Light Weight Key Establishment Scheme for Wireless Sensor Networks

Jilna Payingat, Deepthi P. Pattathil

Department of Electronics and Communication Engineering
National Institute of Technology, Calicut
Kerala, India

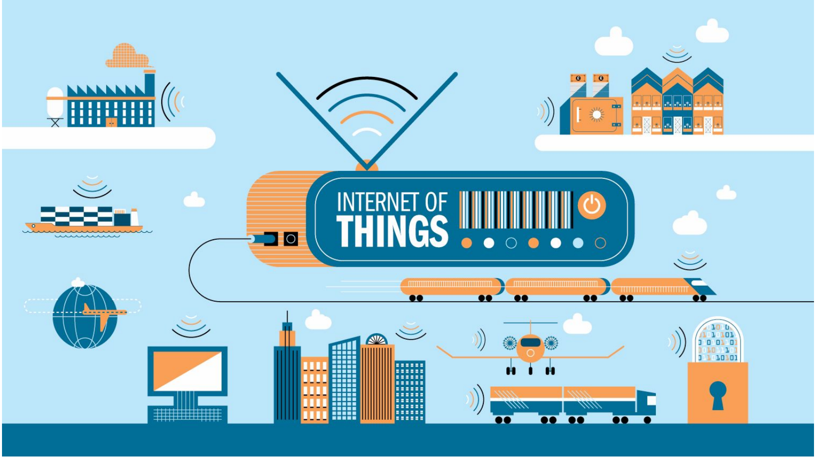
Sixth International Conference on Security, Privacy and Applied Cryptographic Engineering (SPACE 2016)
Dec 16-18, Hyderabad.

December 16, 2016

Overview

- Introduction
- Challenges and Goals
- Basic approaches
- Proposed method
- Performance evaluation
- Conclusion
- References

Introduction (1/2)



- IoT is now becoming “the infrastructure of the information society”

Introduction (2/2)

- The rapid advancements in IoT technologies has led to the deployment of wireless sensor nodes in a variety of applications
- Applications of WSNs
  - Industry automation
  - Health care
  - Military surveillance
- Need to provide confidentiality and authenticity to these sensitive data
- Uses symmetric key algorithms to secure data
- Demands secure and reliable key exchange protocols

Key Establishment Schemes in WSNs

Challenges

- Deployment in hostile environments cause increased vulnerability to attacks
- Resource constrained nature of sensor nodes hinders the use of conventional key distribution schemes

Goals

- Should provide security against eavesdropping
- Should prevent unauthorised nodes from establishing communication with network nodes
- Should ensure connectivity
- Should support node addition

Evaluation Metrics

Efficiency

- Storage efficiency
- Computational cost
- Communication overhead
- Connectivity

Flexibility

- Scalability
- Dependence on deployment knowledge

Security

- Resilience
- Eavesdropping
- Hello flood attack
- Node addition attack
- Node cloning attack

Basic Approaches[1] (1/4)

Global key

- ✓ Single master key
- ✓ Best in terms of efficiency
- ✓ Compromise of any one node reveals the secret key of the entire network

Full pair wise key

- ✓ Each node receives pair wise keys to communicate with every other node in the network
- ✓ High resilience and connectivity
- ✓ Lack of scalability

[1] M.A. Simplcio, P.S. Barreto et.al," A survey on key management mechanisms for distributed wireless sensor networks". *Computer Networks*, vol. 54, no.15, 2010, pp. 2591-2612.

Basic approaches (2/4)

Random key pre-distribution[2]

- ✓ Generate a key pool of size p
- ✓ Load each node with a key ring composed of r keys randomly chosen from the key pool($r < p$)
- ✓ If any two neighbouring nodes share secret key, then a secure link is established
- ✓ Value of r and p determines the connectivity and security of the network

Polynomial based key management[3]

- ✓ A bi-variate, λ degree polynomial over a prime field is loaded in to each sensor node
- ✓ The polynomial is used to generate secret keys
- ✓ Network is secure as long as λ or less nodes are compromised

---

[2] L. Eschenauer and V. D. Gligor, A key management scheme for distributed sensor networks, in *Proc. 9th ACM Conf. Comput. Commun. Security*, 2002, pp. 41-47.

[3] D.Liu, P. Ning, R. Li, "Establishing pairwise keys in distributed sensor networks, *ACM Transactions on Information and System Security (TISSEC)* vol.8, no.1, pp. 41-77.

Basic approaches (3/4)

Key management based on transitory master key [4]

- ✓ Master key is used in the initialization phase for authentication and secret key establishment.
- ✓ The master key is erased after a time-out period
- ✓ Time-out represents a trade-off between connectivity and security

Key management based on hard mathematical problems

- ✓ ECC, Modular arithmetic
- ✓ Highly secure even if nodes are compromised in the initialization phase
- ✓ Computationally intensive and less energy efficient

[4] F. Gandino, B. Montrucchio, M.Rebaudengo, "Key management for static wireless sensor networks with node adding", *IEEE Trans. on Industrial Informatics*, vol. 10, no.2, pp. 1133-1143, July 2014.

Basic approaches (4/4)

Over-the-air key establishment[5]

- Energy efficiency is increased by reducing the computations
- Secret keys generated through a single hash computation
- Method 1: Extract secret keys from received signal strength
  - Communicating channel must be highly dynamic in nature
- Method 2: Leverage channel anonymity for generating secret keys
  - Assumes adversary to be a passive eavesdropper

Requirement: Energy efficient, deterministic and secure protocol

[5] P. Barsocchi, G. Oligeri, and C. Soriente, "Shake: Single hash key establishment for resource constrained devices," *Ad Hoc Networks*, vol. 11, no. 1, pp. 288-297,2013.

Energy Efficient Protocols

Crypto-less Over-the-air-Key Establishment(COKE)[6]

- Based on source indistinguishability of anonymous channels
- Requires a single hash computation
- Probabilistic, not secure against active adversaries

LEAP+[7]

- Based on transitory master key
- Offers zero resilience if a node is compromised in the initialization phase
- Prone to jamming attacks

[6] R. Di Pietro and G. Oligeri, COKE crypto-less over-the-air key establishment," *IEEE Trans. on Information Forensics and Security*, vol. 8, no. 1, pp. 163-173, 2013.

[7] S. Zhu, S. Setia, and S. Jajodia, LEAP+: Efficient security mechanisms for large-scale distributed sensor networks," *ACM Transactions on Sensor Networks (TOSN)*, vol. 2, no. 4, pp. 500-528, 2006

Proposed Method (1/2)

Assumptions

- Homogeneous
- Static
- Supports node addition
- Eavesdropper can listen to all the traffic in the network

Data loaded into the sensor node prior to deployment

- Master key (MK)
- Random integer n_i
- Node identifier ID_i

Proposed Method (2/2)

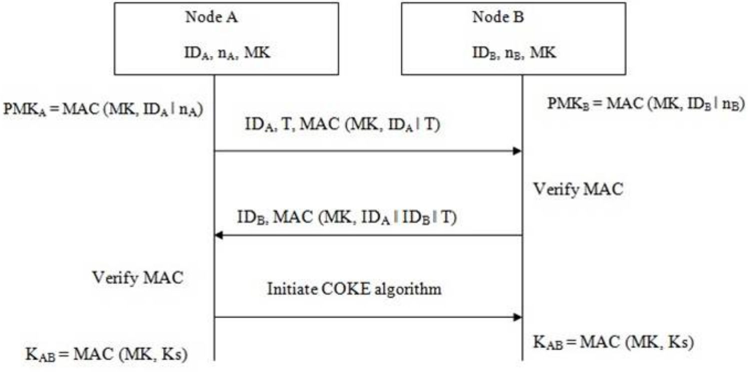


Figure: Proposed key establishment scheme

Security Metric (1/4)

Resilience

Probability that a link between uncompromised nodes is not compromised due to other compromised nodes in the network.

- In the proposed method, key in any link depends upon random data exchanged between the node pair through COKE algorithm.
- Data available to the attacker if a node is compromised
  - MK / PMK
  - Node ID
  - Pair wise secret key with the neighbouring nodes
- Not sufficient to compromise any other link
- Offers high resilience even if nodes are compromised in the initialization phase

Security Metric (2/4)

Hello flood attack

Adversary sends hello messages to the neighbouring nodes with high transmission power

- Hello messages in the proposed scheme consists of an authentication tag generated using the master key
- COKE algorithm is initiated only after successful MAC verification
- Defends Hello Flood attack because only authenticated hello messages are processed by the node

Security Metric (3/4)

Node cloning / Node replication

Adversary loads its own nodes with the compromised information and tries to establish pair-wise keys with the valid nodes.

- Probability that a single key is shared by more than one link is negligibly small
- Establishment of new pair wise keys demands the knowledge of MK
- Resists Node cloning / Node replication attack

Security Metric(4/4)

Node addition attack

Adversary introduces new nodes into the network by loading it with the correct master key.

- Node id's are randomly generated by the base station
- Base station broadcasts a list of valid node ids added in each phase
- Nodes verify their neighbour's ids before initiating secret key establishment.
- Less prone to node addition attack.

Efficiency Metric (1/2)

Computational cost

Two MAC computations at each node for every pair-wise key establishment

Connectivity

Deterministic protocol - secret key is established between every authenticated neighbouring node

Storage requirement

- Initialization phase : node ID, MK, random integer
- Working phase : PMK, node ID, shared secret keys

Efficiency Metric (2/2)

Communication overhead

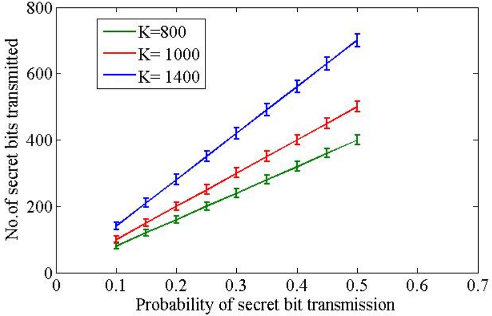


Figure: Number of secret bits transmitted for different values of K[8]

[8] K: Total number of bits transmitted

Table: Overall Comparison

	Proposed scheme	LEAP+	COKE
Storage (in bytes)	738	738	722
Communication overhead (in bytes)	120	36	175
Prob. of eavesdropping a link with nodes compromised in the working phase	0	0	0
Prob. of eavesdropping a link with nodes compromised in the initialization phase	0	1	0
Prob. of node addition attack	0	0	1
Scalability support	YES	YES	YES

Conclusion

- Developed an energy efficient, secure and deterministic key establishment technique for WSNs.
- Combined concepts of transitory master key and over-the-air key establishment
- Compared to COKE, the proposed scheme is secure against active adversaries
- Compared to LEAP, offers high resilience even if nodes are compromised in the initialization phase

References I

M. A. Simplicio Jr, P. S. Barreto, C. B. Margi, and T. C. Carvalho, "A survey on key management mechanisms for distributed wireless sensor networks," *Computer Networks*, vol. 54, no. 15, pp. 2591-2612, 2010.

P. Kotzanikolaou, E. Magkos, D. Vergados, and M. Stefanidakis, "Secure and practical key establishment for distributed sensor networks," *Security and Communication Networks*, vol. 2, no. 6, pp. 595-610, 2009.

D. Du, H. Xiong, and H. Wang, "An effcient key management scheme for wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 2012, 2012.

P. Jilna and D. P. Pattathil, "A key management technique based on elliptic curves for static wireless sensor networks," *Security and Communication Networks*, vol. 8, no. 18, pp. 3726-3738, 2015.

S.-H. Seo, J. Won, S. Sultana, and E. Bertino, Effective key management in dynamic wireless sensor networks," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 2, pp. 371-383, 2015.

P. Barsocchi, G. Oligeri, and C. Soriente, "Shake: Single hash key establishment for resource constrained devices," *Ad Hoc Networks*, vol. 11, no. 1, pp. 288-297, 2013.

R. Di Pietro and G. Oligeri, "Coke crypto-less over-the-air key establishment," *IEEE Trans. on Information Forensics and Security*, vol. 8, no. 1, pp. 163-173, 2013.

S. Zhu, S. Setia, and S. Jajodia, "Leap+: Effcient security mechanisms for large-scale distributed sensor networks," *ACM Transactions on Sensor Networks (TOSN)*, vol. 2, no. 4, pp. 500-528, 2006.

References II

S. Blackshear and R. M. Verma, "R-leap+: randomizing leap+ key distribution to resist replay and jamming attacks," in *Proc. of the 2010 ACM Symposium on Applied Computing. ACM*, 2010, pp. 1985-1992.

Y. H. Kim, H. Lee, D. H. Lee, and J. Lim, "A key management scheme for large scale distributed sensor networks," in *IFIP International Conference on Personal Wireless Communications*, Springer, 2006, pp. 437-446.

L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," in *Proc. of the 9th ACM conference on Computer and communications security, ACM*, 2002, pp. 41-47.

THANK YOU