Hindawi Publishing Corporation
Journal of Sensors
Volume 2015, Article ID 842392, 9 pages
http://dx.doi.org/10.1155/2015/842392

Review Article

Survey of Security Technologies on Wireless Sensor Networks

Qiuwei Yang,[1] Xiaogang Zhu,[2] Hongjuan Fu,[1] and Xiqiang Che[3]

[1]*College of Information Science and Engineering, Hunan University, Changsha, China*
[2]*School of Computer Science and Information Engineering, Hubei University, Wuhan, China*
[3]*ChangSha LeGou Network Technology Co. Ltd., Changsha, China*

Correspondence should be addressed to Xiaogang Zhu; zxg@hubu.edu.cn

Received 14 October 2014; Accepted 14 December 2014

Academic Editor: Chin-Chen Chang

Because of their low cost and adaptability, wireless sensor networks are widely used in civil, military, and commercial fields and other fields. However, since the sensor node in the calculation of the capacity, battery capacity, and storage capacity are restricted by the limitations and inherent characteristics of the sensor networks, compared to traditional networks, which makes wireless sensor networks face more security threats. This paper summarized research progress of sensor network security issues as three aspects, key management, authentication, and secure routing, analyzed and commented on these results advantages and disadvantages and pointed out the future direction of the hot research field.

1. Introduction

The rapid developments in wireless communication, sensor technology, and embedded computing technology have promoted the emergence and development of wireless sensor networks (WSN). Wireless sensor networks consist of a large number of cheap micro sensor nodes deployed in the monitoring area, which is a multihop self-organizing network system formed by wireless communication method, whose purpose is to sense, collect, and process cooperatively the information sensed by sensors in the network distributed area and then forward the results to its users.

Wireless sensor networks, as an emerging network technologies, have risen gradually recently. They can obtain a lot of detailed and reliable information in the network distributed area anytime and anywhere; thus, they are widely used in military defense, industry, agriculture, construction and urban management, biomedical and environmental monitoring, disaster relief, public safety and antiterrorism, hazardous and harmful regional remote control, and so on which are much accounted by many governments. Wireless sensor networks have a very important scientific and practical value.

However, the wireless sensor networks are usually deployed in harsh environments, such as no region or enemy positions in addition the energy, bandwidth, data processing, storage capacity, and other factors of wireless network are limited, which make wireless sensor networks vulnerable to attack. The security of wireless sensor networks is of great social concern. In particular in some important areas (such as military target detection and tracking), once the sensor network is attacked or destroyed, this would likely lead to disastrous consequences. Therefore, the way to design security mechanisms can provide confidentiality protection and authentication features to prevent malicious attacks and create a relatively safe working environment for sensor networks, which is a key issue of whether the wireless sensor networks are practical. Therefore, the issues and challenges faced by wireless sensor network security technology are becoming the main research area all over the world.

In recent years, a lot of research work on key aspects of wireless sensor network security key, protocols, algorithms, architecture, and so on has been done and has made many achievements. This paper summarized research progress situation of sensor network security issues from key management, authentication, and secure routing, three aspects, by analyzing and commenting on these results advantages

and disadvantages and pointed out the direction of future research to explore new solutions.

2. The Basis of Wireless Sensor Networks Security Theory

2.1. The Characteristics of Wireless Sensor Networks. Wireless sensor networks, as a special ad hoc network, compared with other wireless networks, mainly have the following characteristics [1, 2].

(i) *No Central Node*. Wireless sensor network has no absolutely central node, and all nodes are in equal status. Not only is it the gatherers of information but also the forwarders for other nodes transfer information. Network nodes coordinate behavior with each other through a distributed algorithm.

(ii) *Self-Organization.* A wireless sensor network requires every sensor node to be independent and flexible enough to be self-organizing and self-healing according to different situations. There is no fixed infrastructure available for the purpose of network management in a sensor network. This inherent feature brings a great challenge to wireless sensor network security as well. If self-organization is lacking in a sensor network, the damage resulting from an attack or even the hazardous environment may be devastating.

(iii) *Large-Scale.* A wireless sensor network usually consists of thousands of tiny sensors, not primarily depending on the ability to upgrade individual devices but to improve the reliability and stability of the system depending on large-scale and redundancy of embedded devices to work together.

(iv) *Volatility of Network Topology*. In wireless ad hoc network, various factors such as node mobility and decrease of the remaining power of the power control box in the sensor nodes can lead to network topology changes and make the network topology constantly change which is not regular and unpredictable.

(v) *Multihop Routing*. Wireless sensor networks use multihop routing mechanism. Due to the limits of transmitting power and the communication coverage radius, when communicating with other nodes out of the coverage, the node needs the intermediate nodes to forward.

(vi) *Data-Centric Networks*. As nodes are randomly deployed, the relationship between the network and node number is entirely dynamic, showing up that there is no necessary connection between the node number and the node position. User directly reports the events of interest to the networks; then the networks report the information accessed in a specified time to the user. Therefore, the wireless sensor network is a data-centric network.

2.2. WSN Security Needs. According to their own characteristics, the wireless sensor networks differ from the traditional wireless networks, facing more demands especially in terms of security. In order to resist different kinds of security attacks and threats and to ensure the confidentiality of the tasks performed, the reliability of data generated, the correctness of data fusion, and the security of data transmission, the security requirements are mainly in the following areas [3].

(1) Data Confidentiality. Data confidentiality is an important network security need requiring that all sensitive information in the storage and transmission process must ensure its confidentiality. Divulging the content of the information to any unauthorized user is not allowed.

(2) Data Integrity. With the assurance of confidentiality, an attacker could not get the real content of information, but the recipient does not guarantee that the data it receives is correct, because malicious intermediate nodes can intercept, tamper, or disturb the information during the transmission. Through data integrity identification, you can ensure that the data won't change anymore during its transference process.

(3) Data Freshness. Data freshness view is to emphasize that each of the received data is the latest from the sender, which makes it stop receiving repeated information. The main purpose to ensure the freshness of the data is to prevent replay attacks.

(4) Availability. Availability requires the sensor networks that can always provide information access service to the legitimate users according to the preset. But the attacker can make some or all of the sensor network paralyzed by forging and interfering signal or other methods to destroy availability of the system, such as DoS (denial of service) attacks.

(5) Robustness. Wireless sensor networks are highly dynamic and uncertain, including changes in the network topology and the nodes' disappearing or joining. Therefore, the wireless sensor networks under a variety of security attacks should have strong adaptability, and even if a particular attack succeeds, the performance can make the impact minimized.

(6) Access Control. Access control requires the ability to identify the users who access wireless sensor networks to ensure the legitimacy. Access control determines who can access the system, what system resources can be accessed, and how to use these resources.

3. The Research Progress of Wireless Sensor Networks Security

3.1. Key Management. Due to the characteristics of the wireless sensor networks, many mature key management schemes in traditional wireless networks cannot be directly applied to wireless sensor networks. In the security solutions for wireless sensor networks, encryption technology is the basis for a number of security technologies, by encrypting wireless sensor networks that can meet the needs of certification,

confidentiality, nonrepudiation, integrity, and so on. For encryption technology, key management is the key issue to be resolved.

3.1.1. Key Management Schemes Classification. In recent years, researchers have proposed many key management schemes. There can be a variety of categories for these schemes according to the characteristics of them. According to the cryptosystem they used, they can be divided into symmetric and asymmetric key management schemes. According to key distribution methods of the node, they can be split into random key management schemes and deterministic key management schemes. According to the network topology, they can be divided into distributed key management schemes and hierarchical key management scheme, and so on [4].

(1) Symmetric and Asymmetric Key Management. Depending on the difference of cryptosystem, the wireless sensor network key management can be divided into symmetric key management and asymmetric key management. In symmetric key management, the encryption and decryption key of the sensor node are the same, which is simple, and it has a small calculation and storage amount. Comparing with the asymmetric key, the symmetric key has an advantage in terms of computational complexity, but it is inadequate in the aspects of key management and security. Asymmetric key management has been considered unsuitable for wireless sensor networks, mainly due to its relatively high requirement for computing, storage, and communication capabilities of nodes. But with the gradual deepening of the relevant studies, some asymmetric encryption algorithms can now be applied in wireless sensor networks.

(2) Random and Deterministic Key Management. According to the difference of the method in which nodes obtain the key, the key management in wireless sensor network can be split into random key management and deterministic key management. In the random key management, sensor nodes get their keys from the key pool or multiple keys space by random sampling. In deterministic key management, sensor nodes calculate the determination probability to get their keys. The advantages of random key management are a relatively simple way to get the key and the flexible deployment, and its disadvantage is that there may exist part of useless key information in the sensor nodes. The advantages of deterministic key management are that it can obtain more accurate key and the session key can be established directly between any two sensor nodes. Its disadvantage is that flexibility of deployment decreases and computational overhead of key negotiation becomes large.

(3) Distributed and Hierarchical Key Management. Depending on the topology of network, the wireless sensor network key management can be divided into distributed key management and hierarchical key management. In distributed key management, the computation and communication capabilities of sensor nodes are the same, and the key negotiation and update are completed through the mutual cooperation between sensor nodes. In hierarchical key management, network nodes are split into clusters, and each cluster is composed of cluster head and ordinary sensor nodes. The ordinary sensor nodes complete key distribution, consultation, and update through their cluster head. The characteristic of distributed key management is that the neighboring nodes collaborate to achieve key negotiation. The feature of hierarchical key management is that the requirement of computation and storage capacities of the common nodes is not too high, but once the cluster head is captured by the attacker, it will threaten the security of the entire network.

3.1.2. The Typical Schemes of Key Management. Eschenauer and Gligor [5] first proposed a key management scheme for distributed sensor networks. The basic idea of the program is thata large key pool with the total number of the key is S and key identifier are generated first, each node could select m ($m \ll S$) different keys from the key pools randomly; such randomly preassigned manner made any two nodes have a certain probability of existing shared key. If there are shared keys between two adjacent nodes, then select one randomly as the paired key of the two sides to establish a secure channel. Otherwise, the entered node establishes a key path of the two sides through other neighboring nodes which exist shared key after several jumps. The advantages of E-G scheme are mainly reducing the key storage pressure of each node and suitable for large-scale WSN key management. But there are also disadvantages of this program, and its security communication is uncertainly because the establishment of shared key is based on probability.

On the basis of E-G scheme, Chan et al. [6] proposed a q-composite random key predistribution scheme. The specific implementation process of q-composite random key predistribution scheme is basically similar to E-G scheme, except that the E-G program just selects a public key as the main shared key between two nodes, while the q-composite scheme requires that two adjacent nodes can establish the main shared key after the deployment only when there is at least q shared key between them. Compared with the E-G scheme, the q-composite program improves the capacity of resisting capture attacks of nodes but increases the overlap degree of shared key between the nodes and limits the scalability of the network.

Zhu et al. [7] thought that any single key mechanism could not achieve the security needs of wireless sensor networks, so they proposed a LEAP protocol based on multiple key mechanisms to establish secure communications. The protocol maintained four keys in each node: a globally key shared with the base station, a group key shared with all nodes within the network, a paired key shared with neighboring nodes, and a cluster head key shared with the cluster head. Compared with the random key predistribution protocol, the nodes' computation loads and storage space requirements for the LEAP protocol will increase, but it can guarantee that there is a shared key between the nodes needed to exchange data and support a variety of network communication modes.

Donggang et al. [8] proposed a key distribution scheme based node group. The basic idea of the program is that

assuming that the system previously generates a large key pool S, then the S is into several subkey pools, making sure that each node deployment group has a corresponding subkey pool, such as $S_1, S_2, S_3, \ldots$, and that the size of each subkey pool was $|S_1|$. Then the nodes of each deployment group select some keys from the corresponding subkey pool randomly. Due to the fact that the establishment of the secure channel between nodes needs at least one shared key, so it requires there should be public key between the corresponding subkey pools of neighborhood groups to ensure the connectivity between nodes. Donggang et al. set up the repetition factor of the same key between the corresponding subkey pools of adjacent groups. The scheme is more safe, after the node is under attack, it has little impact on the security of other nodes in the network, but the storage overhead of such key management scheme is large; for the resource-constrained wireless sensor networks it is a very serious problem.

Du and Guizani et al. [9] think that many key management schemes which based on symmetric key considered too much about network connectivity and hope to find a method that any two nodes can get shared key while ignore the comminication of the two nodes. In the context of heterogeneous sensor networks, they proposed a route-drive public key management scheme based lightweight ECC, which only allocated communication key for neighbor node. The performance simulation shows that, compared to the symmetric key mechanism, this scheme significantly improved safety and also saved energy and storage space compared to key management schemes of other asymmetric key mechanisms.

3.2. Certification. Network security certification is another important part of the network. It includes identity authentication and message authentication, and methods used are symmetric encryption and asymmetric encryption method. This section summarizes research work on the two modes of certification.

3.2.1. Identity Authentication. Wireless sensor nodes are deployed to work after the domain, on the one hand, to ensure that users have the legal status to join the network, and, on the other hand to effectively prevent unauthorized users from joining, so the wireless sensor network authentication mechanism must be used to determine the user's identity legitimacy. By using legitimate authentication of neighboring nodes or nodes and base stations. Wireless sensor network provides secure access mechanism, when all nodes access the self-organizing network. There are currently certified questions symmetric encryption algorithm based authentication methods and authentication methods based on asymmetric encryption algorithms.

(1) Authentication Based Symmetric Encryption Algorithm. In wireless sensor networks, due to the limited energy of nodes, the nodes of computing power and communication bandwidth, computational overhead of symmetric cryptosystem is much smaller than the asymmetric cryptosystem. Considered from the perspective of resource conservation, the symmetric cryptosystem is the most suitable characteristics for wireless sensor networks.

In 2002, Eschenauer and Gligor [5] first proposed a configuration scheme of shared key that is a symmetric key management, and then secure communication can be established through the preshared key between any pairs of nodes, and also can authenticate the identity of each other. Eschenauer and Gligor's scheme has lowly computational complexity and storage burden but lack of security of the scheme.

In 2003, Chan et al. [6] proposed q-composite random key predistribution scheme based on improved E-G scheme. The model requires that the number of public keys is to be up to q; the program reduces the probability of a certain degree, the session key in wireless sensor networks overlap, and improves the anticapture capabilities and enhanced security. However, to make the part of key overlap reach q and in order to make the probability of the key overlap shared between the neighboring nodes reach preset requirements, thus we require reducing the size of the key pool, so the security may be lowered, and the key is to find a suitable size pool.

In 2005, Bauer and Lee et al. [10] proposed a distributed authentication protocol, using the concept of secret sharing and cryptography groups agree. A network concludes plurality of subgroups; each subgroup equips a base station and subgroups communicate with each other by base station. The program advantage is not employing any high consumption of encryption/decryption program in the certification process, but using the way of secret sharing and group agreed, and its fault tolerance is good; computationally efficient and authentication strength is high. The disadvantage of the program is that all nodes within the subgroup should communicate cooperatively when authenticated, it is likely to cause an information collision when the nodes delivery the determined packet.

In recent years, wireless sensor network authentication in the exploration for symmetric ciphers still did not stop. In 2010 Qiu et al. [11] proposed an efficient extensible authentication protocol to ensure that there is at least one probability of a shared key between two nodes and update the authentication key based on dynamically changing wireless sensor networks. The program has low storage overhead and energy consumption and does not cause much communication overhead. It is suitable for resource-constrained wireless sensor networks.

(2) Authentication Based Asymmetric Encryption Algorithm. Although symmetric cryptosystem has an advantage in the calculation of authentication, it has no strong asymmetric cryptography in terms of safety, and after the elliptic curve cryptosystem proposed, many studies show that even if there is a defect that the amount of computation and storage load are too large, asymmetric keys are still available for wireless sensor networks, asymmetric keys can still be used for wireless sensor networks. Here are some typical asymmetric cryptography schemes.

Watro et al. [12] proposed TinyPK entity authentication scheme based on the RSA algorithm. TinyPK authentication protocol uses a challenge-response mechanism to be able to

perform authentication for external organizations and safely transmit session key to third parties from wireless sensor network. The program uses a low index RSA algorithm, which to some extent reduces the amount of calculation and storage overhead. Meanwhile, in order to make the program adapt to the limited resources of sensor devices, TinyPK designed a protocol to make general nodes only need to perform fast, small resource consumption data encryption and signature verification work and the energy consumption of a large decryption and signature conducted by the work station with relatively ample energy or an external organization. However, TinyPK scheme security is not high. If a node is captured by the authentication, then the entire network will become unsafe, and when the key length is too long, the computational overhead is great.

Benenson et al. [13] proposed strong user authentication protocol which has improved TinyPK scheme: instead of using the key length which is shorter, use elliptic curve cryptography (ECC) which has shorter key length and with the same security strength; instead of traditional single certification, use n certification. The traditional single-user certification is that as long as one user is certified on Renyiyitai host or node; then the user can obtain legal status to enter the entire network, but n certification requires that users at least pass n-t nodes of its communication range, and then the user can obtain legal status, which improves the security to some extent, but its communication overhead is large and cannot prevent denial of service attacks.

Malone-Lee [14] in 2002 first proposed identity-based signature algorithm (IBS). The IBS is an identity-based signcryption scheme by using a concept of signcryption and based on password system on the basis of identity. However, message in dense text sign of this scheme is visible, which makes the message confidentiality threatened; on this basis, Liqun and John proposed an improved identity-based encryption algorithm [15]. The algorithm includes the creation, extraction, encryption, signature, authentication, and decryption of six stages. The similarity with the general IBE encryption algorithm is that the algorithm signs the message with the sender's private key first and then encrypted with the recipient's public key and sends a message signed to the recipient. After receiving cipher text, receiver decrypts the message first, and then according to the message decrypted to verify whether the message sent by the sender to complete the authentication statement. Simulation results show that Malone-Lee algorithm is greatly improved compared to some other identity-based signed algorithms at that time in terms of safety and performance.

In 2006, Piotrowski et al. [16] proved by experiments that, under certain conditions, a large number of public key authentication schemes which can be applied to wireless sensor networks have been proposed. In 2008, An and Peng [17] proposed Tiny ECC certification program and noted that the program is suitable for wireless sensor network applications. Li et al. [18] proposed a combination of public key-based two-way authentication protocol CPK. In 2009, Das proposed a two-factor authentication scheme [19] and used passwords and smart card way to achieve certification. In 2010, Li-Ping Zhang and Yi Wang proposed an id-based authenticated key agreement scheme [20] without a certificate. In 2011, Yeh et al. [21] proposed based on ECC encryption secure user authentication protocols. In 2012, Peng [22] proposed a multi-identity-based authentication scheme and Hong et al. [23] proposed a lightweight interactive authentication scheme. In 2013, Shi and Gong [24] overcome the deficiencies of Manik Lal [19] public key authentication scheme and proposed a new encryption based ECC authentication protocol.

3.2.2. Message Authentication. Message authentication means to confirm the message received from sender statement. Message authentication can be achieved by symmetric encryption and digital signature technology. At present, there are mainly two types of message authentication; one is point-to-point message authentication and the other is broadcast authentication. In a point-to-point message authentication, we can use most of ID authentication methods to achieve. In wireless sensor networks, in order to save resources, broadcast is a common method of transmission. Currently, TESLA protocol is the most classic broadcast authentication protocol, and a lot of research work is commenced on the TESLA protocol.

Perrig et al. [25] proposed a miniature and high efficiency time-based stream authentication protocol TESLA (micro version of TESLA) which tolerate loss package. TESLA's main contribution is the use of symmetric key technology, which achieved asymmetric encryption function, and its main idea is to use key distribution delays and one-way hash functions to achieve the irreversibility broadcast authentication. μTESLA first broadcast a packet through key authentication and then released key. The irreversibility of the one-way hash function can guarantee that no one can get any information authentication key before the release of the key, so there is no way to forge correct broadcast packets before the broadcast packet is certified.

In order to improve μTESLA, Donggang and Peng [26] proposed a modified TESLA protocol, multistage TESLA protocol. First the multistage TESLA protocol introduced schedule and broadcast initialization parameters method to replace the ways of using thin TESLA security parameters in the initialization process. Secondly, the protocol uses a multilevel secret key chain model and abandoned TESLA using secret key chains to sustain long life cycle approach TESLA. In addition, the protocol uses redundant capacity transport mechanisms and random selection strategy to complete the secret key chain publishing tasks, in order to improve network packet loss tolerance and capability of the fight against DoS attacks. While there are many good features of multilevel TESLA, the realization of the protocol is of high complexity and it takes up more of the node memory and computing resources.

The μTESLA protocol is designed for single base station sensor networks. YuLong and Qingqi et al. [27] proposed MM TESLA based on the TESLA (multiple-base station multilevel TESLA) protocol. This paper introduces the idea of threshold cryptography and proposed a broadcast authentication protocol MM TESLA which is suitable for multi station sensor network. MM TESLA and its extensions have high success ratio of authentication, high reliability, and tolerance of high

channel error rates and resist the known levels of DoS, DoM, and false message attack characteristics.

3.3. Security Routing. Routing algorithm is the basis of information transmission and convergence in the wireless sensor networks. As multihop networks, wireless sensor networks have especial characteristics, especially in the aspect of security routing and the need for in-depth research. At present, domestic and foreign scholars have proposed a variety of wireless sensor network routing protocols. This section we will describe several typical security routing protocols.

3.3.1. Data-Centric Security Routing Protocol. In view of the fact that wireless sensor networks is a data-centric network, the data-centric routing protocol has been designed for wireless sensor networks. The protocol takes into account the problem of data redundancy and obtains the fused data through collaboration between the nodes, thus improving data transmission efficiency and saves network energy.

Joanna and Wendi et al. proposed SPIN protocol [28] which is a data-centric adaptive routing protocol. In wireless sensor networks, since nodes sensing data have certain similarities, SPIN protocol can effectively reduce the amount of data transmitted and energy consumption in the network through negotiation between nodes. However, SPIN protocol needs to send inspection packet before sending the packet every time, thus causing a large data transmission delay. In addition, SPIN data broadcast mechanism cannot guarantee the reliability of data transmission.

Chalermek and Ramesh [29] designed a directed diffusion routing protocol specifically for wireless sensor networks, which was based on data-centric routing protocol model. The protocol introduces a network "ladder" concept, combining with the local routing protocol for wireless sensor networks communication. Directed diffusion process is divided into query diffusion, data dissemination, and path reinforcement. Since the establishment of directed diffusion routing requires a flood spread and causes big expense of energy and time, the algorithm is suitable for the scenario, which has a large number of queries but a short time.

Rumor routing that overcomes the problem of excessive spending from establishing forwarding path thought flood spread method was proposed by David and Deborah [30]. Rumor routing basic idea is that time zone sensor node generates agency messages, and agency messages spread outward diffusion along a random path, while the query messages from the sink node also spread along a random path in the network. When the transmission path of agency messages and query messages cross together, there is a full path from a sink node to the event area. Compared with the directed diffusion routing, rumor routing effectively reduces the routing established expense. However, because of rumors that the routing path is generated randomly, the data transmission path is not optimal path, and maybe even routing loops exist.

3.3.2. Location-Based Secure Routing Protocol. Most location-based routing protocols assumed that each node in the network knows own location information, and location nodes can exchange information with their neighbors, so that nodes can use location information to make routing choice without the need to save the routing table, and the typical protocols are GPSR and GEAR.

GPSR (greedy perimeter stateless routing) routing algorithm is the method by directly using geographic information to establish the routing path, which was proposed by Brad and Hsiang-Tsung from Harvard University [31]. GPSR algorithm uses a greedy routing strategy, and each node only needs to know the destination node of the packet and the location information of the next hop of the candidate node, which can make the right choices to send packet without the need for other network topology information, greatly reducing the consumption of maintaining network information; moreover, it has better fault tolerance and scalability, but the agreement does not take into account energy efficiency, easily lead to excessive use of certain nodes and shorten the life cycle of the network.

Yu et al. from the UCLA University, USA [32], proposed GEAR (geographic and energy aware routing) routing algorithm, which combines the directional diffusion routing and GPSR routing methods, considers the node energy in the route, and thus solves the problem of unbalanced energy consumption in GEAR. GEAR assumes that the position information of the event area is known, and the nodes know their location information and residual energy. In addition, the node via a simple Hello message exchange mechanism will be able to know the location information and residual energy information for all nodes. Routing mechanism based on these address locations and energy information establish the optimal path from aggregation node to the event area to avoid flooding, reducing the overhead of route established. However, due to the lack of sufficient topology information, GEAR may reduce the routing efficiency when encounter routing void in the routing process.

3.3.3. The Security Routing Protocol Based on Hierarchical Structure. Sensor nodes are divided into multiple clusters in the hierarchical routing protocol; each cluster has a cluster head node that can not only control communication between nodes within a cluster, but also gather and fuse data of the cluster area. Then each cluster head node will send the fused data to the gateway node, which can reduce the traffic and maintain node power consumption. Typical routing protocols are LEACH and TEEN.

A research group of Professor Wendi Rabiner et al. from Massachusetts Institute of Technology proposed that LEACH (low energy adaptive clustering hierarchy) protocol [33] is a classic clustering class routing protocol. Each round LEACH algorithm consists of establishment phase and data transmission phase of a cluster head. The algorithm allows nodes in the network balanced energy consumption and prolongs the network life cycle. But LEACH does not guarantee the position and amount of cluster heads in system, which makes the elected cluster heads distributed unevenly.

TEEN [34] was proposed on the basis of LEACH. The basic idea is that a cluster head is selected randomly periodically and equiprobably, and the other noncluster head nodes based on the nearest principle joined in appropriate cluster to form the virtual cluster and make energy of the whole network load evenly distributed to each sensor node, which can reduce network energy consumption and extend the network life cycle. In the process of establishing the cluster, the cluster head node broadcasts hard threshold and soft threshold to the other nodes, which can strike a reasonable balance between accuracy and data transmission network energy consumption by adjusting the two thresholds. Each round TEEN protocol consists of establishment phase and stable data transfer phase of clusters. TEEN agreement by a reasonable set of hard and soft thresholds only transmits the information of interest to users, which can effectively reduce traffic and the power consumption of the system. Simulation studies show that TEEN protocol is more effective than LEACH protocol. But like LEACH protocol, TEEN also will encounter similar Hello flood attacks, selective forwarding attacks, witch attacks, and so on.

3.3.4. The Security Routing Protocol Based on Multipath Transmission. Multipath routing can effectively improve the success rate of data messages submission and balance node energy consumption to prolong the survival time of the node, while multipath routing is an effective prevention method against selective forwarding attacks.

Ouadjaout et al. [35] proposed a new multipath routing SMRP and, on this basis, designed the SELF. In SELF, the control nodes in wireless sensor network send a key update command every one given slot. When the normal nodes receive the key update command, they will update their keys and report update result to the control nodes in their own cluster. The control nodes regard the normal nodes which have not updated their own keys in time as captive nodes and send making-invalid broadcast in the cluster. As a result, SELF can prevent the enemy from pretending to be a legal node by making use of the keys of captured sensor nodes.

Aiming at the problem of the traditional anonymous routing protocols being single path, Zhang et al. [36] proposed a multipath protocol MPRASRP and it can effectively prevent attackers from obtaining the identity of the source node and the destination node, thereby preventing attackers from further tracking the information processing among two nodes. The method to guarantee node anonymity is that the identity of the source node and the destination node are encrypted by the destination node public key, and only the destination node can decrypt the packet. The protocol can effectively prevent the middleman attack and even under harsh environmental conditions is also very effective, but the protocol does not prevent replay attacks.

The basic idea of the MSR [37] protocol is that, firstly, the original pieces of information are divided into subdata packets by removing code; then the subdata packets are sent out via the multiple paths. Finally, these pieces of information are combined by destination node. The agreement includes a random multipath enhanced, passive confirmation and cancellation code. Only when you need to build a random path, passive confirmation can analyze safety behavior of neighbors based on the monitor passive traffic, reduces the routing header, has a good defense against common attacks, and thus guarantees the safety of the route.

4. Some Prospects for Future Research

In recent years, we made a lot of new achievements in wireless sensor network security. However, there are still many shortcomings in security and network applicability. Based on the analysis and summary of WSN security research work above, this section will make a few prospects for future research from key management, authentication, and secure routing, three aspects.

(1) Key Management

(i) *More Efficient Asymmetric Key System.* As the features of wireless sensor network node resource are limited, asymmetric key system has been considered unsuitable for wireless sensor networks; after elliptic curve cryptography (ECC) has been proposed, asymmetric key system application in wireless sensor networks has become possible. Compared to the symmetric key system, asymmetric key system has great advantages in terms of management and security keys. In recent years, many scholars have proposed many effective key management schemes based on ECC public key infrastructure. The space of research in this area is still large in future, and the application prospects are very broad.

(ii) *Apply to Key Management Scheme of Network.* In recent years, the development of network technology puts forward higher requirements and challenges for wireless sensor network security such as the perception of information privacy issues, problems with the mobile network and Internet security systems integration, and controlling reliability issues. Obviously, the key management system which is suitable for the Internet of Things must be able to meet the security needs above. This also provides researchers with a more research space.

(2) Certification

(i) *The Establishment of a Trust Model.* Establishing trust model between nodes can reduce communication overhead between nodes and improve the efficiency of certification to some extent. It can greatly reduce system overhead to improve the network lifetime, particularly through large-scale network of trust mechanism.

(ii) *Improved Public Key Algorithm.* The public key algorithm has its advantages in terms of safety, but the calculation is too big and there is some difficulty in resource-constrained wireless sensor networks applications. How to reduce the computational complexity

of this section is one of the hot and difficult current researches.

(3) Security Routing

(i) *Multipath Routing Protocol.* In recent years, traditional single-layer sensor network only concerns the effective use of energy node, but it does not consider security issues. The researchers began to focus on multipath routing protocol security and research how to avoid the secure routing protocols which has been the victim node and the potential victim node, but currently the secure routing protocols consider the situation in which the victim node has been detected. For the victim nodes have not yet been detected, secure routing protocols can be a direction on how to avoid future research.

(ii) *Routing Protocol Hierarchy.* In addition, due to the particularity of the hierarchical sensor networks structure, they are convenient for security solutions while providing additional management overhead and other issues hierarchy; therefore, routing protocol hierarchy is a research focus in recent years.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgments

This work was sponsored by the National Natural Science Foundation of China (no. 61300036), Projects in the National Science & Technology Pillar Program (no. 2013BAH38F01), and the Foundation for University Key Teacher by the Ministry of Education, China.

References

[1] J. P. Walters, Z. Q. Lian, W. S. Shi et al., "Wireless sensor network security: a survey," in *Security in Distributed, Grid, Mobile, and Pervasive Computing*, Auerbach Publications, Boca Raton, Fla, USA, 2006.

[2] M. Sharifnejad, M. Sharifi, M. Ghiasabadi, and S. Beheshti, "A survey on wireless sensor networks security," in *Processing of the 4th International Conference: Sciences of Electronic, Technologies of Information and Telecommunications*, Hammamet, Tunisia, March 2007.

[3] P. G. Shah, "Network security protocols for wireless sensor networks: a survey," http://www.niitcrcs.com/iccs/papers/2005_42.pdf.

[4] S. Qian X, *The Key Management Scheme in Wireless Sensor Networks*, University of Science and Technology of China, Hefei, China, 2009.

[5] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," in *Proceedings of the 9th ACM Conference on Computer and Communications Security*, pp. 41–47, November 2002.

[6] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," in *Proceedings of the IEEE Symposium on Security and Privacy*, pp. 197–213, Washington, DC, USA, May 2003.

[7] S. Zhu, S. Setia, and S. Jajodia, "LEAP: efficient security mechanisms for large-scale distributed sensor networks," in *Proceedings of the 10th ACM Conference on Computer and Communications Security (CCS '03)*, pp. 62–72, ACM Press, New York, NY, USA, October 2003.

[8] D. Liu, P. Ning, and W. Du, "Group-based key pre-distribution in wireless sensor networks," in *Proceedings of the ACM Workshop on Wireless Security*, pp. 11–20, 2005.

[9] X. J. Du, M. Guizani, Y. Xiao, and H.-H. Chen, "Transactions papers a routing-driven Elliptic Curve Cryptography based key management scheme for Heterogeneous Sensor Networks," *IEEE Transactions on Wireless Communications*, vol. 8, no. 3, pp. 1223–1229, 2009.

[10] K. Bauer and H. Lee, "A Distributed Authentication Scheme for a Wireless Sensing System," in *Proceedings of the 2nd International Workshop on Networked Sensing System*, pp. 210–215, San Diego, Calif, USA, 2005.

[11] Y. Qiu, J. Y. Zhou, J. Baek et al., "Authentication and key establishment in dynamic wireless sensor networks," *Sensors*, vol. 10, no. 4, pp. 3718–3731, 2010.

[12] R. Watro, D. Kong, S.-F. Cuti, C. Gardiner, C. Lynn, and P. Kruus, "TinyPK: securing sensor networks with public key technology," in *Proceedings of the 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks*, pp. 59–64, Washington, DC, USA, October 2004.

[13] Z. Benenson, N. Gedicke, and O. Raivio, "Realizing robust user authentication in sensor networks," in *Proceedings of the Workshop on Real-World Wireless Sensor Networks*, pp. 135–142, Stockholm, Sweden, June 2005.

[14] J. Malone-Lee, Identity-based signcryption, cryptology ePrint archive, http://eprint.Iacr.org.

[15] L. Chen and J. Malone-Lee, "Improved identity-based signcryption," in *Public Key Cryptography—PKC 2005: 8th International Workshop on Theory and Practice in Public Key Cryptography, Les Diablerets, Switzerland, January 23–26, 2005. Proceedings*, vol. 3386 of *Lecture Notes in Computer Science*, pp. 363–379, Springer, Berlin, Germany, 2005.

[16] K. Piotrowski, P. Langendoerfer, and S. Peter, "How public key cryptography influences wireless sensor node life-time," in *Proceedings of the 4th ACM Workshop on Security of Ad Hoc and Sensor Networks*, pp. 169–176, 2006.

[17] A. Liu and P. Ning, "TinyECC: a configurable library for elliptic curve cryptography in wireless sensor networks," in *Proceedings of the International Conference on Information Processing in Sensor Networks (IPSN '08)*, pp. 245–256, Saint Louis, Mo, USA, April 2008.

[18] J. J. Li, L. Tan, and D. Y. Long, "A new key management and authentication method for WSN based on CPK," in *Proceedings of the International Colloquium on Computing, Communication, Control, and Management, (CCCM '08)*, vol. 2, pp. 486–490, Guangzhou, China, August 2008.

[19] M. L. Das, "Two-factor user authentication in wireless sensor networks," *IEEE Transactions on Wireless Communications*, vol. 8, no. 3, pp. 1086–1090, 2009.

[20] L.-P. Zhang and Y. Wang, "An ID-based authenticated key agreement protocol for wireless sensor networks," *Journal of Communications*, vol. 5, no. 8, pp. 620–626, 2010.

[21] H. L. Yeh, T. H. Chen, P. C. Liu, T. H. Kim, and H. W. Wei, "A secured authentication protocol for wireless sensor networks using Elliptic Curves Cryptography," *Sensors*, vol. 11, no. 5, pp. 4767–4779, 2011.

[22] S. W. Peng, "An ID based multiple authentication schemes against attacks in wireless sensor networks," in *Proceedings of IEEE 2nd International Conference on Cloud Computing and Intelligent Systems (CCIS '12)*, pp. 1436–1439, 2012.

[23] Y. H. Hong, Y. H. Zeng, and Y. J. Huang, "Mutual message authentication protocol in wireless sensor networks," in *Proceedings of the International Conference on Intelligent Information and Networks*, pp. 121–126, 2012.

[24] W. Shi and P. Gong, "A new user authentication protocol for wireless sensor networks using elliptic curves cryptography," *International Journal of Distributed Sensor Networks*, vol. 2013, Article ID 730831, 7 pages, 2013.

[25] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. E. Culler, "SPINS: security protocols for sensor networks," *Wireless Networks Journal*, vol. 8, no. 5, pp. 521–534, 2002.

[26] D. Liu and P. Ning, "Multi-level μTESLA: a broadcast authentication system for distributed sensor networks," *ACM Transactions on Embedded Computing Systems (TECS)*, vol. 3, no. 4, pp. 800–836, 2004.

[27] Y. L. Shen, Q.-Q. Pei, and J.-F. Ma, "MMμTESLA: broadcast authentication protocol for multiple-base-station sensor networks," *Chinese Journal of Computers*, vol. 30, no. 4, pp. 539–546, 2007.

[28] W. R. Heinzelman, J. Kulik, and H. Balakrishnan, "Adaptive protocols for information dissemination in wireless sensor networks," in *Proceeding of the 5th Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom '99)*, pp. 174–185, Seattle, DC, USA, August 1999.

[29] C. Intanagonwiwat, R. Govindan, and D. Estrin, "Directed diffusion: a scalable and robust communication paradigm for sensor networks," in *Proceedings of the 6th Annual International Conference on Mobile Computing and Networking*, pp. 56–57, Boston, Mass, USA, 2000.

[30] D. Braginsky and D. Estrin, "Rumor routing algorthim for sensor networks," in *Proceedings of the 1st ACM International Workshop on Wireless Sensor Networks and Applications (WSNA '02)*, pp. 22–31, Atlanta, Ga, USA, 2002.

[31] B. Karp and H. T. Kung, "GPSR: Greedy Perimeter Stateless Routing for wireless networks," in *Proceedings of the 6th Annual International Conference on Mobile Computing and Networking*, pp. 243–254, Boston, Mass, USA, August 2000.

[32] Y. Yu, R. Govindan, and D. Estrin, "Geographical and energy aware routing: a recursive data dissemination protocol for wireless sensor networks," Tech. Rep. UCLACSD TR-01-0023, 2001.

[33] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient communication protocol for wireless micro sensor networks," in *Proceedings of the 33rd Hawaii International Conference on System Sciences*, Maui, Hawaii, USA, 2000.

[34] A. Manjeshwar and D. P. Agrawal, "TEEN: a routing protocol for enhanced efficiency in wireless sensor networks," in *Proceedings of 15th International Parallel and Distributed Processing Symposium Workshops (IPDPS '01)*, Issues in Wireless Networks and Mobile, pp. 2009–2015, San Francisco, Calif, USA, April 2000.

[35] A. Ouadjaout, Y. Challal, N. Lasla, and M. Bagaa, "SEIF: secure and efficient intrusion-fault tolerant routing protocol for wireless sensor networks," in *Proceedings of the 3rd International Conference on Availability, Security, and Reliability (ARES '08)*, pp. 503–505, IEEE Computer Society, Barcelona, Spain, March 2008.

[36] Z. M. Zhang, C. G. Jiang, and J. Deng, "Multiple-path redundancy secret anonymous routing protocol for wireless sensor networks," in *Proceedings of the 6th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM '10)*, pp. 1–4, IEEE, Chengdu, China, September 2010.

[37] M. A. Moustafa, M. Youssf, and N. M. El-Dering, "MSR: a multipath secure reliable routing protocol for WSNs," in *Proceedings of the 9th IEEE/ACS International Conference on Computer Systems and Applications (AICCSA '11)*, pp. 54–59, Sharm El-Sheikh, Egypt, December 2011.