



An Effective Group-Based Key Establishment Scheme for Large-Scale Wireless Sensor Networks using Bivariate Polynomials

Authors:

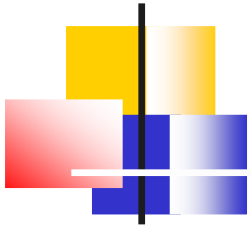
Ashok Kumar Das and Indranil Sengupta

**Department of Computer Science and Engineering
Indian Institute of Technology, Kharagpur 721 302, India**

January 5, 2008

WISARD 2008: A Workshop in COMSWARE 2008, Bangalore, India

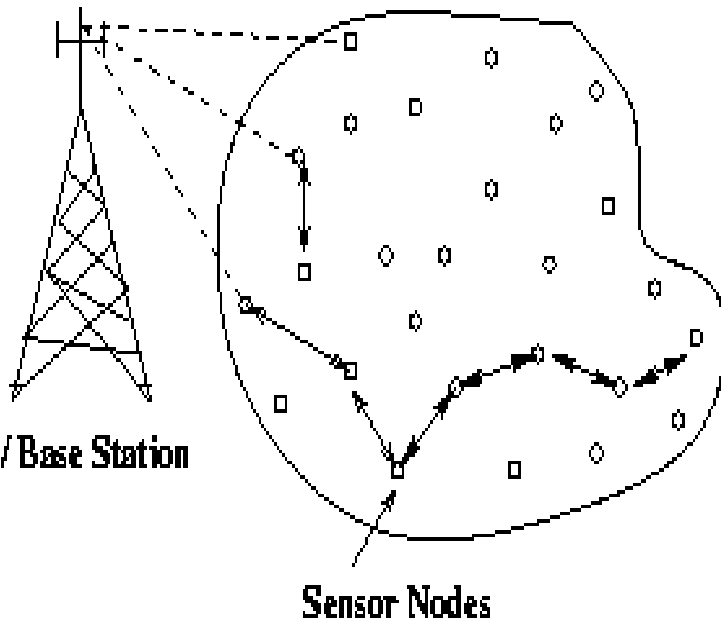
Outline of Talk



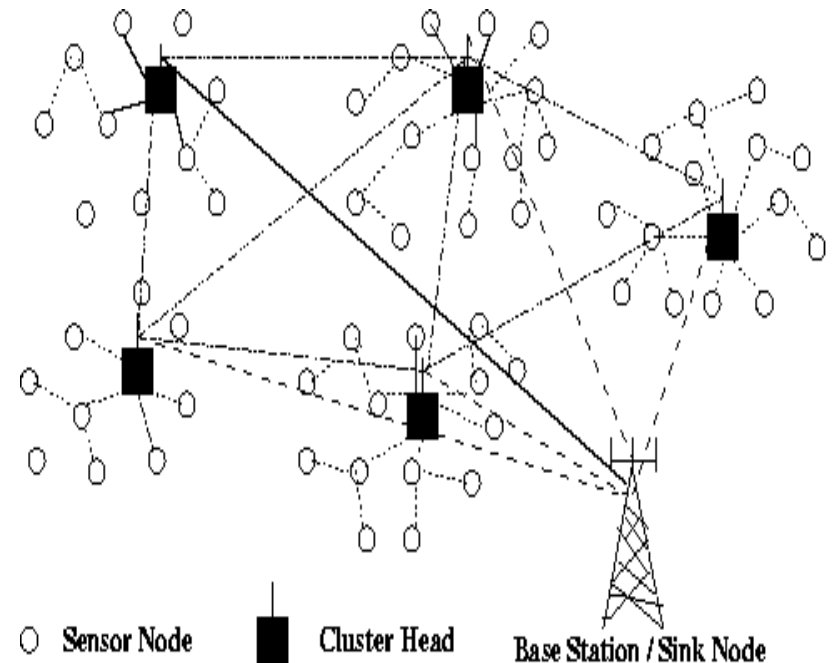
1. Brief overview of wireless sensor networks (WSNs)
2. Brief overview of existing polynomial-based Key Distribution in WSNs
3. Proposed key establishment scheme in static WSNs
4. Conclusion

Overview of Wireless Sensor Networks (WSNs)

■ Distributed WSNs



■ Hierarchical WSNs



Overview of Wireless Sensor Networks (WSNs) (continued...)



- Basic Characteristics of typical MICA2 and MICA2-DOT motes [Crossbow Technology Inc.]

	MICA2	MICA2-DOT
Processor	8-bit 7.7 MHz Atmega 128	8-bit 4 MHz Atmega 128
RAM	4K bytes	4K bytes
ROM	128K bytes	128K bytes
EEPROM	512K bytes	512K bytes
Default packet size (under TinyOS)	29 bytes	29 bytes
Power supply	2 AA batteries	1 coin cell battery



Security Issues in WSNs

- In many applications, such as target tracking, battlefield surveillance and intruder detection, wireless sensor networks are often deployed in hostile unattended environments
- Sensing data and sensing readings need to be protected properly
- Many protocols and algorithms do not work in hostile environments without security
- Security becomes one of the major concerns where there are potential attacks against sensor networks
- Due to resource-constraints, public key routines (RSA, Diffie-Hellman Key Exchange, ElGamal) not feasible in most sensor networks
- Symmetric ciphers (AES, DES, RC5) are viable options for d/encryptions of data

Existing Key Distribution Mechanisms in WSNs

□ Bootstrapping Protocol

• Phase 1: Key Pre-Distribution Phase

- Done in offline by a key setup server (i.e., the base station)

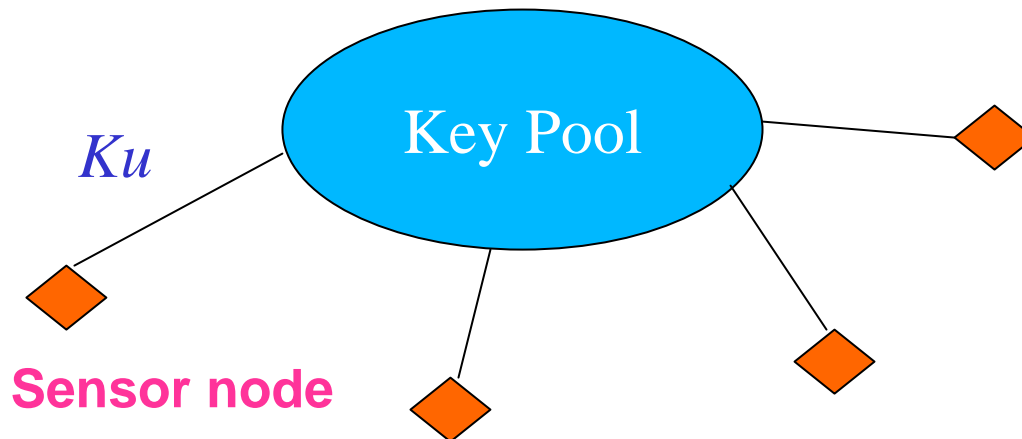


Fig: Key Pre-Distribution Phase

Existing Key Distribution Mechanisms in WSNs

(continued...)



- **Phase 2: Direct Key Establishment / Shared Key Discovery Phase**

- Executed after deployment of sensor nodes in a target field
- Two neighbors u and v share a key k , if they a common key between their key rings K_u and K_v

- *Physical neighbors*

- *Key neighbors*

- *Direct neighbors*

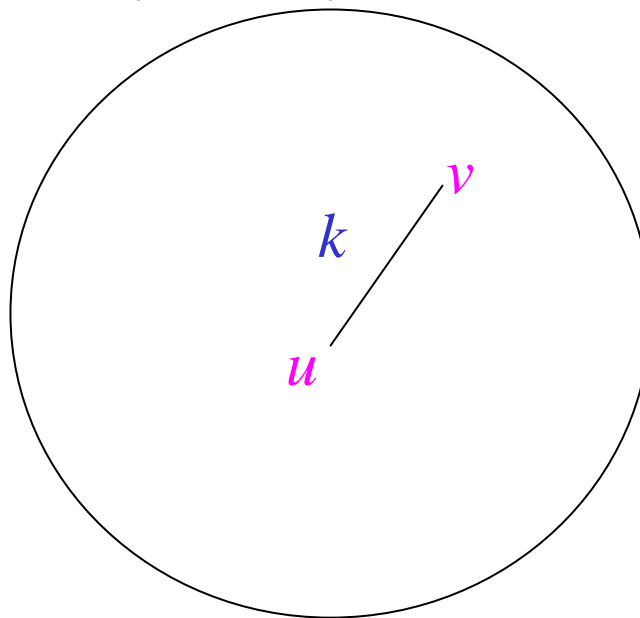


Fig: Direct Key Establishment Phase

Existing Key Distribution Mechanisms in WSNs (continued...)

- **Phase 3: Path Key Establishment Phase**

- Executed after direct key establishment phase (if required)
- If two neighbors u and v not sharing a direct key, they establish a direct key if there exists a secure path between them
- Node u securely sends the key k shared between u and v to its direct neighbor

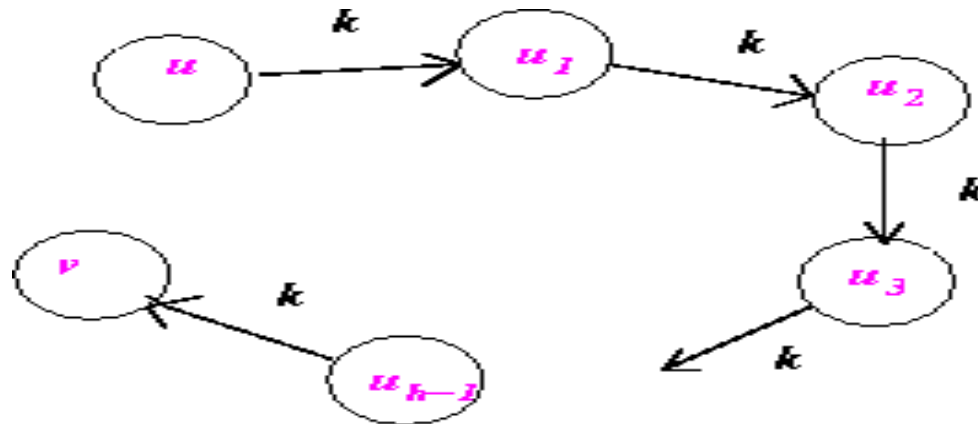


Fig: h -hop Path Key Establishment Phase



Existing Key Distribution Mechanisms in WSNs

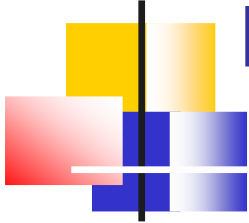
(continued...)

- **Evaluation metrics**

- Scalability
- Overheads (storage, communication and computation)
- Network connectivity : probability that two neighbor sensor nodes share a common key
- Resilience against node capture: $P_e(c)$ probability that an adversary can decrypt secret communication between two non-compromised nodes u and v when c nodes are already being captured.

If $P_e(c) = 0$, we call a key distribution mechanism as unconditionally secure or perfectly resilient against node capture.

Existing Polynomial-Based Key Distribution in WSNs

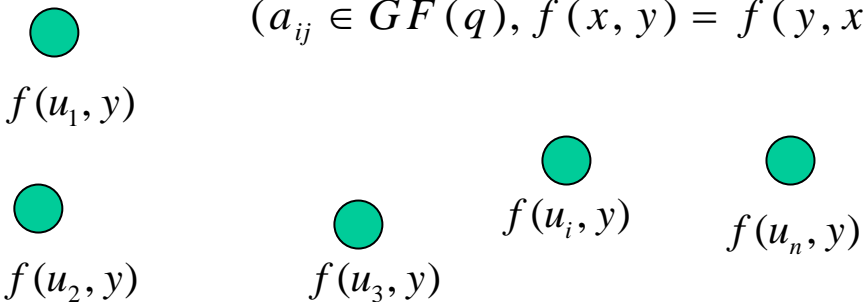


Key Pre-Distribution Phase

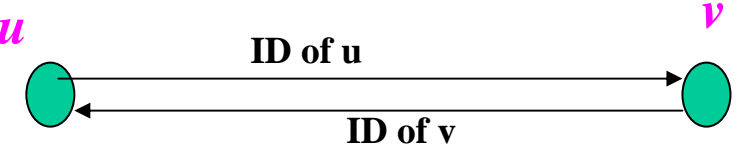
Generate a single t -degree polynomial over

$$GF(q): f(x, y) = \sum_{i,j=0}^t a_{ij} x^i y^j,$$

$$(a_{ij} \in GF(q), f(x, y) = f(y, x))$$



Direct Key Establishment Phase



$$f(u, v) = k_{u,v} = f(v, u)$$

Analysis

Network Connectivity:

- 100 %

Resilience against node capture:

- Unconditionally secure and t -collusion resistant (Not perfectly secure)
- More than t nodes captured by an adversary
 >> Compromise of whole network

Scalability:

- Very small

Proposed Efficient Group-Based Key Establishment Scheme in Static WSNs



❑ Motivation

✓ Network performance of the location-aware schemes degrades dramatically when the deployment error is larger

✓ We propose a group-based location-aware scheme based on existing polynomial-based key distribution scheme proposed by Blundo et al.

✓ Provides always unconditional security against sensor node capture and 100% connectivity.

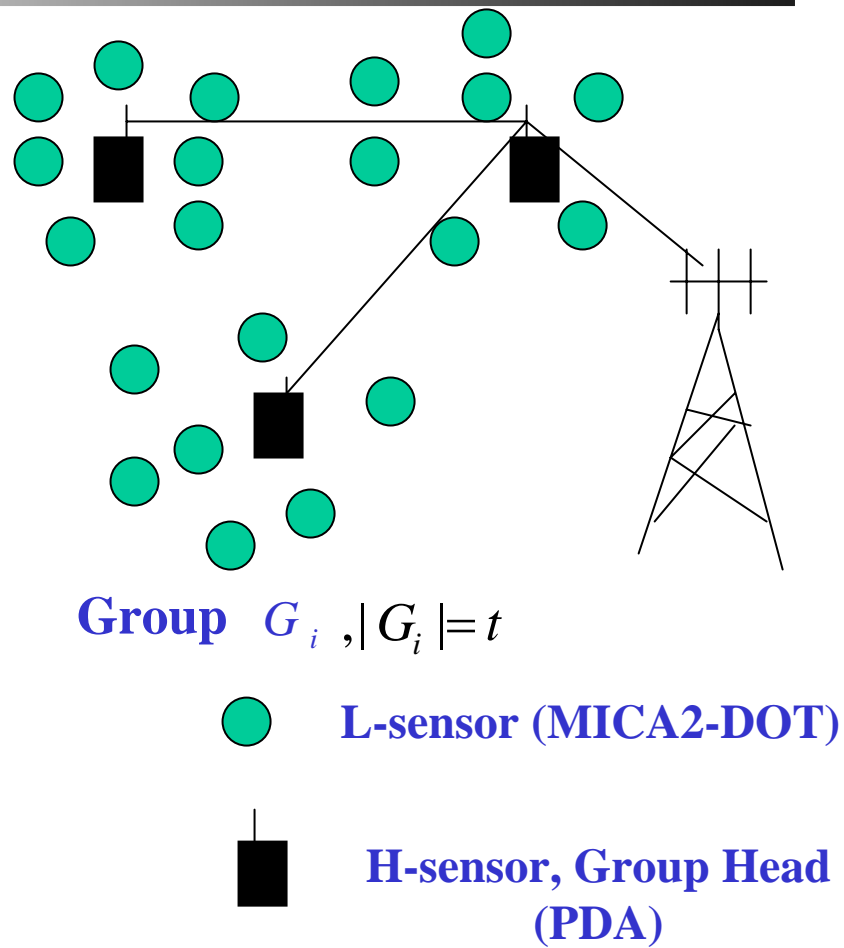


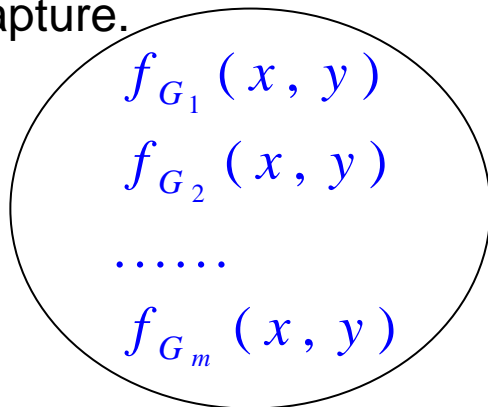
Fig. Our Network Model

Proposed Efficient Group-Based Key Establishment Scheme in Static WSNs

(Continued...)



- **Key Pre-Distribution Phase**
- Target field is partitioned into m equal disjoint groups G_i ($i = 1, 2, \dots, m$)
- Each group consists of a group head (H-sensor) GH_i and at most $(t-1)$ L-sensor nodes so that our scheme will always be unconditional secure against node capture.



- Generate a t -degree symmetric bi-variate polynomial $f(x, y)$ over $GF(q)$ for all group heads ($t \gg m$)
- Generate a t -degree symmetric bi-variate polynomial $f_{G_i}(x, y)$ for each group G_i

ID
MK_{GH_i}
$f(GH_i, y)$
$f_{G_i}(GH_i, y)$

Key ring of GH_i

ID
MK_u
$f_{G_i}(u, y)$

Key ring of u

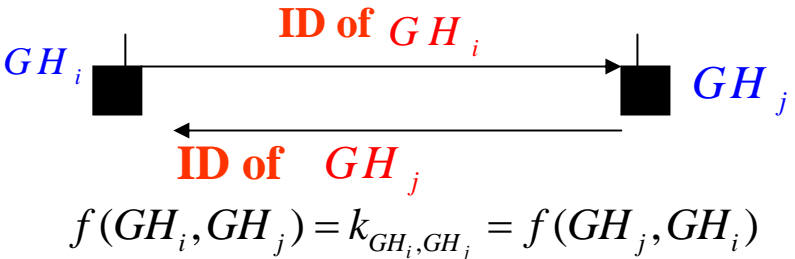
Polynomial pool of m t -degree polynomials

Proposed Efficient Group-Based Key Establishment Scheme in Static WSNs

(Continued...)

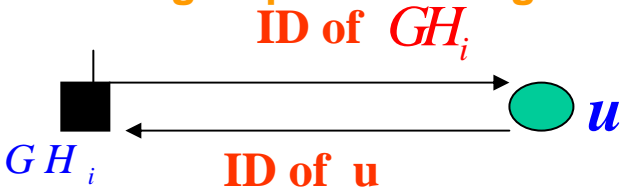


- **Direct Key Establishment Phase**
- **Inter-group pairwise key establishment between group heads**



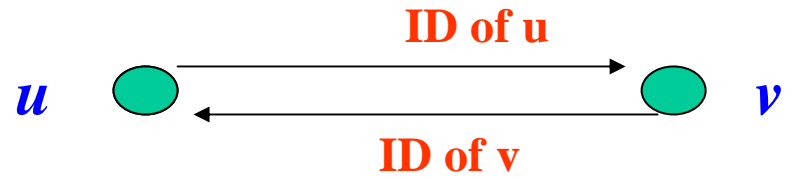
- **Intra-group pairwise key establishment**

Case-I: group-head to regular node



$f_{G_i}(GH_i, u) = k_{GH_i, u} = f_{G_i}(u, GH_i)$

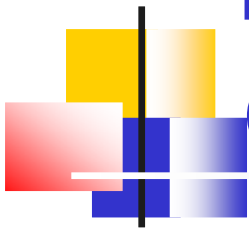
Case-II: regular head to regular node



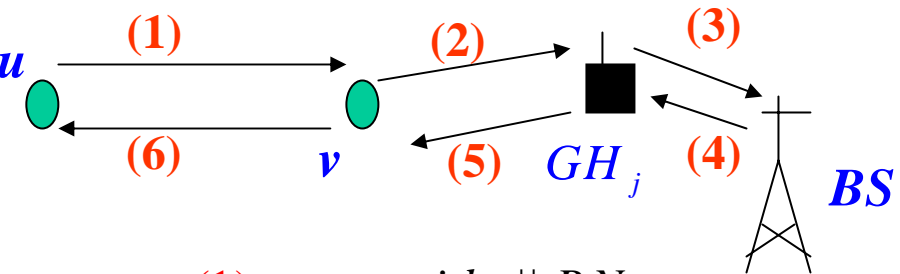
$f_{G_i}(u, v) = k_{u, v} = f_{G_i}(v, u)$

Proposed Efficient Group-Based Key Establishment Scheme in Static WSNs

(Continued...)



Case-III: regular node to regular node in other deployment group



- (1) $u \rightarrow v : id_u \parallel RN_u$
- (2) $v \rightarrow GH_j : (T = (id_u \parallel id_v \parallel RN_u \parallel RN_v)) \parallel MAC_{MK_v}(T)$
- (3) $GH_j \rightarrow BS : msg(2)$
- (4) $BS \rightarrow GH_j : (E_{MK_u}(k_{u,v} \oplus id_u \oplus RN_u), E_{MK_v}(k_{u,v} \oplus id_v \oplus RN_v))$
- (5) $GH_j \rightarrow v : msg(4)$
- $[k_{u,v} = (k_{u,v} \oplus id_v \oplus RN_v) \oplus (id_v \oplus RN_v)]$
- (6) $v \rightarrow u : E_{MK_u}(k_{u,v} \oplus id_u \oplus RN_u)$
- $[k_{u,v} = (k_{u,v} \oplus id_u \oplus RN_u) \oplus (id_u \oplus RN_u)]$

Proposed Efficient Group-Based Key Establishment Scheme in Static WSNs (Continued...)

■ Dynamic Node Addition Phase (in Deployment Group G_i)

- Not good idea to deploy more than t nodes in any deployment group, leads to not unconditionally security
- deploy only h nodes in initial deployment and remaining $(t-h)$ nodes for dynamic node addition in a group

Regular sensor node addition

ID
MK_u
$f_{G_i}(u, y)$

Group head node addition

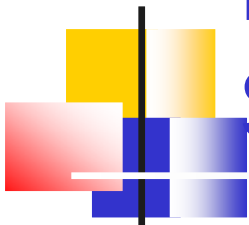
ID
$MK_{GH'_i}$
$f(GH'_i, y)$
$f_{G_i}(GH'_i, y)$

Proposed Efficient Group-Based Key Establishment Scheme in Static WSNs (Continued...)



- **Analysis**
- **Storage Overhead:**
 - ID + master key + one t -degree polynomial share ($(t+1) \log q$ bits)
- **Communication Overhead:**
 - node's own ID (most cases)
- **Computational Overhead:**
 - one efficient poly evaluation
- **Network Connectivity:**
 - 100% connectivity
- **Resilience against sensor node capture:**
 - unconditionally secure

Proposed Efficient Group-Based Key Establishment Scheme in Static WSNs (Continued...)



- Comparison of resilience against node capture with existing schemes

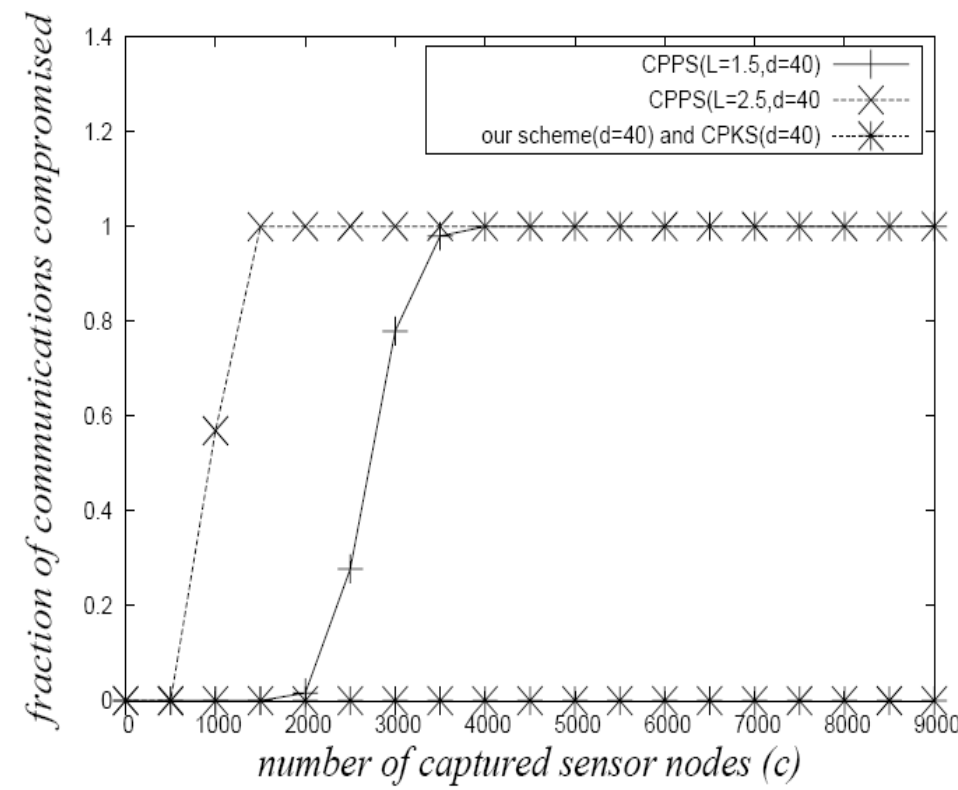
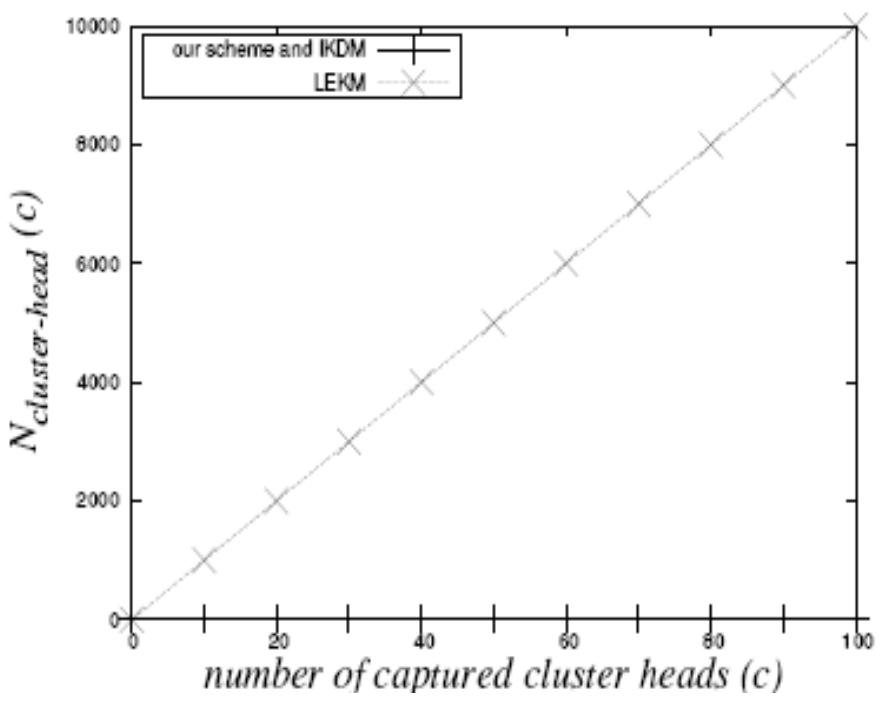
<i>number of captured sensor nodes</i>	<i>fraction of communications compromised between non-compromised nodes</i>						
	EG scheme	q-composite	polynomial-based	polynomial-pool	LEKM	IKDM	our scheme
0	0.0000	0.0000	0.0000	0.0000	0	0	0
50	0.6358	0.2278	0.0000	0.0000	0	0	0
100	0.8674	0.6771	0.0000	0.8842	0	0	0
150	0.9517	0.9109	0.0000	1.0000	0	0	0
200	0.9824	0.9898	0.0000	1.0000	0	0	0
250	0.9936	1.0000	1.0000	1.0000	0	0	0
300	0.9977	1.0000	1.0000	1.0000	0	0	0
350	1.0000	1.0000	1.0000	1.0000	0	0	0
400	1.0000	1.0000	1.0000	1.0000	0	0	0
450	1.0000	1.0000	1.0000	1.0000	0	0	0
500	1.0000	1.0000	1.0000	1.0000	0	0	0

Proposed Efficient Group-Based Key Establishment Scheme in Static WSNs

(Continued...)

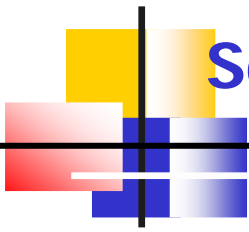


- Resilience against group head (cluster head) capture
- Resilience against sensor node capture with CPKS and CPPS



In the network initialization phase

Proposed Efficient Group-Based Key Establishment Scheme in Static WSNs (Continued...)



	Storage	Communication	Computation	Connectivity	Security
EG scheme	m key ids +keys	Key ids	High	reasonable	poor
q-composite	m key ids + keys	Key ids	High	reasonable	Better than EG
Poly-pool	s' poly shares	Poly shares' ids	High	reasonable	Better than EG
LEKM	Single key	Cluster node's id	Very low	100%	Better than above
IKDM	Two keys	Cluster nodes' id	Very low	100%	Better than above
CPKS	c keys + ids	Node's id	Very low	High	Unconditional
CPPS	c poly shares + ids	c Poly ids	Poly eval	High	Lower than CPKS
Our scheme	poly-share + MK	Node's id	Poly eval	100%	Always Unconditional

Proposed Efficient Group-Based Key Establishment Scheme in Static WSNs (Continued...)



■ Summary

- ✓ Provides 100% network connectivity (any two nodes in a deployment group can establish a pairwise secret key)
- ✓ Provides unconditional security against node capture
- ✓ Supports dynamic node addition after initial deployment
- ✓ Provides better trade-off between network connectivity, security, communication and computational overheads compared to those for the existing related schemes.



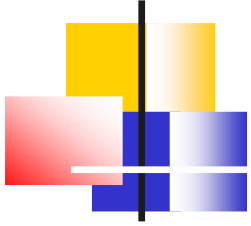
Key References

- [1] C. Blundo, A. D. Santis, A. Herzberg, S. Kutten, U. Vaccaro, and M. Yung. Perfectly-secure key distribution for dynamic conferences. In *Advances in Cryptology- CRYPTO'92, LNCS 740*, Berlin, August 1993, pp. 471--486.
- [2] L. Eschenauer and V. D. Gligor. A key management scheme for distributed sensor networks. in *the 9th ACM Conference on Computer and Communication Security*, November 2002, pp. 41--47.
- [3] H. Chan, A. Perrig, and D. Song. Random key predistribution schemes for sensor networks. In *IEEE Symposium on Security and Privacy*, Berkeley, California, 2003, pp. 197--213.
- [4] D. Liu, P. Ning, and R. Li. Establishing pairwise keys in distributed sensor networks. *ACM Transactions on Information and System Security*, vol. 8, no. 1, pp. 41--77, 2005.



Key References (continued...)

- [5] D. Liu and P. Ning. Improving key pre-distribution with deployment knowledge in static sensor networks. *ACM Transactions on Sensor Networks*, vol. 1, no. 2, pp. 204--239, 2005.
- [6] G. Jolly, M. Kuscü, P. Kokate, and M. Yuonis. A low-energy key management protocol for wireless sensor networks. In *Proceedings of the Eighth IEEE ISCC'03*, Turkey, June 30 - July 3 2003.
- [7] Y. Cheng and D. Agrawal. An improved key distribution mechanism for large-scale hierarchical wireless sensor networks. *Ad Hoc Networks (Elsevier)*, vol. 5, no. 1, pp. 35--48, 2007.



Thank You !