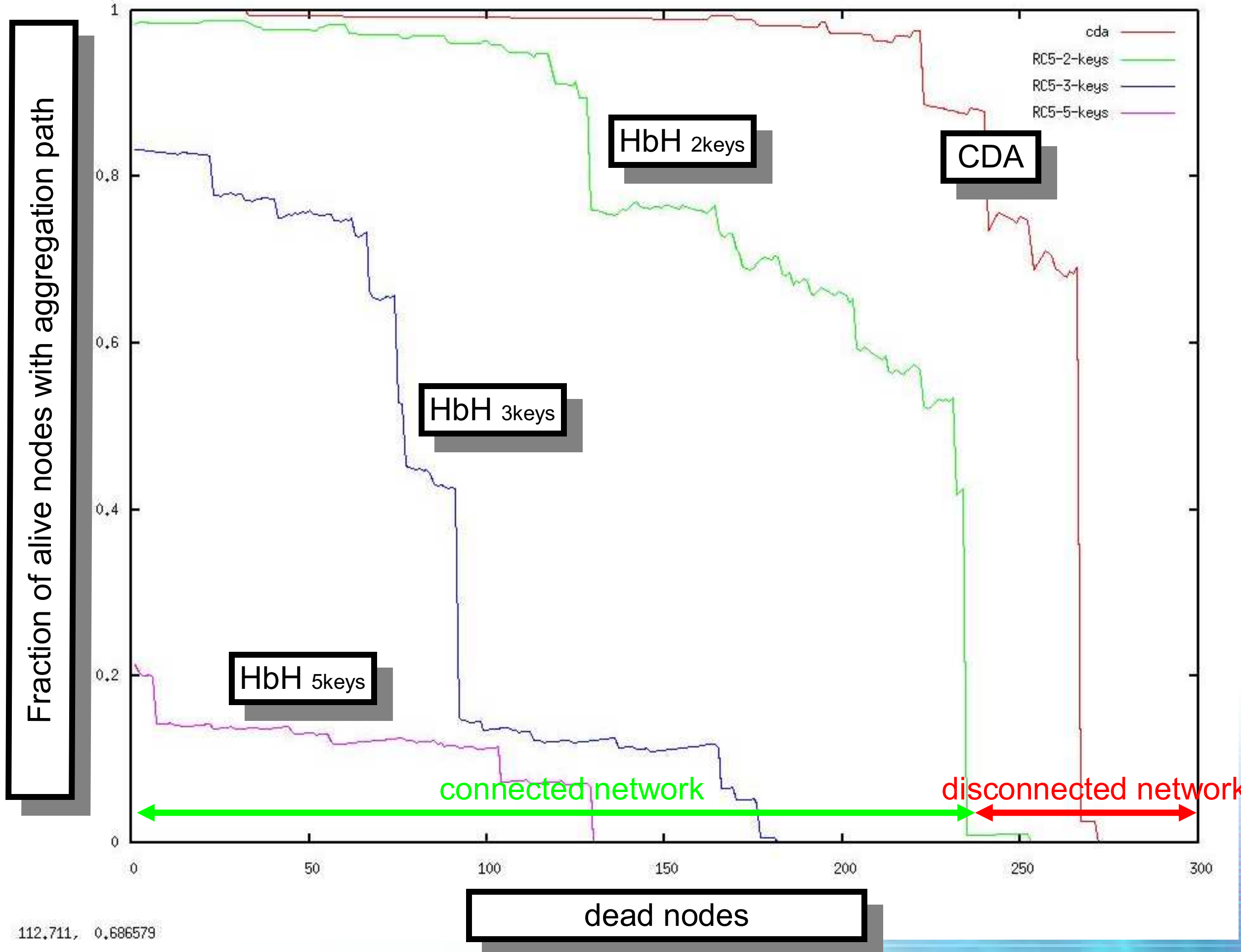


Glomosim: **2548 nodes 1000x1000, static radio range, 20 neighbors, 10 min simulation time…**

Empowered by Innovation NEC

Robustness CDA vs. H-b-H…

…indicated by number of alive pathes from sensor nodes to sink node

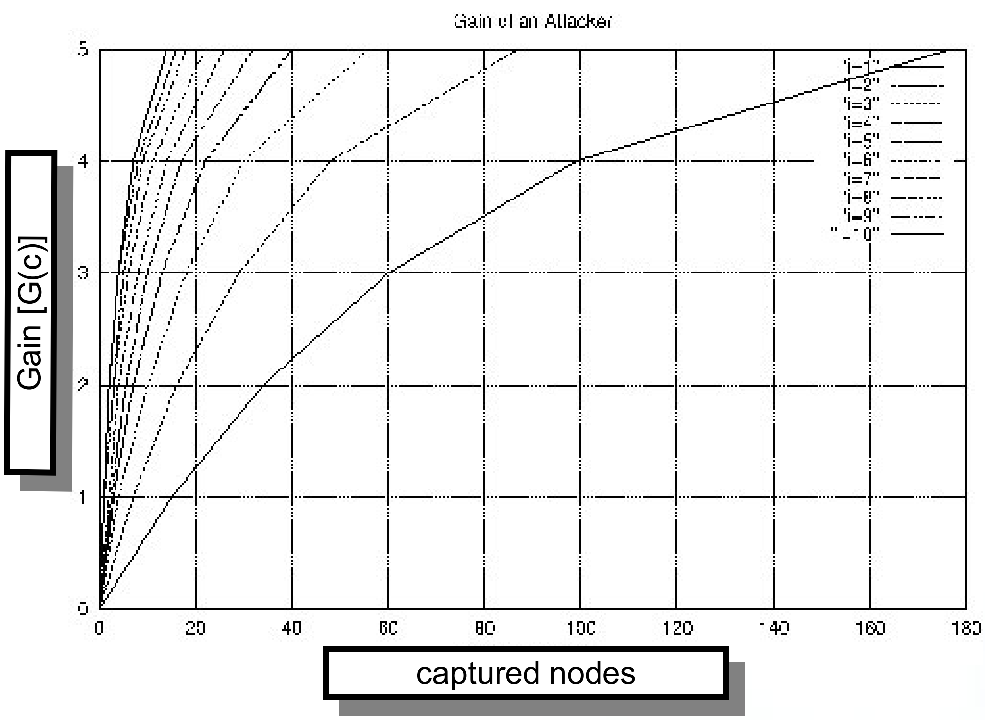


Glomosim: **one RR with 318 nodes, static radio range, 20 neighbors, 10 min simulation time…**

Empowered by Innovation NEC

Security (Capture resistance)…

Average number of captured nodes per distance *i* that ensure a particular level of gain for the attacker with a probability higher *80%*.



Gain $P[G(c)<G(c+1)]$

"unaware" attacker

$$\frac{\sum_{i=1}^{l} P(i,l)}{l} \; \frac{r-(c-1)}{r}$$

"smart" attacker

$$P(l,l)\,\frac{r-(c-1)}{r}$$

parameters: l=10, 5 keys, P(i,l)=i/10 => unaware 50 (vs. 4) nodes, smart 12 (vs. 1) nodes

Empowered by Innovation NEC

Conclusion/Next Steps…

Conclusion

- CDA much more robust and flexible for reverse multicast traffic than H-by-H enc.
- better *overall* security
- Currently: CDA with PH supporting
  aggregation functions “average”
  “*detect moving obstacle*”

Empowered by Innovation NEC

Conclusion/Next Steps…

Next Steps

- CDA supporting min/max operation e.g. OPES (done WiOpt'05)
- CDA on asymmetric PH e.g. ElGamal on elliptic curve points (in prep. ACM SASN)
- tinyPEDS – tiny persistent encrypted data storage (in prep. Infocom)
- FP6 STREP UbiSec&Sens – fully fledged security architecture

ZCK (1)…

- Two people meet and want to authenticate
- There is no supporting infrastructure like passport system
- Establish a step-by-step trust relationship based on personal experience
- These people want to be able to **recognize** each other again

⇒ suitable for

- sensor networks
- P2P networks,
- secure routing,
- secure data aggregation, etc.

ZCK (2)…

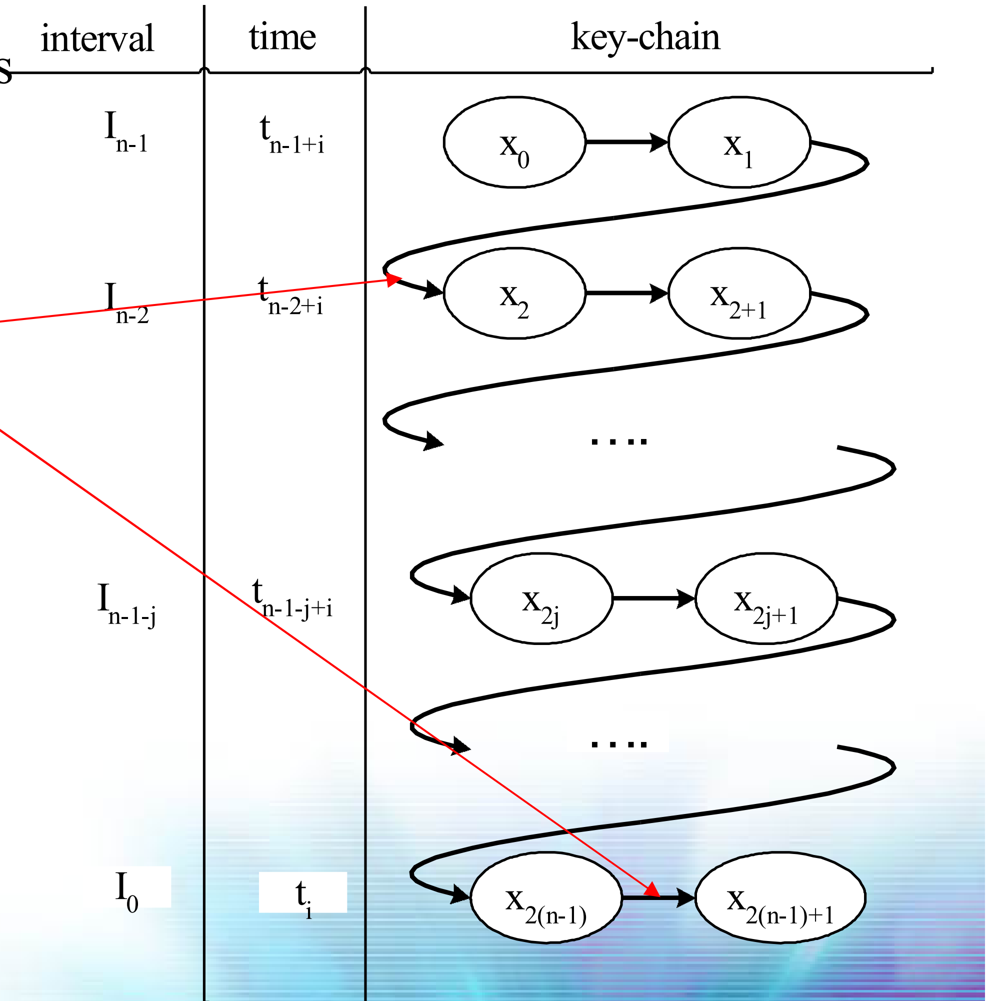
- Based on Lamport's hash chain:
  - 2 hash chains $x_{i+1} = h(x_i)$
  - one generated at A, the other at B
  - anchors x_0 are "*private keys*" per communication pair
  - final elements x_n are "*public keys*"
- Public key is bound to service (not device) at first meeting
- *A* needs to store *B*'s public key which is then associated to previous experience

IC (1)…

- **Similarity:** same functionality as a MAC scheme using a symmetric key determined by an asymmetric key-exchange protocol
- **Provides:** "*proof of identity*" for ZCK authentication protocol
  - *Exchange a key that in turn is used for authentication in the ZCK protocol*
- **Assumes:** some infrastructure, devices with moderate computing power, and loose time synchronization

IC (2)…

- Divide time into intervals let a set of keys be valid for only one time interval
- Alice holds secret anchor x_0 and public key $PK=x_{2(n-1)+1}$.
- Public key is signed by CA at time interval t to compute certificate $<t, PK>_{CA}$
- Alice sends Bob her certificate.
- At current time c she proofs knowledge of corresponding keys of the key-chain.
- Same for Bob



Empowered by Innovation NEC

IC (3)…

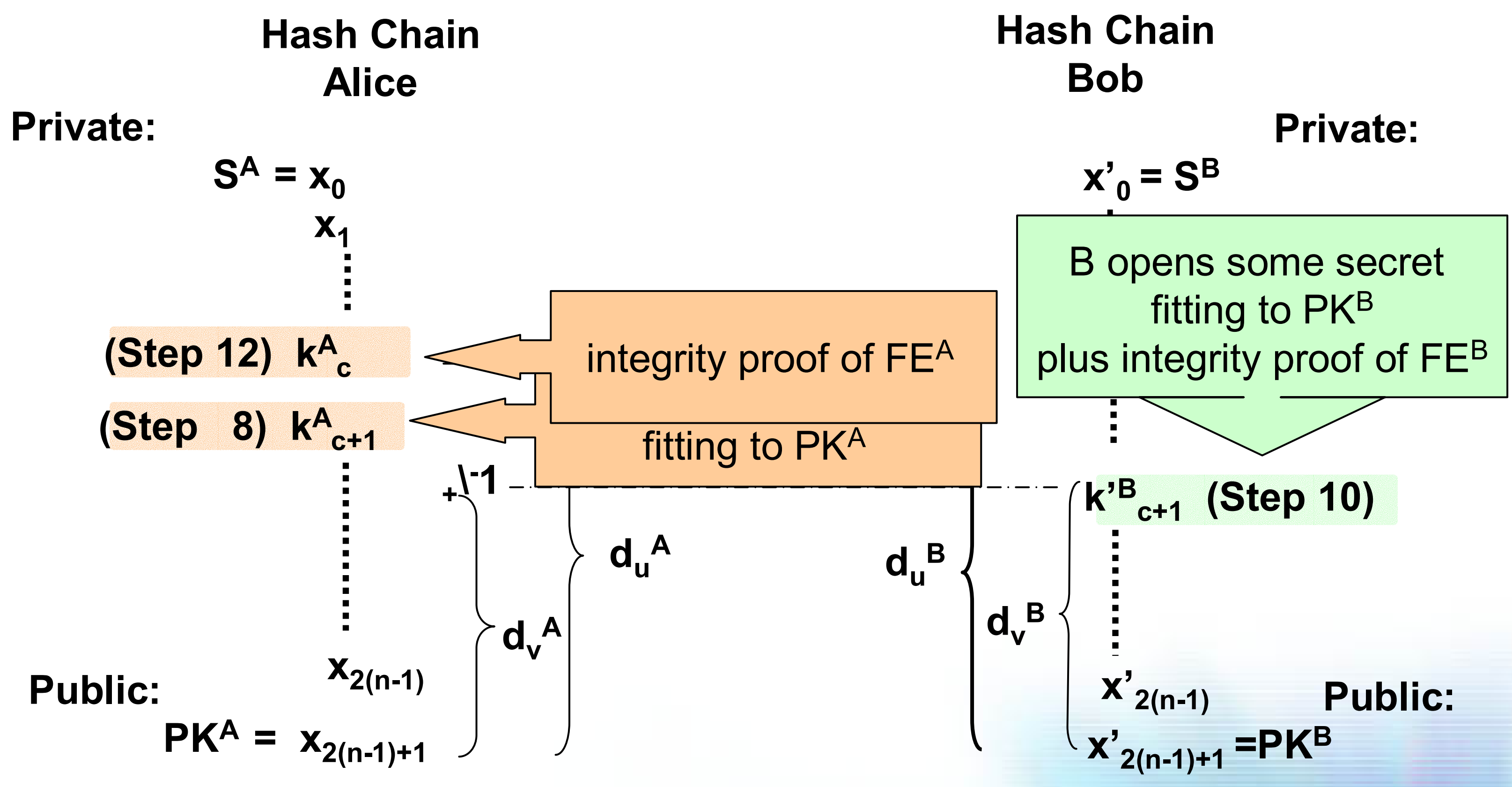
0: A->B		"hello"	certificate exchange
1: A<-B		r_B	
2: A->B		$r_A \parallel <t_u, id_A, r_B, PK^A>_{CA}$ (with $PK^A=x^A_{2(n-1)+1}$)	
3: A<-B	B verifies CA sign	$<t_v, id_B, r_A, PK^B>_{CA}$ (with $PK^B=x^B_{2(n-1)+1}$)	
4:	A verifies CA sign		compute time differences
5:	A determines t_i^A * B determines t_j^B **		
6: A->B	A chooses k-chain with FE^A fin. el.	$(FE^A)_{k_c^A}$ (with $k_c^A= x^A_{2(n-1-duA)}$)	ZCK key exchange
7: A<-B	B chooses k-chain with FE^B fin. el.	$(FE^B)_{k_{c+1}^B}$ (with $k_{c+1}^B= x^B_{2(n-1-dvB)+1}$)	
8: A->B	A opens key	k^A_{c+1}	knowledge proof of corresponding keys (next slide)
9:	B: $h^l(k^A_{c+1})= PK^A$		
10: A<-B	B opens key	k^B_{c+1}	
11:	A: $h^m(k^B_{c+1})= PK^B$		
12: A->B	A opens key	k^A_c	
13:	B: $h(k^A_c)= k^A_{c+1}$		
14:	A and B store FE^A and FE^B for ZCK		key storage

< l (steps 4–12)

* with d_u^A= i-u and d_v^A= i-v
** with d_u^B= j-u and d_v^B= j-v
} time differences [#Interval]

*** $l=2d_u^B$+/-{0,1}
**** $m=2d_v^A$+/-{0,1}
} iteration times of h

IC (4)…



Empowered by Innovation NEC

Links…

BMB+F IPonAir (2001-2004)
"Next Generation Wireless Internet"
Koordinator: Prof. M. Zitterbart
Partner: 15
http://www.iponair.de

EU IST IP: Daidalos I + II (2004-2008)
"Designing Advanced Network Interfaces for the Delivery and Administration Of Location independent, Optimised Personal Services"
Koordinator: Ricardo Pascoto
Partner: 46
http://ist-daidalos.org

EU IST STREP: UbiSec&Sens (2006-2009)
"Ubiqituous Sensing and Security in the European Homeland"
Koordinator: Dirk Westhoff
Partner: 8

Q&A…

J. Girao, D. Westhoff, M. Schneider, **CDA: Concealed Data Aggregation for Reverse Multicast Traffic in Wireless Sensor Networks**, 40th International Conference on Communications, IEEE ICC 2005, Seoul, Korea, Mai 2005.

J. Girao, D. Westhoff, M. Acharya, **Concealed Data Aggregation for Reverse Multicast Traffic in Wireless Sensor Networks: Encryption, Key Pre-distribution and Routing**, IEEE Transactions on Mobile Computing.

M. Acharya, J. Girao, D. Westhoff, **Secure Comparison of Encrypted Data in Wireless Sensor Networks**, IEEE supported WiOpt'05.

J. Girao, M. Schneider, D. Westhoff, **CDA: Concealed Data Aggregation in Wireless Sensor Networks**, ACM Workshop on Wireless Security (WiSe04) - poster, in conjunction with ACM MobiCom 2004, Philadelphia, USA, October 2004.

A. Weimerskirch, D. Westhoff, S. Lucks, E. Zenner, **Efficient Pairwise Authentication Protocols for Sensor and Ad-hoc Networks: Theory and Performance Analysis**, Sensor Network Operations, Editors: Jennifer Carruth, Thomas F. La Porta, IEEE Press Monograph, September 2004.

A. Weimerskirch, D. Westhoff, **Identity Certified Zero-Common Knowledge Authentication**, ACM Workshop on Security of Ad Hoc and Sensor Networks in conjunction with the 10th ACM SIGSAC Conference on Computer and Communications Security, ACM SASN'03, October 2003.

Weimerskirch, D. Westhoff, **Zero-Common Knowledge Authentication for Pervasive Networks**, Selected Areas in Cryptography, SAC'03, Springer-Verlag LNCS, August 2003, Ottawa, Ontario, CA.

Empowered by Innovation NEC