Asian Journal of Information Technology 5 (3) : 339-345, 2006

Research on The Security in Wireless Sensor Network

[1,2]L. Weimin, [1,3]Y. Zongkai, [1]C. Wenqing and [1]T. Yunmeng
[1]Department of Electronic and Information Engineering,
Huazhong University of Science and Technology, Wuhan, 430074, China
[2]University of Communication Commanding, Wuhan, 430010, China
[3]Huazhong Normal University, Wuhan, 430079, China

Abstract: As sensor networks edge closer towards wide-spread deployment, security issues become a central concern. Typical sensors possess limited computation, energy, computation, memory resources and they are always deployed in a harsh, unattended or hostile environment, so the security issues posed by sensor networks represent a rich and challenging field of research problems. In this study, we probe into various security requirements with regard to Wireless Sensor Network (WSN) and analyze status quo of the security in WSN from three aspects: key management, identity authentication as well as attacks and countermeasures. In conclusion, we point out its development direction based on the analysis and remark of problems remaining unsolved in WSN.

Key words: Sensor network, security, key management, authentication, attacks, countermeasures

INTRODUCTION

Wide-spread deployment of sensor networks is on the horizon. Wireless Sensor Network is an ad-hoc mobile network that includes sensor nodes with limited computation and communication capabilities. Due to the fact that individual sensor nodes may be deployed in harsh, unattended or hostile areas and that communication among sensor nodes is via wireless links, sensor networks are highly vulnerable to various attacks. Many applications, such as military targets sensing and tracking, are mainly dependent on the secure operation of a sensor network and it may lead to serious consequences if the network is compromised or disrupted. Up to now, much research has focused on making sensor networks feasible and useful and has not concentrated on security.

The energy-constrained nature of the sensor networks makes the problem of incorporating security very challenging. Compared with conventional desktop computers, sensor nodes have limited processing power, storage, bandwidth, and energy, so the design of the security protocols for sensor networks should be geared towards conservation of the sensor resources. A solution must strike a tradeoff between the security provided and the consumption of energy, computing and communication resources in the nodes.

The rest of the study is organized as follows. Section 2 describes various security requirements with regard to WSN. In Section 3, we analyze status quo of the security in WSN from three aspects: key management, identity authentication as well as attacks and counter- measures. Section 4 points out the development direction of WSN based on the analysis and remark of problems remaining unsolved in WSN.

SECURITY REQUIREMENTS

Wireless sensor networks have some vivid characteristics, such as limited storage, power, communication capability, massive large-scale sensor nodes deployment and variable network topology. These characteristics present many challenges for the design of protocols to bootstrap the establishment of a secure communications infrastructure from a collection of sensor nodes which may have been pre-initialized with some secret information but have had no prior direct contact with each other. A desirable security solution for wireless sensor network should satisfy the requirements[1-3] as follows.

Confidentiality: A sensor network should not leak sensor readings to neighboring networks. In many applications (e.g. key distribution) nodes communicate highly sensitive data. Once these sensitive data are captured, the security in the wireless network can't be guaranteed, so only authorized user can have access to the secret keys established and other confidential information (e.g., the identifier of each sensor node). Moreover, confidentiality

Corresponding Author: Weimin L., Department of Electronic and Information Engineering, Huazhong University of Science and Technology, Wuhan, 430074, China

should be provided by keys with as small a scope as possible to discourage a single break from compromising a large portion of the sensor network. The standard approach for keeping sensitive data secret is to encrypt the data with a secret key that only intended receivers possess, hence achieving confidentiality.

Authenticity: Message authentication is important for many applications in sensor networks. An adversary can easily inject messages, so the receiver needs to make sure that the data used in any decision-making process originates from the correct source. Informally, data authentication allows a receiver to verify that the data really was sent by the claimed sender. At the same time, the access to the shared key should be confined to only those authenticated parties in the protocol.

Integrity: In communication, data integrity ensures the receiver that the received data is not altered or tampered in transit by an adversary. In wireless sensor network, we achieve data integrity through data authentication, which is a stronger property. Moreover, the shared key must be ensured not to be modified or influenced by the outsiders and attackers.

Freshness: Given that all sensor networks stream some forms of time varying measurements, it is not enough to guarantee confidentiality and authentication; we also must ensure each message is fresh. Informally, data freshness implies that the data is recent, and it ensures that no adversary replayed old messages. Furthermore, a key establishment process ideally should guarantee its participants that each shared key is fresh, that is to say, the secret key has not been reused by one of the participants.

Scalability: The number of sensor nodes in a sensor network can be several orders of magnitude higher than the nodes in an ad hoc network and these sensors are densely deployed in large numbers. Moreover, the topology of a sensor network changes very frequently in the sense that they allow addition and deletion of sensor nodes after deployment to extend the network or replace failing and unreliable nodes without physical contact. Therefore, large wireless sensor networks cannot utilize a security scheme that has poor scaling properties for establishing and maintaining a key for the wireless sensor network as a whole or for some large subset of nodes. Dynamic environmental conditions also require the security solutions to adapt over time to changing connectivity and system stimuli.

Availability: The services provided by the security solutions in wireless sensor network must ensure that confidentiality and authentication services are available to authorized parties when needed, protecting against active attacks that attempt to interrupt service within the network. To ensure the availability of message protection, the sensor network should protect its resources from unnecessary processing of key management messages in order to minimize energy consumption and extend the life of the network. In addition, security functions should not limit the availability of the network.

Self-Organization: As wireless sensor networks must be self-organization, the security solutions must adapt themselves to the corresponding environment. It often will not be known prior to deployment where wireless sensor network will operate and where a particular node will be located. The immediate neighboring nodes of any DSN node will not be known in advance in most circumstances and in general the number of neighbors, the distances or power required to send a messages with a particular error rate from one node to another will not be known in advance. As a consequence, security solutions can't make any assumptions on sensor nodes with regard to network deployment.

Flexibility: Sensor networks will be used in dynamic scenarios where environmental conditions, threat, and tasks may change rapidly. Changing tasks may require sensors to be removed from or added to an established sensor network. Furthermore, two or more sensor networks may be fused into one or a single network may be split into two. Security schemes must be flexible enough to provide solutions for all the potential scenarios a sensor network may encounter.

STATUS QUO OF THE SECURITY IN WIRELESS SENSOR NETWORK

Traditional network security solutions based on infrastructures using trusted third parties are impractical for large scale WSN because of the unknown network topology prior to deployment, communication range limitations, intermittent sensor-node operation and network dynamics. Current proposals for security protocols in sensor networks optimize for the limited capabilities of the nodes and the application specific nature of the networks, but do not consider security as a goal. During the past few years, security has become a topic of interest in sensor networks research and a number of solutions for securing WSN have been proposed. We review related work that deals with security issues in a wireless sensor network from three aspects:

key management, identity authentication as well as attacks and countermeasures.

Key management: A key management procedure is an essential constituent of network security. Security solutions require the keys to be kept out of reach of the adversary. Moreover, sensor networks have energy-wise and computational constraints, therefore it is necessary to maintain a balanced security level with respect to those constraints.

Recently, Eschenauer and Gligor[4] propose a key management scheme designed to satisfy both operational and security requirements of wireless sensor network. The scheme includes selective distribution and revocation of keys to sensor nodes as well as node re-keying without substantial computation and communication overhead. It relies on probabilistic key sharing among the nodes of a random graph and uses simple protocols for shared-key discovery, path-key establishment, key revocation, re-keying and incremental addition of nodes.

Chan *et al*.,[5] present three new mechanisms for key establishment using the framework of pre-distributing a random set of keys to each node. First, the q-composite keys scheme trades off the un-likeliness of a large-scale network attack in order to significantly strengthen random key pre-distribution's strength against smaller-scale attacks. Second, the multi-path reinforcement scheme shows how to strengthen the security between any two nodes by leveraging the security of other links. Finally, the random pair-wise keys scheme perfectly preserves the secrecy of the rest of the network when any node is captured and also enables node-to-node authentication and quorum- based revocation.

Jolly *et al*.,[6] propose a cryptographic key management protocol, which is based on the IBSK scheme[7], but only two symmetric keys are required to be pre-deployed at each sensor. The protocol supports the eviction of the compromised nodes and the energy consumption overhead introduced by the key management is remarkably low thanks to the multi-tier network architecture in which only sensor-to-gateway secure sessions are allowed and reports order-of-magnitude improvement in energy saving as compared to the original IBSK scheme and Kerberos-like schemes.

Perrig *et al*.,[2] present a set of security protocols for sensor networks: SPINS, which is a suite of security building blocks optimized for resource-constrained environments and wireless communication. SPINS has two secure building blocks: SNEP and μTESLA. SNEP provides data confidentiality, two-party data authentication, and data freshness, but it can't support efficient broadcast authentication. μTESLA is a new protocol which provides authenticated broadcast for severely resource-constrained environments.

Zhu *et al*.,[8] describe a key management protocol for sensor networks: LEAP, which is designed to support in-network processing, while at the same time restricting the security impact of a node compromise to the immediate network neighborhood of the compromised node. LEAP supports the establishment of four types of keys for each sensor node: an individual key shared with the base station, a pairwise key shared with another sensor node, a cluster key shared with multiple neighboring nodes and a group key that is shared by all the nodes in the network. The protocol used for establishing and updating these keys is communication and energy efficient, and minimizes the involvement of the base station. LEAP also includes an efficient protocol for inter-node traffic authentication based on the use of one-way key chains.

Du *et al*.,[9] propose a new key pre-distribution scheme, which substantially improves the resilience of the network compared to the existing schemes. This scheme exhibits a nice threshold property: when the number of compromised nodes is less than the threshold, the probability that any nodes other than these compromised nodes are affected is close to zero. This desirable property lowers the initial payoff of smaller scale network breaches to an adversary, and makes it necessary for the adversary to attack a significant proportion of the network.

Liu *et al*.,[10] present a general framework for establishing pair-wise keys between sensors on the basis of a polynomial-based key pre-distribution protocol and two efficient instantiations of the general framework: a random subset assignment key pre-distribution scheme and a grid-based key pre-distribution scheme. These two schemes have a number of nice properties including high probability to establish pair-wise keys, tolerance of node captures and low communication overhead. Finally, this study presents a technique to reduce the computation at sensors required by these schemes.

Wadaa *et al*.,[11] propose a scalable key management scheme for sensor networks consisting of a large-scale random deployment of commodity sensor nodes that are anonymous. The proposed scheme relies on a location-based virtual network infrastructure and is built upon a combinatorial formulation of the group key management problem. Primary features of this scheme include autonomously computing group keys and dynamically computing the mapping of nodes to group keys using a simple hash function. The scheme scales well in the size of the network and supports dynamic setup and management of arbitrary structures of secure group communications in large-scale wireless sensor network.

A common assumption made by these random key pre-distribution schemes is that no deployment knowledge is available. Noticing that in many practical scenarios, certain deployment knowledge may be available a priori. Du *et al*.,[12] propose a novel random key pre-distribution scheme that exploits deployment knowledge and avoids unnecessary key assignments. The performance of sensor networks can be substantially improved with the use of our proposed scheme, including connectivity, memory usage and network resilience against node capture.

Identity authentication: One of the main challenges of securing communication is identity authentication or enabling receivers to verify that the received data really originates from the claimed source and was not modified en route. Traditional authentication frameworks based on public key cryptography are not suitable for sensor networks since the sensor network will ultimately consist of small, low-powered devices. The limited computational and storage resources available to sensors necessitates alternatives other than authentication based on public key certificates.

Authenticated broadcast requires an asymmetric mechanism, otherwise any compromised receiver could forge messages from the sender. Unfortunately, asymmetric cryptographic mechanisms have high computation, communication and storage overhead, which make their usage on resource-constrained devices impractical. μTESLA proposed by Perrig *et al*.,[2] overcomes this problem by introducing asymmetry through a delayed disclosure of symmetric keys, which results in an efficient broadcast authentication scheme.

Zhu *et al*.,[8] point out that μTESLA is not suitable for inter-node traffic authentication because it does not provide immediate authentication. This is because a node receiving a packet has to wait for one μTESLA interval to receive the delayed disclosed MAC key and a sensor node has to buffer all the unverified packets. Both the latency and the storage requirements of this scheme make it unsuitable for authenticating all traffic, although it suffices when authenticating infrequent messages broadcast by a base station. They propose a one-way key chain based authentication scheme which provides a solution to this problem. A salient feature of this scheme is that it supports source authentication without precluding in-network processing and passive participation.

Liu *et al*.,[13] point out that μTESLA requires initial distribution of certain information based on unicast between the base station and each sensor node before the actual authentication of broadcast messages. Due to the limited bandwidth in wireless sensor networks, this initial unicast-based distribution severely limits the application of μTESLA in large sensor networks. They present a novel technique to replace the unicast-based initialization with a broadcast-based one and further explore several techniques that improve the performance, the robustness as well as the security of the proposed method. The resulting protocol satisfies several nice properties, including low overhead, tolerance of message loss, scalability to large networks and resistance to replay attacks as well as some known DoS attacks.

Bohge *et al*.,[14] explore the task of providing data and entity authentication for hierarchical ad hoc sensor networks. Their sensor network model consists of three tiers of devices with varying levels of computational and communication capabilities. Moreover, they present a new type of certificate called a TESLA certificate, which can be used by low-powered nodes to perform entity authentication. Their framework authenticates incoming nodes, maintains trust relationships during topology changes through an efficient handoff scheme, and provides data origin authentication for sensor data. In addition, their framework assigns authentication tasks to nodes according to their computational resources, with resource-abundant access points performing digital signatures and maintaining most of the security parameters.

Attacks and countermeasures: Unless the developers take security into account at design time, sensor networks and the protocols they depend on will remain vulnerable to various attacks.

DoS attack: Some network deployments are vulnerable to immensely more powerful adversaries, let alone wireless sensor network. Strictly speaking, a DoS attack is any event that diminishes or eliminates a sensor network's capacity to perform its expected function. Hardware failures, software bugs, resource exhaustion, environmental conditions, or any complicated interaction between these factors can cause a DoS attack. Wood *et al*.,[15] present the layers of a typical sensor network and describes each layer's DOS attack types and defenses.

Sybil attack: In a Sybil attack[16], a single node presents multiple identities to other nodes in the network. The Sybil attack can significantly reduce the effectiveness of fault-tolerant schemes such as distributed storage dispersity, multi-path routing and topology maintenance. Replicas, storage partitions or routes believed to be using disjoint nodes could in actuality be using a single adversary presenting multiple identities.

Newsome *et al.*,[17] systematically analyze the threats posed by the Sybil attack to wireless sensor networks and demonstrate that the attack can be exceedingly detrimental to many important functions of the sensor network such as routing, resource allocation, misbehavior detection, etc. Furthermore, they establish a classification of different types of the Sybil attack, which enables us to better understand the threats posed by each type and better design countermeasures against each type, then propose several novel techniques to defend against the Sybil attack.

Sinkhole attack: In a sinkhole attack, the adversary's goal is to lure nearly all the traffic from a particular area through a compromised node, creating a metaphorical sinkhole with the adversary at the center. Because nodes on or near the path that packets follow have many opportunities to tamper with application data, sinkhole attacks can enable many other attacks. Sinkhole attack is very difficult to defend against, especially when it's used in combination with wormhole attack, and the best solution is to carefully design routing protocols[18] in which sinkhole attacks are meaningless.

Wormhole attack: In the wormhole attack, an adversary tunnels messages received in one part of the network over a low latency link and replays them in a different part. Wormhole attacks more commonly involve two distant malicious nodes colluding to understate their distance from each other by relaying packets along an out-of-bound channel available only to the attacker. Hu *et al.*,[19] present a technique for detecting wormhole attacks, but it requires extremely tight time synchronization and is thus infeasible for most sensor networks. Furthermore, they also present a new, general mechanism called packet leashes[20] for detecting and thus defending against wormhole attacks and present a specific protocol called TIK to implements leashes. Kwok[21] designs a protocol to implement a collaboration of GPS and non-GPS nodes as an aid to prevent this type of attack. Hu *et al.*,[22] propose a cooperative protocol whereby nodes share directional information to prevent wormhole endpoints from masquerading as false neighbors.

HELLO flood attack: Many protocols require nodes to broadcast HELLO packets to announce themselves to their neighbors and a node receiving such a packet may assume that it is within radio range of the sender. This assumption may be false: a laptop-class attacker broadcasting routing or other information with large enough transmission power could convince every node in the network that the adversary is its neighbor. The simplest defense[18] against HELLO flood attacks is to verify the bidirectionality of a link before taking meaningful action based on a message received over that link.

Selective forwarding attack: Multi-hop networks are often based on the assumption that participating nodes will faithfully forward received messages. In a selective forwarding attack, malicious nodes may refuse to forward certain messages and simply drop them, ensuring that they are not propagated any further. A simple form of this attack is when a malicious node behaves like a black hole and refuses to forward every packet she sees. However, such an attacker runs the risk that neighboring nodes will conclude that she has failed and decide to seek another route. A more subtle form of this attack is when an adversary selectively forwards packets. An adversary interested in suppressing or modifying packets originating from a select few nodes can reliably forward the remaining traffic and limit suspicion of her wrongdoing. Multipath routing[23] can be used to counter these types of selective forwarding attacks.

CONCLUSIONS

In this study, we summarize various security requirements with regard to Wireless Sensor Network and analyze status quo of the security in WSN from three aspects: key management, identity authentication as well as attacks and countermeasures. Thus far, there are still many problems remaining unsolved in WSN security.

Intrusion detection: Sensor nodes may not have global identifier because of the large amount of overhead and large number of sensors. However, a malicious sensor node may exist before WSN deployment and participate in the key pre-distribution and establishment which can lead to the exposure of all the information in the wireless sensor network. Therefore, a feasible scheme must be designed to convince that the corresponding party is not a compromised node before source authentication and data authentication. In general, up to our knowledge, existing solutions for securing WSN assume unique node identifiers, therefore, these schemes can't be applicable in true wireless sensor network.

Management and maintenance of key database: Since WSN may be deployed in hostile areas where communication is monitored and nodes are subject to capture and surreptitious use by an adversary, WSN requires cryptographic protection of communications, sensor capture detection, key revocation and sensor

disabling. Hence, each node needs to manage and maintain a key database. However, typical sensors possess limited computation, energy, computation and memory resources, so how to determine the scale of each cluster and the number of keys to be store in the database as well as how to dynamically manage and maintain the database during key establishment, re-keying and key revocation deserve our attention.

Secure routing: Current proposals for routing protocols in sensor networks optimize for the limited capabilities of the nodes and the application specific nature of the networks, but do not consider security. Owing to the fact that individual sensor nodes may be deployed in harsh, unattended, hostile areas and that communication among sensors is via wireless links, sensor networks are highly vulnerable to various attacks. However, the best solution to defend some attacks is to carefully design routing protocols and algorithms, so these protocols must be designed with security as a goal, analyzing related trust requirements, establishing threat models and presenting security goals.

REFERENCES

1. Haowen C. and P. Adrian, 2003. Security and Privacy in Sensor Networks. IEEE Computer, 36: 103-105.
2. Adrian, P., S. Robert and W. Victor *et al*., 2002. SPINS: Security protocols for sensor networks. J. Wireless Networks, 8: 521-534.
3. Adrian, P., S. John and W. David, 2004. Security in Wireless Sensor Networks. Communications of the ACM, 47: 53-57.
4. Laurent E. and D.G. Virgil, 2002. A key-management scheme for distributed sensor networks. In: Proceedings of the 9th ACM Conference on Computer and Communications Security (CCS2002). Washington D.C.: ACM Press, pp: 41-47.
5. Chan, H., A. Perrig and D. Song, 2003. Random key predistribution schemes for sensor networks. In: Proceedings of IEEE 2003 Symposium on Research in Security and Privacy. Berkeley, CA: IEEE Computer Society, pp: 197-213.
6. Jolly, G., M.C. Kuscu, P. Kokate and M. Younis, *et al*., 2003. A Low-Energy Key Management Protocol for Wireless Sensor Network. In: Proceedings of the Eighth IEEE International Symposium on Computers and Communication (ISCC'03). Turkey, 1: 335-340.
7. Carman, D., P. Kruus and B. Matt, 2000. Constraints and approaches for distributed sensor network security. Technical Report #00-010, NAI Labs, Available on, http://download.nai.com/products/media/nai/zip/nailabsreport-00-010-final.zip.D., pp: 1-126.
8. Sencun Z., S. Satia and S. Jajodia, 2003. LEAP: Effcient Security Mechanisms for Large-Scale Distributed Sensor networks. In: Proceedings of ACM Conference on Computing and Communication Security (CCS'2003). Washington: ACM Press, pp: 62-72.
9. Wenliang D., D. Jing, S.H. Yunghsiang and V. Pramod, 2003. A Pairwise Key Pre-distribution Scheme for Wireless Sensor Networks. In: Proceedings of the 10th ACM Conference on Computer and Communications Security (CCS), Washington: ACM Press, pp: 1-10.
10. Donggang, L. and N. Peng, 2003. Establishing pairwise keys in distributed sensor networks. In: Proceedings of the 10th ACM Conference on Computer and Communications Security (CCS), Washington: ACM Press, pp: 52-61.
11. Ashraf, W., O. Stephan and W. Larry *et al*., 2004. Scalable Cryptographic Key Management in Wireless Sensor Networks. In: Proceedings of the 24th International Conference on Distributed Computing Systems Workshops (ICDCSW'04). Tokyo: IEEE Computer Society, March, pp: 796-802.
12. Wenliang, D., D. Jing and S.H. Yunghsiang *et al*., 2004. A Key Management Scheme for Wireless Sensor Networks Using Deploying Knowledge. In: Proceedings of INFOCOM2004. Hong Kong: IEEE Computer Society, pp: 172-183.
13. Donggang, L. and N. Peng, 2003. Efficient distribution of key chain commitments for broadcast authentication in distributed sensor networks. In Proc. of the 10th Annual Network and Distributed System Security Symposium (NDSS2003). San Diego, California: Internet Society Press, pp: 263-276.
14. Mathias, B. and T. Wade, 2003. An Authentication Framework for Hierarchical Ad Hoc Sensor Networks. In: Proceedings of ACM Workshop on Wireless Security (WiSE'03). San Diego, California, USA: ACM Press, pp: 79-87.
15. Wood, A. and J. Stankovic, 2002. Denial of Service in sensor networks. IEEE Computer, 35: 54-62.
16. John, R.D., 2002. The sybil attack. In: Proceedings of First International Workshop on Peer-to-Peer Systems (IPTPS '02). Cambridge, MA, USA: Springer-Verlag of Lecture Notes in Computer Sci., 2429: 251-260.
17. James, N., S. Elaine and S. Dawn *et al*., 2004. The Sybil Attack in Sensor Networks Analysis & Defenses. In: Proceedings of Third International Symposium on Information Processing in Sensor Networks (IPSN'04). Berkeley, California, USA: ACM Press, pp: 259-268.

18. Karlof, C. and D. Wagner, 2003. Secure routing in wireless sensor networks: Attacks and counter-measures. In: First IEEE International Workshop on Sensor Network Protocols and Applications (SNPA 2003). Anchorage, AK, USA: IEEE Computer Society, pp: 113-127.
19. Hu, Y.C., A. Perrig and D.B. Johnson, 2002. Wormhole detection in wireless ad hoc networks. Department of Computer Science, Rice University. Technical report TR01, pp: 384.
20. Yih, C.H., P. Adrian, B.J. David and L. Packet, 2003. A Defense against Wormhole Attacks in Wireless Ad Hoc Networks.In: Proceedings of the Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2003). San Francisco, CA: IEEE Computer Society, 3: 1976-1986.
21. Jackson, K., 2004. A Wireless Protocol to Prevent Wormhole Attacks. A Thesis in TCC 402 Presented to the Faculty of the School of Engineering and Applied Science University of Virginia, Available on: www.cs.virginia.edu/~evans/theses/kwok.pdf, pp: 1-52.
22. Lingxuan, H. and E. David, 2004. Using Directional Antennas to Prevent Wormhole Attacks. In Proceedings of the 11th Annual Network and Distributed System Security Symposium (NDSS2004). San Diego, California: Internet Society Press, pp: 144-154.
23. Ganesan, D., R. Govindan and S. Shenker *et al*., 2001. Highly-resilient, energy-efficient multipath routing in wireless sensor networks. Mobile Computing and Communications Review, 4: 1-13.