ISSN 1000-9825, CODEN RUXUEW
Journal of Software, Vol.17, No.12, December 2006, pp.2577−2588
DOI: 10.1360/jos172577

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

传感器网络安全研究*

李　平[1]，林亚平[1,2+]，曾玮妮[1]

[1](湖南大学 计算机与通信学院,湖南 长沙　410082)
[2](湖南大学 软件学院,湖南 长沙　410082)

Search on Security in Sensor Networks

LI Ping[1], LIN Ya-Ping[1,2+], ZENG Wei-Ni[1]

[1](College of Computer and Communications, Hu'nan University, Changsha 410082, China)
[2](College of Software, Hu'nan University, Changsha 410082, China)
+ Corresponding author: Phn: +86-731-8821932, Fax: +86-731-8821932, E-mail: yplin@hnu.cn

Li P, Lin YP, Zeng WN. Search on security in sensor networks. *Journal of Software*, 2006,17(12):2577−2588. http://www.jos.org.cn/1000-9825/17/2577.htm

Abstract: Security issue of sensor networks is greatly different from that of conventional networks, in terms of its specific requirements, constrained resources of nodes, and variety of network characteristics. The security architecture of sensor networks is proposed, trying to outline a general illustration on this area. The following three topics are discussed: 1) Security primitives such as SKE, MAC and PKC; 2) Various keying mechanisms for the key management issue; 3) Joint considerations on network-related issues including routing, energy and fault tolerance. Other open security issues and further challenges are also addressed.
Key words: security; sensor network; key management; authentication; energy-aware

摘　要: 由于传感器网络自身的一些特殊需求,加上其节点资源非常有限和网络特征的多样性,其安全问题在很大程度上不同于传统网络.给出了传感器网络的安全体系结构,力图对该领域的研究进行整体的描述.讨论了3个方面的问题: 1) 所采用的密码体制,如SKE,MAC,PKC等; 2) 密钥管理中的多种密钥建立算法; 3) 路由、能耗和容错等多因素相关的综合考虑.最后,简要介绍了其他一些安全问题以及该领域今后的研究热点.
关键词: 安全;传感器网络;密钥管理;认证;能量感知
中图法分类号: TP393　　文献标识码: A

1 Introduction

Dramatic improvements in micro-electro-mechanical systems (MEMS) technology, combined with advanced

* Supported by the State Scholarship Fund of China under Grant No.20023034 (国家留学基金); the Provincial Natural Science Foundation of Hu'nan, China under Grant No.06jj20049 (湖南省自然科学基金); Scientific Research Fund of Hu'nan Provincial Education Department of China under Grant No.06B005 (湖南省教育厅科研资助项目); the Subject Foundation of the 10th Five-Year Plan of Hu'nan Provincial Education Department of China (湖南省教育厅十五重点学科建设基金)

Received 2004-02-06; Accepted 2005-07-08

wireless communications, have made available sensor networks of large scale. A typical sensor network has hundreds to millions of sensor nodes. Each sensor node is typically low-cost, limited in computation and information storage resources, highly power constrained, and communicates over a short-range wireless network interface. These described features ensure a wide range of applications for sensor networks, including military provision, environment monitoring and exploring on man-unreachable circumstances.

However, it seems that the security issue of sensor networks has not been considered as sufficiently as it should be[1]. Although research on sensor networks are motivated due to their tremendous applications, security requirements only arise for military purpose. While on traditional networks, the security issue has gained much interest. Moreover, due to limited resources of hardware, normally used cryptographic techniques cannot be simply applied in this emerging field. On the other hand, those reasons will make security research more challenging. A variety of new algorithms and protocols have come into being, and some of them have made significant contributions on this research field. However much more unexplored still remains in this area.

As the security issue covers too many detailed topics to discuss, we propose the security architecture of sensor networks in this paper, and we summarize current research achievements based on this architecture, for purpose of making materials more organizable. We investigate the security issue in three aspects, such as security primitives, key management, and network-based security mechanisms. The main reason for such a consideration is that there exists a fundamental contradiction between the origin of sensor networks and conventional security characteristics. Notes that sensor nodes are typically low cost, taking responsibility for sensing and data aggregation[2], it is impossible for sensors to load sufficient security services. In addition, we still lack necessary support on node identification from network layer[3]. On the contrary, conventional security focuses on a single entity to achieve system security based on securing every individual in the network. Based on the available security primitives supported by current cryptography research, we address the key management issues and inspect the performance of security mechanisms in network environment. The essential problem of the formal item is how to construct variant identity-based keying infrastructures to achieve necessary individual security. While on the latter one, the security issue is analyzed systematically based on network-wide communications, with widened constraints caused from network routing, energy consumption and etc., in order to make those schemes more adaptive and scalable to sensor networks. The rest of this paper is organized as follows. Section 2 gives an overview on sensor network security, with a summary of security properties on different levels. Section 3 presents discussions on variant security primitives. Section 4 provides a detailed analysis of the key management issues; and multi-issue related security mechanisms are addressed in Section 5. To make this survey more comprehensive, other related issues are provided in Section 6, and the paper is concluded in Section 7.

2 Overview of Sensor Networks Security

In this section, we generally describe the following aspects of sensor networks: constrained conditions, security requirements and security architecture.

2.1 Constrained conditions

- *Topology maintenance*. Sensor nodes are assumed to be deployed throughout the sensor field before the network begins to work. There are three phrases related to network topology maintenance and change: pre-deployment and deployment phase, post-deployment phase and re-deployment of additional nodes phase. Normally global or local sensible information is pre-loaded on a sensor node in the first phase. In the latter two deployment phases, network topologies are prone to frequent changes due to node device failure, varying task dynamics, and addition of the new nodes.

- *Hardware constraints*. References [4,5] provide detailed performance parameters for prototype of their own productions. For example, Smart Dust nodes are equipped with 8-bit processor, 512 bytes RAM, and 8Kbytes flash memory for instructions execution. Only 4500 bytes are available for application code space. Although hardware performance has improved greatly according to the latest figures offered by Ref.[6], and definitely the development will maintain fairly high speed in the future, the available resources of sensor nodes are still very tight.
- *Energy constraints*. For every sensor node, power consumption is divided into three domains: Sensing, communication and data processing. Reference [7] shows that a sensor node expends maximum energy in data communication. Thus the design of algorithms and protocols is inevitably influenced by the corresponding power expenditures. However, we still lack comprehensive figures for quantitative analysis.
- *Inability of tamper resistance*. As sensor nodes may be deployed in hostile or unattended areas, they would take much risk of physical attack by an adversary. In the worst case, sensible information stored in a sensor node may be compromised, causing some part of the network vulnerable to security attack.

2.2 Security requirements

2.2.1 Security goals

Various security requirements on sensor networks are presented in almost all the related papers[4,9,10]. As a summary, we classify those requirements into three security levels:

- *Message-Based level*. Similar with that in conventional networks, this level deals with data confidentiality, authentication, integrity and freshness. Symmetric key cryptography and message authentication codes are necessary security primitives to support information flow security. Also data freshness is necessarily required as lots of content-correlative information is transmitted on a sensor network during a specific time.
- *Node-Based level*. Situations such as node compromise or capture are investigated on this level. In case that a node is compromised, loaded secret information may be improperly used by adversaries.
- *Network-Based level*. On this level, more network-related issues are addressed, as well as security itself. A major benefit of sensor networks is that they perform in-network processing to reduce large streams of raw data into useful aggregated information. Protecting it is critical. The security issue becomes more challenging when discussed seriously in specific network environments. Firstly, securing a single sensor is completely different from securing the entire network, thus the network-based anti-intrusion abilities have to be estimated. Secondly, such network parameters as routing, node's energy consumption, signal range, network density and etc., should be discussed correlatively. Moreover, the scalability issue is also important with respect to the redeployment of node addition and revocation.

2.2.2 Performance metrics

As addressed above, it's definitely insufficient to access a scheme based on its ability to provide secrecy. Reference [10] proposes the following evaluation metrics:

- *Resilience against node capture*. On the network-based level, the fraction of total communications that are compromised is required to be estimated once a capture of several nodes occurs.
- *Resistance against node replication*. This issue needs to be seriously investigated as the captured node may be cloned and thus adversaries gain more control of the network.
- *Revocation*. Like regular process on node addition, the revocation mechanism is always necessary for detection and insulation of the misbehaving nodes.

- *Scale*. Performance of the above security characteristics needs to be generally inspected, corresponding to different network scales.

2.3 Security architecture of sensor networks

In order to give a general view on security issues addressed in sensor networks, we present the security architecture of sensor networks in Fig.1. As described above, three-level security requirements outline the principles of algorithm design on security mechanisms. We list the corresponding issues for each level in detail. In order to achieve securing available communications and applications in sensor networks, such as identity authentication, routing, data aggregation and etc., most security researches focus on the following three aspects: security primitives, key management and network-related security strategies. Security primitives manage a minimal protection to information flow and a foundation to create secure protocols. Those security primitives are systematical key encryption (SKE), message authentication codes (MAC), and public key cryptography (PKC). The aspect of key management deals with three basic factors in the design of a key infrastructure for sensor networks: Key pre-distribution, key discovery and key maintenance. The issue of network-related security strategies combines communications throughout the entire network, integrates power and routing awareness, and promotes holistic working performance within tolerable costs. In the rest of this paper, we will analyze current research on security of sensor networks according to the classifications of those three aspects.

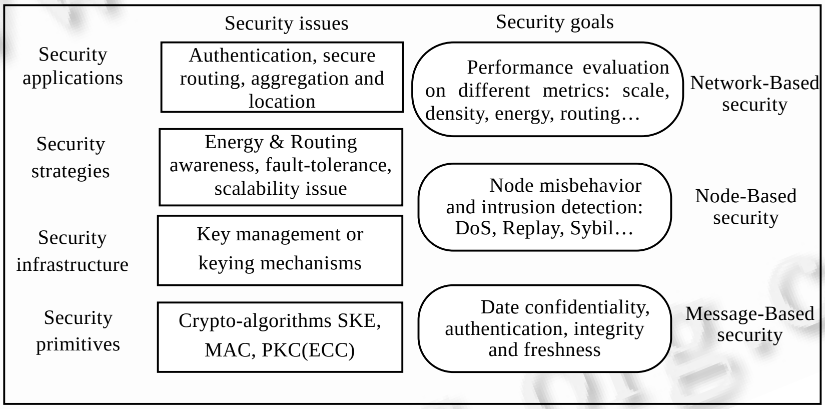
Security issues
Security goals
Security applications
Authentication, secure routing, aggregation and location
Performance evaluation on different metrics: scale, density, energy, routing…
Network-Based security
Security strategies
Energy & Routing awareness, fault-tolerance, scalability issue
Node misbehavior and intrusion detection: DoS, Replay, Sybil…
Node-Based security
Security infrastructure
Key management or keying mechanisms
Security primitives
Crypto-algorithms SKE, MAC, PKC(ECC)
Date confidentiality, authentication, integrity and freshness
Message-Based security

Fig.1 Security architecture of sensor networks

3 Security Primitives

3.1 Alternative symmetric key algorithms

- *Block cipher*. There exist arguments on how to choose a suitable symmetric encryption algorithm due to the constrained conditions of sensor networks. It is worth noticing that Ref.[11] develops the methods for deriving the computational overhead of the embedded architectures in general for a number of popular cryptographic algorithms. Such factors should be taken into account for overall evaluation of the word size and architecture, memory access latency, costliness of basic operations and etc. Table 1 gives a brief performance comparison of the several famous symmetric algorithms.
- *Encryption mode and data freshness*. In order to achieve semantic security, the counter (CTR) mode is normally used since the same plaintext sent at different times is encrypted into different ciphertext. Data freshness can be achieved by creating a random nonce N_M, along with the request message to the receiver.

- *Message authentication*. In order to achieve authentication and message integrity, message authentication code is needed. As the generated block ciphers can be reused, CBC-MAC is generally adopted. In addition, it is efficient and fast, and reduces the memory footprint needed for the MAC calculations.

Table 1 Alternative symmetric key algorithms

	Key/Hash	Type	Block	Overhead	Performance assessments[11−13]
DES	64-bit	Block	64bit	512-entry SBox table,256-entry table permutation	**Security strengths**: DES may not withstand a brute-force attack from modern computers. Stream ciphers are vulnerable to key-stream reuse. **Costliness of basic operations**: The workhorse of the IDEA is the multiply instructions, while for RC5 it is rotations. **Performance comparison**: A. RC5 is normally faster than RC4 due to 32-bit word operations. B. RC5 is 1.5 times faster than IDEA. **Possible energy reduction**: AES can reduce up to 33.05%, Kasumi 16.6% and DES 10% energy cost due to optimization method adopted.
AES	128, 192, 256-bit	Block	Variable	AES-128 (4,10):832 bytes required AES-256 (8,14):1142 bytes required	
Kasumi	128	Block	64bit	10,000 gates required for one instance generation	
RC5	64bit	Block	64bit	Minimum 32 -bit word computation	
RC4	128bit	Stream	8bit	64-entry SBox, 256-entry table permutation	
IDEA	128bit	Block	64bit	fifty-two 16-bit sub-keys are required	
TEA	128bit	Block	64bit	No preset tables or long set up times	
MD5	128bit	One-Way hash	512bit	Any large substitution tables are not required	
SHA1	128bit	One-Way hash	512bit	An array of eighty 32-bit words are required	

3.2 Probable application of public-key cryptography

PKC issue in sensor networks has long been considered as “not possible” due to hardware constraints of sensors. However, there is almost no quantitative analysis that supports this widely accepted conclusion. To the best of our knowledge, the first attempt on feasibility of PKC utilization in sensor network environment is Ref.[8], which is based on available network production ZigBee[5]. In such a network, a new entity called security manager is involved, whose hardware resources are sufficient for public-key operations. The authors of Ref.[8] propose a hybrid authentication key establishment scheme based on ECC (elliptic curve cryptography). The scheme puts the cryptographic burden on security manager, eliminates high-cost public-key operations at sensor side, thus achieves authentication between a sensor and a security manager during key establishment.

However, in the hybrid scheme sensors are also assumed unable to perform PKC operations. Reference [14] presents the implementation of ECC over F_{2p} for sensor networks based on MICA2[15] mote. Related figures show that public keys can be generated within 34 seconds, and the distribution among nodes of shared secrets is also achieved within reasonable costs. The latest research[16] begins to focus on optimization of the essential operations in PKC such as public key authentication. As symmetric-key based protocols are complicated and always subject to attack by adversaries, PKC utilization would be the next research focus in sensor networks security along with preliminary achievements on development of the related productions.

4 Key Management Issues

Key management plays a very key role in deploying security strategies of sensor networks, including key pre-distribution, key discovery and key maintenance. Since a sensor node couldn’t predetermine which nodes will be its direct neighbors before deployment phase, it is essential to bootstrap the establishment of a secure communication infrastructure during the pre-deployment phase. In this section, two different kinds of keying infrastructures are presented.

4.1 Multiple keying infrastructure

A single keying protocol will not be optimal for sensor network topologies, densities, sizes and scenarios[17]. Different types of keys are required to satisfy different security requirements, i.e., encryption of sensor readings, authenticated indications and etc. In addition, keys are also used as proofs of the owner's identity due to the lack of asymmetric key algorithm support at present.

4.1.1 PRF-Based key establishment

Hence how to achieve different key establishments becomes focus of the related algorithm design. Mathematically supported by the one-way property of pseudo-random function (PRF)[18], PRF-based key establishment enables each node to compute a key shared with the others. Assume that $\{f_K\}$ is a family of pseudo-random functions, from a key K, a node can derive other keys with various inputs, as $K0=f_K(0)$ for encryption and $K1=f_K(1)$ for authentication.

4.1.2 Related security mechanisms

- LEAP[9]

LEAP supports the establishment of four types of keys for each sensor node: an individual key K_u^m shared with the base station, a pairwise key K_{uv} shared with another sensor node, a cluster key K_u^c shared with multiple neighboring nodes, and a group key K_u^G that is shared by all the nodes in the network for broadcast communications of the base station. Before deployment, every node is preloaded with the two types of keys: K_u^m and K_I, which are used to derive other keys by applying PRF operations.

- LiSP[19]

Regarding data-centric routing and possible multi-level communication architecture, more attention is focused on the group-heads (GH) rather than a single sensor node. Message key (*MK*) sequences are used for encrypting/decrypting data packets with frequent renewal mechanisms on group communications. The proposed protocol uses authentication key instead of individual key for reducing its function to only verification on a node's identity.

4.1.3 Advantages and insufficiencies

- *Advantages*. By the establishment of those kinds of keys, a *secure path* between a node and BS (or CH according to the related architecture) has formed. Scalability is achieved well based on this kind of infrastructure as it supports various communication patterns, and it is effective in the key discovery phase, without a prior knowledge of post-deployment configuration and message exchange. Moreover, the meaning of group key could be expanded for purpose of securing hierarchical routing[3,20] in current sensor networks..
- *Insufficiencies*. Considerable CPU performance is required. Every sensor node needs to keep global information of the network, thus additional process mechanisms are required for possible alternate topology. Moreover, the security of this infrastructure is based on a common random function, and the security of that kind of function is not addressed. Furthermore, current research[14] shows that pseudo-random number generator has a negative effect on performance as it relies solely on a node's unique ID for seeding.

4.2 Pairwise keying infrastructure

Current Research pays more and more attentions on practical pairwise key pre-distribution scheme, which enables any two sensors to communicate securely with each other. The essential problem of the pairwise key issue has two aspects: One is how to enable any two sensors to share a common key with *minimum key information required* for every sensor node. The other is how to perform localized key establishment, preventing possible network failure once a small number of nodes are compromised. In terms of pairwise key scheme, there are two extreme design cases: Probabilistic key distribution and polynomial pool-based key distribution.

4.2.1 Probabilistic key distribution

Totally different from the schemes described above, probabilistic key distribution scheme is designed to make sure that at least *a key-shared path* exists in “almost certain” situation. Reference [21] puts forward the idea of probabilistic key-sharing and related shared-key discovery protocol, which makes a significant contribution on that kind of algorithm design. This scheme picks a random pool (set) of keys *S* out of the total possible key space. For each node, *m* keys are randomly selected from the key pool *S* and stored into the node’s memory. This set of *m* keys is called the node’s key ring. The number of keys in the key pool |*S*| is chosen such that two random subsets of size *m* in *S* will share at least one key with some probability *p*.

The authors of Ref.[21] abstract a sensor network as a random graph *G*(*n*,*p*), with the wireless communication rang limit *n*′, where *n* denotes the number of sensor nodes, *p* the probability that a link exists between any two nodes. Given a desired global probability P_c for graph connectivity, $p=\frac{\ln(n)-\ln(-\ln(P_c))}{n}$ is held. Let *d* be the expected degree of a node, thus $d = p\cdot(n-1) = p'\cdot(n'-1)$, where *p*′ is the probability that any two nodes share at least one key. As a key ring is randomly generated and pre-loaded to each node, $p'=1-\frac{((|S|-m)!)^2}{(|S|-2m)!\times|S|!}$ can be achieved. Thus the relationship between |*S*| and *m* can be determined for a desired P_c. For example, if *n*=10,000 and we want this network to be “almost certainly” *connected* with probability P_c=0.99999, then every node should have a key ring size of *m*=200 for a pool size of |*S*|=100,000 keys, under the assumption that each node has a wireless neighborhood connectivity of 40 nodes.

Reference [10] makes improvements on security strength, which requires *q* common keys (*q*>1), instead of just one. The composite *K* takes the form of $K=hash(k_1||k_2||\ldots||k_q)$. Figures show that the amount of key overlap increases, so does the resilience of the network against node capture.

4.2.2 Polynomial pool-based pairwise key predistribution

As addressed above, a bivariate *t*-degree polynomial is used to generate keys. However, this polynomial-based key pre-distribution scheme can only tolerate no more than *t* compromised nodes, and the value of *t* is limited due to the memory constraints of sensor nodes[22]. The idea of a pool of multiple random bivariate polynomials is desirable. The basic idea of the polynomial pool-based scheme can be considered as the expansion on the meaning of “key”. That is, this scheme is also based on the concept of “key pool”, whereas keys are expressed as different polynomials. Ref.[23] presents an instantiation on this idea, modeling a sensor network with a total of *N* sensor nodes as an *n*-dimensional hypercube. Thus the problem of pairwise key establishment is transformed to the connectivity issue in the hypercube model.

4.2.3 Pairwise key predistribution with deployment knowledge

For most of the applications, the sensors have low mobility, and it is reasonable to conclude that although it is difficult to precisely pinpoint sensors’ positions, it is often possible to approximately determine their locations. That is, a sensor is usually within a certain distance from its target location. By taking advantage of this observation, a location-aware deployment model for static sensor networks is developed in Ref.[24]. Similarly, [25] proposes a pairwise key pre-distribution scheme using deployment knowledge. As sensors are assumed to be pre-arranged in a sequence of smaller groups and then be dropped out sequentially, it is also reasonable to conclude that sensor groups dropped next to each other have a better chance to be close to each other on the ground.

By pre-distributing the secret keys among the sensors before deployment, key pool based pairwise key techniques are energy-efficient. Their goal is to use less memory to achieve a higher level of connectivity. However, a small number of compromised nodes may reveal a large fraction of pairwise keys shared between regular nodes. Due to the limitation on memory, it is difficult to achieve both a high connectivity and a perfect resilience. The following points need to be considered on the design of pairwise key schemes: 1) Avoiding pre-loading global sensible information on each node if possible; 2) Integration of multiple analysis model helps promote working performance as a whole; 3) Routing issue is necessarily to be addressed as it is not possible to transmit messages directly from one node in the network to another.

On the other hand, PKC techniques would eliminate the above problem. Because of its asymmetry property, sensors do not need to preload the keys among the sensors. The main focus of using PKC in sensor networks is on its expensive computation and communication overhead. Hence, it is in a dilemma to choose pairwise key or PKC. Recently, an extensive set of papers have studied pairwise key management schemes. We believe PKC will be another attractive research field for sensor networks in the coming years.

4.3 Group key issue

In some situations, sensors in adjacent areas are assumed to organize themselves to cooperate and fulfill a certain tasks. Different from clusters addressed in hierarchically organized sensor networks, a sensor group is normally created dynamically, according to specific commands emitted by the base station. Once a group is generated, the most important problem in group communication is group key management issue, including such aspects as dynamic distribution and negotiation of the initial key for a newly created group, group rekeying due to node addition or revocation, and group-identity based key scheme to secure multi-hop route to the based station. Among those three aspects, the group rekeying issue has attracted research interest as it deals with how to prevent continuous attacks with respect to node compromise and topology maintenance. PCGR (predistribution and local collaboration-based group rekeying) schemes are proposed in Ref.[26], based on the idea that future group keys can be preloaded to the sensor nodes before deployment, and neighbors can collaborate to protect and appropriately use the preloaded keys. However, in this field few research achievements are available on dynamic group establishment at present.

5 Multi-Issue Related Security Mechanisms

So far as we have introduced, we still lack a comprehensive view on network security from a system level. Key management issues are discussed for the purpose of achieving individual security, which is largely different from that of the entire network. Moreover, separated from considerations of network-related issues, a security mechanism would lose its practical value on applications. That is, the realization of various security schemes is greatly influenced by different requirements from upper applications, services provided by the lower layers, and constraints due to the properties of sensor networks. Those factors include largely different network scale, packet loss, load balancing, energy consumption, routing—aware property and etc. However, research achievements on this area are still on preliminary stage at present.

5.1 Authenticated broadcast in a time synchronized condition

μTESLA

Reference [4] makes contributions on providing the authentication scheme (μTESLA) through a delayed disclosure of symmetric keys in BS-to-all nodes communications. The authors first create a key chain $K_0,K_1,K_2,\ldots$, and the key K_0 (or K_B) is loaded in every node before deployment. Except K_0, each key of the key chains corresponds to a time interval and all packets sent within one time interval are authenticated with the same key. μTESLA achieves authenticated broadcast by two steps: The sender first broadcast the packets along with their MAC. Since the message is encrypted with K_i at that time, no one does know if that message is not a spoof from an adversary. After a time interval δ, the sender then broadcasts the key K_i. By verifying $K_0=h^i(K_i)$, the receiver then authenticates the packets received at a time interval δ before it is actually broadcasted by the sender. However, μTESLA is designed for base station broadcast. It is much more complicated when this issue is addressed in node-based broadcast.

5.2 Energy-Effective and routing-aware issues

- Routing-Based considerations

SPINS[4] has also addressed a measurable analysis on energy costs of adding security protocols as well as μ TESLA. Experimental figures based on SNEP protocol analysis show that most of the overhead arises from the transmission of extra data rather than from any computational costs. However, a security scheme only based on such hierarchy will consume much more energy if the network and physical layer information is not jointly considered[27]. It reveals a contradiction between logical hierarchy and hierarchical routing. Although various keying mechanisms are available, most of these mechanisms are irrelative to the issues of routing and network topology. We believe pairwise or group keys must be established and maintained on a hop-by-hop basis.

- Security level corresponding to energy cost

Possible communication security threats may cause different degrees of criticality on various types of messages in the sensor network. The idea of customized security mechanisms is to classify the data existing in the network into different security levels[28]. Normally the messages on the higher lever are less frequent than those on the lower lever on information exchange. Thus it’s practical and meaningful to adopt cost-effective security mechanisms on lower level messages, while on the highest level, strong encryptions are required in spite of the resulting overhead.

- Improving security without additional energy

Reference [29] applies NOVSF (non-blocking orthogonal variable spreading factor) code-hopping technique in security design without utilizing additional power for implementation. NOVSF codes are computed by assigning data blocks to time slots, where different permutations are used in every session. As a base station periodically updates mapping permutations, an adversary would have to first find the mapping pattern for the particular session before security attack on sensor nodes.

5.3 Fault-Tolerance

- One way hash-based key recovery

It is not uncommon to occur message loss due to the instantaneous failure of the network. By adopting a key-buffer with t length and applying hash computation repeatedly, a node can recover up to t lost session keys (MK)[19]. The preconditions of such a mechanism are: 1) the whole system is loosely time synchronized; 2) the node for key recovery should receive the authenticated key sequences not beyond the interval of $t\times T_{refresh}$ (refreshment interval).

- Seamless *MK* re-keying

The idea of seamless re-keying[19] is motivated by the challenge that how to switch to the new session key without disrupting the ongoing data transmission. ReKeyingTimer and key-slots are adopted to meet such requirement. The two key-slots are used to store the two keys, denoted as $\{MK_1,MK_2\}$, one is for current data encryption, and the other is for the nearest future. On receiving Initkey packet, a sensor node then sets ReKeyingTimer that expires after $T_{refresh}/2$. When the timer expires, the node switches the active key to MK_2, replacing MK_1 in the key-slot. The following key sequences are shifted to cover the place MK_2 once stored. The node then sets ReKeyingTimer to expire after $T_{refresh}$ for future key switching.

6 Other Open Issues

- *Issues on Base Station security protection*. Aside from the sensor nodes, the security issue of the base station should not be ignored, as the failure of the base station represents a central point of failure. Reference [30] points out that the base station may be more vulnerable than normal nodes to some degree, and considers strategies against a variety of threats that can lead to the failure of the base station.
- *DoS-resistance issue*. References [31,32] list various kinds of DoS attacks probably occur in sensor networks. For the purpose of promoting DoS-resistance capability on routing, Ref.[33] proposes a security mechanism to make sure another disjoint secure path available even if an intruder takes down a single node or path. However, factual situations are far more complicated than what the authors have addressed.
- *IDS issue and node misbehavior detection*. IDS (intrusion detection system) is commonly used in conventional networks, while it can hardly be applied to sensor networks at present as IDS agent is fairly expensive, and how to distribute the detection tasks over the nodes still remains a problem. The first attempt to achieve basic function of IDS is to detect possible misbehaviors of isolated nodes. Reference [10] proposes a distributed voting system to estimate the reliability of a nodes based on votes of several nodes. However, challenges arise as it still lacks an effective mechanism to deploy trust strategies between inner-network entities.

7 Conclusions

Although research on sensor networks security has achieved many notable results as addressed above, opportunities still remain in this area. On one hand, with the promotion of node’s hardware performance and further research achievements, former accepted assumptions are more likely to be unsuited. Available examples are addressed in this paper such as PKC utilization. On the other hand, more challenges arise due to the continuous change of requirements. Areas are yet unexplored including optimization of security mechanisms in terms of resources and network environment, group re-keying infrastructure, and effective detection on DoS attacks. With respect to the security architecture, future research would possibly focus on cost-effective cryptographic algorithms, feasible IDS strategies over the network, and the scalability of security mechanisms regarding various performance metrics.

Acknowledgments

Much of the review presented in this paper was the outcome of the first author’s academic visit in MSA (mobile system architecture) group, Department of Computer Science, Manchester University and the second author’s visit in the Department of Computer Science and Engineering, University of Texas at Arlington. We would like to show special thanks to Dr. N. Zhang and Dr. Y. Liu for their helpful suggestions and kind support. Finally, we would like to thank the anonymous reviewers for their comments and suggestions.

References:

[1] Chong CY, Kumar SP. Sensor networks: Evolution, opportunities, and challenges. Proc. of the IEEE, 2003,91(8):1247−1256.

[2] Krishnamachari L, Estrin D, Wicker S. The impact of data aggregation in wireless sensor networks. In: Proc. of the 22nd IEEE Int’l Conf. on Distributed Computing Systems. Vienna: IEEE Computer Society, 2002. 575−578.

[3] Ren FY, Huang HN, Lin C. Wireless sensor networks. Journal of Software, 2003,14(7):1282−1291 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/14/1282.htm

[4] Perrig A, Szewczyk R, Wen V, Culler D, Tygar JD. SPINS: Security protocols for sensor networks. In: Proc. of the 7th Annual Int’l Conf. on Mobile Computing and Networks. Rome: ACM Press, 2001. 189−199.

[5] The official website of the ZigBee alliances. http://www.zigbee.org

[6] Doumit S, Agrawal DP. Self-Organized criticality and stochastic learning-based intrusion detection system for wireless sensor networks. MILCOM 2003—IEEE Military Communications Conf., 2003,22(1):609−614.

[7] Akyildiz IF, Su W, Sankarasubramaniam Y, Cayirci E. Wireless sensor networks: A survey. Computer Networks, 2002,38(4): 393−422.

[8] Huang Q, Cukier J, Kobayashi H, Liu BD, Zhang JY. Fast authenticated key establishment protocols for wireless sensor networks. In: Proc. of the 2nd ACM Int’l Conf. on Wireless Sensor Networks and Applications. San Diego: ACM Press, 2003. 141−150.

[9] Zhu S, Setia S, Jajodia S. LEAP: Efficient security mechanisms for large-scale distributed sensor networks. In: Proc. of the 10th ACM Conf. on Computer and Communications Security (CCS 2003). Washington D.C., 2003. 62−72.

[10] Chan H, Perrig A, Song D. Random key predistribution schemes for sensor networks. In: Proc. of the IEEE Symp. on Research in Security and Privacy. Oakland: IEEE Computer Society, 2003. 197−213.

[11] Ganesan P, Venugopalan R, Peddabachagari P, Dean A, Mueller F, Sichitiu M. Analyzing and modeling encryption overhead for sensor network nodes. In: Proc. of the WSNA. 2003. 151−159.

[12] Biryukov A. Block ciphers and stream ciphers: The state of the art. http://www.esat.kuleuven.ac.be/~abiryuko/lecturenotes.pdf

[13] Chen X, Woo T. Energy efficient data encryption algorithms. 2002. http://www.vlsi.uwaterloo.ca/thwoo/ece750report.pdf

[14] Malan DJ, Welsh M, Smith MD. A public-key infrastructure for key distribution in Ting OS based on elliptic curve cryptography. http://airclic.eecs.harvard.edu/publications/secon04.pdf

[15] Crossbow I. Technology MICA2: Wireless measurement system. http://www.xbow.com/ Products/Product_pdf_files/Wireless_pdf/ 6020-0042-04_A_MICA2.pdf

[16] Du WL, Wang RH, Ning P. An efficient scheme for authenticating public keys in sensor networks. In: Proc. of the 6th ACM Int’l Symp. on Mobile Ad Hoc Networking and Computing (MobiHoc 2005). Urbana-Champaign: ACM Press, 2005. 58−67.

[17] NAI Laboratory. Advanced research on distributed sensor network security. http://www.networkassociates.com/us/_tier0/nailabs/ _media/documents/dsns.pdf

[18] Goldreich O, Goldwasser S, Micali S. How to construct random functions. Journal of the ACM, 1986,33(4):792−807.

[19] Park TJ, Arbor A, Shim IB. LiSP: A light-weight security protocol for wireless sensor networks. ACM Trans. on Embedded Computing Systems, 2004,3(3):634−660.

[20] Estrin D, Govindan R, Heideman J, Kumar S. Next century challenges: Scalable coordination in sensor networks. In: Proc. of the 5th Annual ACM/IEEE Int’l Conf. on Mobile Computing and Networking. New York: ACM Press, 1999. 263−270.

[21] Eschenauer L, Gligor VD. A key-management scheme for distributed sensor networks. In: Proc. of the 9th ACM Conf. on Computer and Communications Security. Washington DC: ACM Press, 2002. 41−47.

[22] Blundo C, Santis AD, Herzberg A, Kutten S, Vaccaro U, Yung M. Perfectly-Secure key distribution for dynamic conferences. In: Advances in Cryptology—CRYPTO’92. Santa Barbara: LNCS, 1992. 471−486.

[23] Liu DG, Ning P, Li RF. Establishing pairwise keys in distributed sensor networks. ACM Trans. on Information and System Security, 2005,8(1):41−77.

[24] Liu DG, Ning P. Location-Based pairwise key establishments for static sensor networks. http://discovery.csc.ncsu.edu/~pning/pubs/ sasn03.pdf

[25] Du W, Deng J, Han YS, Varshney PK. A pairwise key pre-distribution scheme for wireless sensor networks. In: Proc. of the 10th ACM Conf. on Computer and Communications Security. Washingtion: ACM Press, 2003. 42−51.

[26] Zhang W, Cao G. Group rekeying for filtering false data in sensor networks: A predistribution and local collaboration-based approach. http://www.cse.psu.edu/~wezhang/papers/paper-infocom05.pdf

[27] Lazos O, Poovendran R. Energy-Aware secure multicast communication in ad-hoc networks using geographic location information. In: Proc. of the IEEE Int’l Symp. on Advances in Wireless Communications (ISWC 2002). Victoria: IEEE Press, 2002. 201−204.

[28] Slijepcevic S, Potkonjak M, Tsiatsis V, Zimbeck S, Srivastava MB. On communication security in wireless ad-hoc sensor network. In: Proc. of the 11th IEEE Int'l Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE 2002). Pittsburgh: IEEE Computer Society, 2002. 139−144.

[29] Cam H, Ozdemir S, Muthuavinashiappan D, Nair P. Energy-Efficient security protocol for wireless sensor networks. http://www.eas.asu.edu/~hasancam/publications/security_sensor-2003.pdf

[30] Deng J, Han R, Mishra S. Enhancing base station security in wireless sensor networks. http://www.cs.colorado.edu/department/publications/reports/docs/CU-CS-951-03.pdf

[31] Wood AD, Stankovic JA. Denial of service in sensor networks. IEEE Computer, 2002,35(10):54−62.

[32] Karlof C, Wagner D. Secure routing in wireless sensor networks: Attacks and countermeasures. In: Proc. of the 1st IEEE Int'l Workshop on Sensor Network Protocols and Applications. Piscataway: IEEE Press, 2003. 113−127.

[33] Deng J, Han R, Mishra S. A performance evaluation of intrusion-tolerant routing in wireless sensor networks In: Proc. of the 2nd Int'l Workshop on Information Processing in Sensor Networks (IPSN 2003). California: IEEE Press, 2003. 349−364.

附中文参考文献:

[3] 任丰原,黄海宁,林闯.无线传感器网络.软件学报,2003,14(7):1282−1291. http://www.jos.org.cn/1000-9825/14/1282.htm

LI Ping was born in 1972. He is a Ph.D. candidate at the College of Computer and Communications, Hu'nan University. His current research areas are security and network cryptography.

LIN Ya-Ping was born in 1955. He is a professor and doctoral supervisor at the College of Software, Hu'nan University, and a CCF senior member. His research areas are computer networks and machine learning.

Zeng Weini was born in 1982. She is a Ph.D. candidate at the College of Computer and Communications, Hunan University. Her current research areas are security and network cryptography.