www.sensorsportal.com

Sensors & Transducers

© 2014 by IFSA Publishing, S. L.
http://www.sensorsportal.com

Researches on the Security of Cluster-based Communication Protocol for Wireless Sensor Networks

[1] Yanhong Sun, [2] Ming Tang

[1] College of Computer and Information Engineering, Hohai University
Fochen West Road No. 8, Jiangning Development Zone,
Nanjing City, Jiangsu Province, 211100, China
[2] Dept. of Information Technology Communication University of China, Nanjing,
Moonlight Square, Longjiang Community, Nanjing City, Jiangsu Province, 210036, China
[1] Tel.: 13851750157
[1] E-mail: jsjxy@hhu.edu.cn

Received: 20 April 2014 /Accepted: 30 June 2014 /Published: 31 August 2014

Abstract: Along with the in-depth application of sensor networks, the security issues have gradually become the bottleneck of wireless sensor applications. To provide a solution for security scheme is a common concern not only of researchers but also of providers, integrators and users of wireless sensor networks. Based on this demand, this paper focuses on the research of strengthening the security of cluster-based wireless sensor networks. Based on the systematic analysis of the clustering protocol and its security enhancement scheme, the paper introduces the broadcast authentication scheme, and proposes an SA-LEACH network security enhancement protocol. The performance analysis and simulation experiments prove that the protocol consumes less energy with the same security requirements, and when the base station is comparatively far from the network deployment area, it is more advantageous in terms of energy consumption and t more suitable for wireless sensor networks. *Copyright © 2014 IFSA Publishing, S. L.*

Keywords: Wireless sensor network, Cluster-based communication protocol, Security, Key.

1. Introduction

The security issue of wireless sensor networks (WSN) is an important aspect in its applications, and especially in military application fields, it is extremely important. Current researches on sensor networks mainly focus on how to save energy and effectively extend the life cycle of the networks. These researches mainly suppose that nodes in the networks are trusted regardless of malicious attacks on the network nodes. However, in practical applications, WSNs are generally configured in harsh environment, unmanned areas or enemy positions, and besides that, WSNs are inherently fragile, and they are more vulnerable to security threats than traditional networks. Specially, the malicious nodes in the network would destroy the confidentiality and authentication of the network to destroy its normal operation.

The security dangers in WSNs are due to the openness of network deployment area and the broadcast properties of radio networks. To guarantee the secret arrangement of tasks and the secure transfer and fusion of task execution results, WSNs need to implement some most basic security mechanisms: encryption and decryption, authentication, secure multicast, network hierarchy management, trust level routing, intrusion tolerance strategies and etc.

The basic date transmission of WSNs is broadcast communications. To save the communications time and the network bandwidth with the consideration of the broadcast characteristics of the wireless communications and the existence of a large number of sensor nodes in sensor networks, the base station usually needs to broadcast command messages to nodes, and the broadcast messages are easy to be corrupted or inserted with malicious information. If those corrupted or inserted messages and commands are accepted without doubt, sensor nodes will not complete expected goals of the networks. Especially in hostile environment such as battlefields and counter-terrorism systems, the nodes must be able to authenticate broadcast messages from the base station and determine the true source of the messages, and otherwise they will receive forged commands, thus causing great losses. Therefore, the broadcast authentication plays a very role in the security system of the entire network.

For the broadcast communications in large-scale networks, the sensor networks with hierarchical structures can decrease the redundancy of the number of re-broadcast, reduce conflicts by broadcasting, and shorten the broadcast complete time. The sensor networks with hierarchical structures are usually organized in clusters. Compared to ordinary member ones, the cluster heads are responsible of authenticating, forwarding broadcast message from the base station, and collecting and integrating data transmitted from member nodes. Attacks on the cluster heads are more destructive than on ordinary ones, so their security is more worthy of the attention. And due to that, it is very necessary to introduce an adequate security mechanism, especially a cluster broadcast authentication mechanism inside the clusters, in a cluster-based network. In a cluster-based network, to guarantee the legitimacy and integrity of broadcast information, a layered-based authentication is necessary, including broadcast message authentication from the base station by the cluster head nodes, broadcast message authentication from the cluster head nodes by the member nodes, and member node identification authentication by the cluster heads.

For the security issues in the cluster-based communication protocol in WSNs, the SA-LEACH is introduced in this paper based on the reasonable improvement of the LEACH. The SA-LEACH is a new security-enhancement cluster-based scheme with cluster head candidate authentication as well as broadcast authentication inside clusters. The scheme realizes the cluster head broadcast authentication during the stages of cluster formation and stabilization with lower communication energy consumption. In addition, the SA-LEACH also provides authentication for ordinary member nodes when they join clusters to effectively prevent malicious nodes from joining clusters. The SA-LEACH can guarantee the authenticity, confidentiality, integrality and freshness of the network communications in a certain extent.

This rest of the paper is structured as the followings: Part 2, analyzing current researches on the security issues of cluster-based sensor network; Part 3, describing the design and implementation process of the SA-LEACH protocol; Part 4, evaluating performance and analyzing simulation experiments of the SA-LEACH protocol; and summarizing the conclusions with further work prospects in the final part.

2. Current Researches on Security Issues of Cluster-based Sensor Networks

Due to the outstanding performance of the cluster-based routing scheme in terms of low network energy consumption and extending network lifetime, researchers have been continuously introducing more efficient cluster-based schemes while gradually starting to pay attention to security issues in cluster-based sensor networks.

Just as a surface routing protocol, the cluster-based routing scheme faces attacks including forgery, alteration, replaying messages, selective forwarding attacks, sinkholes, wormholes, Sybil and Hello flood attacks.

The cluster heads in a cluster-based sensor network are extremely important to its normal operation, and therefore they are also the main targets in attacks on cluster-based networks. If a malicious node is elected as a cluster head, a certain number of nodes in the network will join the malicious node and accept its control. Malicious nodes can launch attack such as sinkholes, selective forwarding attacks and etc.

The cluster heads in the LEACH directly communicate with the base station via single hops, and have a certain resistance against sinkholes, wormholes and Sybil. Many nodes play the role of a cluster head by turn in the LEACH, making it hard for attackers to locate and launch attacks on cluster heads. However, it is not enough to only provide security protection from periodic changes of cluster heads. Because the nodes join the corresponding clusters according to the strength of signals, malicious attackers can easily use Hello flood attacks to broadcast to the entire network with high power, making a large number of nodes join the cluster, and then the malicious nodes can launch attacks such as selective forwarding and modifying the data package to destroy the network. It should be pointed out that the flood refers to that malicious nodes send messages to a large number of nodes with the maximum power and attract node to join clusters.

Based on the above analysis, a security mechanism necessary for protect the LEACH cluster-based scheme includes: to guarantee the confidentiality and authentication of communication data in the network, making it hard for attackers to acquire usable data to attack the network; to require identification authentication of the cluster head when ordinary nodes join the cluster, authenticating broadcast for ADV messages of candidate cluster heads; to prove that ordinary nodes are legal in the network before the cluster head accepts their join, prove the common node in the network is the legitimate nodes, i.e. ordinary nodes need certification to cluster heads send Join-REQ message.

To guarantee the security of cluster-based sensor networks, many researchers in recent years have proposed some key management schemes and security strengthening scheme for cluster-based routing protocols, such as SCAF, RLEACH, SLEACH, Sec-LEACH, sec-HSN and etc. The following is an introduction for typical ones.

SCAF [1]: this scheme uses a two-way evaluation between cluster heads and member nodes, and filters out malicious nodes before the network begins to choose cluster heads, preventing malicious nodes from becoming cluster heads.

RLEACH [2]: this scheme is proposed with random pairwise keys (RPK) to strengthen the security of cluster-based routing protocols. Its main contribution is to provide an effective secure communication guarantee for the LEACH, and improve the RPK to be suitable for cluster-structured sensor networks.

Dynamic key establishment protocol [3]: it is introduced to guarantee the secure communications between member nodes and cluster heads for clustered sensor network. In regard to the characteristics of periodic changes of cluster heads in a cluster-based network, the two protocols can establish new keys between member nodes and new cluster heads during the change of cluster heads. The first one uses a simple hash and XOR operations to establish keys dynamically between cluster heads and member nodes, and the storage consumption of each node in it is a certain number. The second one uses a polynomial key distribution scheme, and its storage consumption is a little higher than the first one, but it takes no additional communication cost in its key establishment process.

SLEACH [4]: it distributes a symmetric key for each node shared with the base station before the network deployment. With the help of the base station, it authenticates adv messages from cluster head. The whole SLEACH clustering scheme is in 3 steps: preparation stage for the network deployment, cluster formation stage and stabilization stage. The same with the LEACH, the SLEACH also supposes that the nodes in the network can communicate directly with the base station.

Security analysis of the SLEACH: The goal of the SLEACH protocol is to provide access control and prevent attackers from participating in the network operation, particularly to prevent attackers from becoming cluster head nodes. However, loading only two keys in each node can’t provide the mechanism of proving legal identification to the cluster heads for valid nodes. In addition, ordinary nodes share keys only with the base station, and cluster heads can’t authenticate monitoring data from ordinary nodes, and they can only forward all monitoring data along with aggregated data to the base station. The base stations will authenticate the legal identification of nodes and the legitimacy of the monitoring data and that greatly increases the communication cost within the network, increases the station's burden, and decreases the working efficiency of the network.

Sec-LEACH [5]: the protocol studies the network model with similar assumptions as in the LEACH and SLEACH, namely the nodes in the network can adjust its energy of sending data, and communicate directly with the base station at the cost of the highest energy consumption.

Security analysis of the Sec-LEACH: The Sec-LEACH protocol does not authenticate the broadcast messages of the candidate cluster heads, and it only explains that the authentication for adv messages can refer to the SLEACH scheme. In addition, the Sec-LEACH protocol only considers that the nodes send data to the cluster heads and provides specific measures to guarantee the communication security, but it does not consider that the cluster heads need to broadcast messages similar to the commands to members in the stabilization stage, that is to say that the Sec-LEACH has no reliable authentication mechanisms for clusters.

Sec-HSN [6]: it is a key distribution scheme for heterogeneous cluster-based sensor networks. In the network model, there are a certain number of high-energy nodes (sensor nodes with strong energy as well as computing communication capabilities) and massive low energy nodes (ordinary sensor nodes). In the network operation period, high energy nodes act as cluster heads, and low energy nodes do as member nodes within clusters. The protocol is not suitable isomorphism sensor networks.

The SLEACH, Sec-LEACH and Sec-HSN are security encryption schemes all aiming at the LEACH clustering protocol. In the SLEACH, Each sensor node distributes two keys: one is shared with the base station, and the nodes use it to compute message authentication codes for the authentication communication between the nodes and the base station; the other is the latest key in one-way hash chain generated by the base station, the nodes uses it to identify malicious cluster head nodes with the help of the base station. However all candidate cluster heads in the SLEACH require transmitting radius set to reach the base station when sending ADV messages, and the energy consumption is higher. In the Sec-LEACH, each node pre-distributes K keys from the key pool, and compared with the SLEACH, its main advantage is the secure communication between cluster heads and member nodes without the base station involved. The Sec-HSN is a key management scheme for cluster-based sensor networks.

3. Design of the SA-LEACH Protocol

The broadcast operations of cluster head nodes are relatively frequent in cluster-based sensor networks. In the cluster formation stage, nodes independently becoming cluster heads need to broadcast *adv* messages to nodes in the networks to declare its cluster head status; in the stabilization stage, the cluster heads not only aggregate the monitoring data from members inside the clusters and send them to the base station, but also need to release the queries and commands to cluster members to control their operation. For possible security attacks on cluster-based sensor networks, it is necessary to provide broadcast authentication for the two broadcasts of the cluster heads to guarantee that the network nodes work under the control of legal cluster head nodes. The SLEACH and Sec-LEACH consider the broadcast authentication issues of cluster heads in the cluster formation stage, but they require the cluster heads to send adv messages to the base station that will authenticate, and the communication energy consumption is higher. For the broadcast authentication in the stabilization stage, documents [7] and [8] propose to use cluster keys (those shared by all nodes inside the clusters, including shared by cluster heads) to authenticate the messages broadcast from the cluster heads, and the potential security risk is that any node will reveal the cluster keys if captured.

3.1. Model and Symbol Convention of the SA-LEACH Protocol

The SA-LEACH protocol in this paper is a network model for all nodes with equal storage, computation and communication capability except base stations. The network has two layers, namely the whole WSN is divided into a number of clusters, and each cluster consists of a cluster head node and a certain number of member nodes. The scheme is also designed based on the following reasonable hypotheses:

1) The base station can be trusted with the ability of intrusion detection, and it can detect whether the node state is normal or not and thus determines whether to trigger the operation of deleting nodes or not.

2) All nodes can directly communicate with the base station at the highest energy, and in order to save energy, they rarely do it. In most cases only cluster heads send aggregated data directly to the base station.

3) A node can judge the distance of a message source relative to itself, such as according to the intensity of the received signals.

4) A single hop communication is between cluster head nodes and members, as well as between cluster heads and base stations.

5) All nodes including the base station are loose time synchronization [9-11].

The meanings of the symbols used in the protocol are as the following:

Q Size of the key pool;

w Size of each key ring loaded; to each node;

G All nodes in the whole network;

IDX A unique global node identifier;

RN Random number;

H HASH function;

p Percentage of the number of cluster heads to the all nodes in each round in the network;

r Counter, recording the round number of the network's operation;

c Loop number of the network's operation;

KIDj, s A key used by the node j to authenticate the identification of cluster heads in Round s in a certain loop;

KSIDj, C A key set used by the node j to authenticate the identification of cluster heads in cth loop;

KIDj,BS A symmetric key shared by the node j and the base station;

OHCX A HASH chain generated by the node x;

δ µTESLA timeslot used by the cluster heads during the broadcast insert the cl;

commX A convention value for the HASH chain used by the node x;

MaxD Key delay declared from µTESLA used by the cluster heads during the broadcast insert the clusters;

E(K,X) Encrypt the message X with the key K;

MAC(K,X) A message authentication code computed with the key K for message X;

⇒ → Broadcast and unicast respectively.

3.2. Secure Clustering Scheme of the SA-LEACH

Similar to other security enhancement clustering schemes, the SA-LEACH is composed of three steps: preparations before the network deployment, cluster formation stage and stable stage.

3.2.1. Preparations before the Network Deployment

1) Before the network deployment, the SA-LEACH creates a key pool with the size of *Q, and* assigns a global unique node identifier $ID_{x.}$ $ID_{x.}$ is input as a seed into PRNG to generate w pseudo random numbers. Round Q to get w remainders as R_x, and select w keys in accordance with R_x from Q to load into each node.

2) The base station uses random number RN_m and single-way hash function to generate a *RN* chain with the length of 1/*p* (which is ideally the percent of cluster heads among all nodes in the network). Make

RN_1 as the conventional value of the RN chain. Then the base station computes the key $K_{ID_j,\ s}$=*H(ID_j* || s ||RN_s）used in the first loop for each node (1/*p* is one loop in the network operation), in which, *s* refers to the number of round, and $0 \le s \le (1/p)$-1. Make up the key set KS_{ID_j} with 1/*p* $K_{ID_j,\ s}$ to load the nodes in accordance to ID_j. (The suffix 0 means that the key set is used in the first loop after the network deployment, and the loop number starts from 0.)

3) The base station generates a one-way hash chain OHC_{BS} for broadcast authentication, and make its convention value as $comm_{BS}$. Suppose the announcement interval time of OHC_{BS} as *δ*. Load *δ and* $comm_{BS}$ into each node.

4) Each node loads PRNG and a symmetrical key $K_{ID_j,\ BS}$ shared with the base station to guarantee the direct communication security of nodes with the base station after the nodes become the cluster head nodes and the communication security when the base station declares the key set of the next loop. Each node maintains a counter *r* to record the rounds of the current work. Its value is 0 initially, and increases with 1 each round after the network deployment.

3.2.2. Cluster Formation Stage

Step 1: The base station broadcast the command of Start and authenticates this command with the broadcast authentication scheme μTESLA. After a period of δ, the base station declares the authentication key for this command, and all nodes can authenticate its legitimacy. If it is true, all nodes will execute the step 2.

Step 2: A node randomly selects a number between 0～1, and compares it with the threshold *T (n).* If the number is less than *T (n),* the node will become the cluster head in this round. Once the node selects itself to become the cluster head (marked as CH_i), CH_i will first generate a one-way hash chain for the broadcast authentication OHC_{Ch_i} and makes the conventional value of the chain as $comm_{CH}$, the maximum time delay of the broadcast in the clusters as Max_D and the z^th^ key in its one-way hash chain as OHC^Z_{Chi}. CH_i broadcasts the *adv* message of itself as the cluster head, and the message includes its identifier, a current value *nonce* and $comm_{CHi}$, and uses the s^th^ key $K_{Chi,s}$ (*s*=*r mod (*1/*p)*)in the key set $KS_{Ch_i,C}$ to compute MAC value (the number 0 loop is $KS_{ID_j,\ 0}$ the base station directly loads into the nodes after the network deployment).

$$CH_i \Rightarrow G : ID_{CH_i} \parallel adv \parallel nonce \parallel comm_{CH_i} \parallel$$
$$\parallel Max_D \parallel MAC\left(K_{CH_i,S}, ID_{CH_i} \| adv \| nonce \| comm_{CH_i} \| Max_D\right) \quad (1)$$

Step 3: Non-cluster head nodes N_i collect all broadcast messages of cluster heads and record the signal intensity. The base station broadcasts the command of Stop, and all nodes stop the broadcasting and cache information into the standby. The authentication process of this command is the same as that of the command of Start.

Step 4: The base station broadcasts RN_s to all nodes.

Step 5: Non-cluster head nodes receive RN_s, and then get $K_{Chi,s}$ in accordance to each candidate cluster head by computing *H(* ID_{CH_i}|| s ||RN_s. $K_{Chi,s}$ is used to authenticate the cache information in step (2). If the authentication passes, these broadcast messages are considered to be sent from legal cluster heads. The legal cluster identifiers CH_i is sent to PRNG respectively to generate w random numbers to get R_{Chi}, Non-cluster head nodes N_i computer b∈(R_{Ch_i}∩R_{N_i}) to get the set of cluster head nodes sharing its key, and select the cluster head with the strongest signal to join. It sends the request message *join_req* to the cluster head. The message includes the cluster head identifier, node identifier and *b*. To guarantee the authentication of the node identification, it uses the key in accordance to *b to* compute MAC for *join_req* and sends to CH_i.

$$N_i \rightarrow CH_i : ID_{N_i} \parallel ID_{CH_i} \parallel join\_req \parallel b \parallel nonce \parallel$$
$$\parallel MAC\left(K_{[b]}, ID_{N_i} \| ID_{CH_i} \| join\_req \| b \| nonce\right) \quad (2)$$

Step 6: The cluster head receives all requests and send the confirmation message to all nodes requesting to join. The message includes cluster head identifier and work interval in accordance to each cluster member node. Its MAC computed with the first key OHC^1_{Chi} on the OHC_{CHi} . Non-cluster head nodes receive the message and cache it. After the period of Max_D , the cluster head declares the authentication key of the previous time period, and all nodes can correctly authenticate the confirmation message from the cluster head broadcast.

$$CH_i \Rightarrow N_i : ID_{CH_i} \parallel ID_{N_i} \parallel \left(\ldots,\left\langle ID_{N_i}, T_{N_i}\right\rangle,\ldots\right) \parallel$$
$$\parallel sched \parallel MAC\left(OHC^z_{CH_i}, ID_{CH_i} \| \left(\ldots,\left\langle ID_{N_i}, T_{N_i}\right\rangle,\ldots\right) \| sched\right) \quad (3)$$

When the cluster formation phase ends, the network is divided into several clusters. However, the ordinary nodes only select those cluster heads sharing keys with them to join, and therefore some orphan nodes will exist after each round of cluster formation. There are two ways to deal with the orphan nodes: one is to make it as an independent cluster in the current round, and the node acts not only as a cluster member but also as the cluster head, responsible for monitoring data and sending them monitoring results to the base station; the other is to let the node asleep to save energy in the current round.

3.2.2. Stabilization Stage

The operations of the SA-LEACH in the stabilization stage mainly include three types: the first is that after the cluster formation, the nodes in the cluster perform monitoring task respectively during their active time interval and send data to the cluster heads in the authentication mode, and then the cluster heads aggregate and send data to the base station; the second is that the base station sends the key set that will be used in the next round of loop to the cluster heads in the current round, and the cluster head nodes update the current key set in their own storage area; and the third is that the cluster heads broadcast to member nodes in the cluster with messages similar to the operation commands.

The nodes send monitoring data to the cluster heads:

$$N_i \rightarrow CH_i : ID_{N_i} \parallel ID_{CH_i} \parallel nonce \parallel \\ \parallel E\left(K_{[b]}, ID_{N_i} \| ID_{CH_i} \| data_{N_i} \| nonce\right) \tag{4}$$

The cluster heads send aggregated data to the base station:

$$CH_i \rightarrow BS : ID_{CH_i} \parallel ID_{BS} \parallel nonce \parallel \\ \parallel E\left(K_{CH_i \cdot BS}, ID_{CH_i} \| ID_{BS} \| nonce \| F\left(\ldots, data_{N_i}, \ldots\right)\right) \tag{5}$$

The base station receives the data from the cluster heads and sends them the key set used in the next round of loop.

$$BS \Rightarrow CH_i : ID_{BS} \parallel ID_{CH_i} \parallel nonce \parallel \\ \parallel E\left(K_{CH_i \cdot BS}, ID_{BS} \| ID_{CH_i} \| nonce \| KS_{CH_i \cdot c+1}\right) \tag{6}$$

If the cluster heads do not send any data to the base station in the stabilization stage, it will arrange a new key set request message *NKS_req* by the end of the current work, and the cluster heads will send this message to the base station:

$$CH_i \rightarrow BS : ID_{CH_i} \parallel ID_{BS} \parallel NKS\_req \parallel nonce \mid \\ \parallel MAC\left(K_{CH_i \cdot BS}, ID_{CH_i} \| ID_{BS} \| NKS\_req \| nonce\right) \tag{7}$$

The base station receives the request and sends the key set used in the next round of loop to the cluster head.

In the stabilization phase, the cluster heads need to broadcast command messages inside the cluster, such as query, update and etc.

$$CH_i \Rightarrow N_i : ID_{CH_i} \parallel ID_{N_i} \parallel cmd \parallel nonce \parallel \\ \parallel MAC\left(OHC^{z}_{CH_i}, ID_{CH_i} \| ID_{N_i} \| cmd \| nonce\right) \tag{8}$$

The cluster heads broadcast messages inside the cluster and use the zth key in the one-way hash chain $OHC^{z}{}_{Chi}$ to compute MAC. The nodes in the cluster receive and store the messages in the buffet, and after the maximum delay Max_D, the cluster heads declare the correspondent $OHC^{Z}{}_{CH_i}$. The nodes in the cluster receive the key to compute whether H($OHC^{Z}{}_{CH_i}$) is equal to $OHC^{Z\text{-}1}{}_{CH_i}$ to judge the legitimacy of $OHC^{Z}{}_{Ch_i}$ If they are the same, the cluster heads use $OHC^{Z}{}_{Ch_i}$ to authenticate $MAC(OHC^{Z}{}_{CH_i}, ID_{CH_i}||ID_{N_i}|| ||cmd||nonce)$. If the authentication passes, it will receive the broadcast message and replace $OHC^{Z\text{-}1}{}_{Ch_i}$ with $OHC^{Z}{}_{Ch_i}$, otherwise the message will be discarded. cmd is the command broadcast from the cluster heads.

4. Performance Evaluation and Simulation Analysis of the SA-LEACH Protocol

4.1. Security Analysis

Compared with the LEACH protocol, the SA-LEACH protocol provides authentication, integrity, confidentiality and freshness for communications between nodes. Its biggest advantage is that it introduces appropriate authentication mechanisms for broadcast message of nodes in a local area. It includes the *adv* message authentication from the candidate cluster heads during the cluster formation stage and broadcast authentication when the cluster heads broadcast *cmd* messages. The candidate cluster head authentication guarantees that attackers can't disguise as cluster heads to attract ordinary nodes to join because they do not know the key $K_{CH_i, s}$ used in the current loop and in the current round of the network. During the cluster formation phase, the candidate cluster heads generate a one-way hash OCH_{Ch_i} used in the broadcast authentication in the stabilization phase, and send the conventional value to the cluster members, so the cluster heads can use OCH_{CH_i} for broadcast authentication inside the cluster in the stabilization stage.

In the SA-LEACH secure cluster-based scheme, the candidate cluster heads broadcast the *adv* message of its cluster head status and use $K_{CH_i, s}$ in the current round to computer MAC, and the base station broadcasts RN_s. Each ordinary node gets

$K_{CH_i,s}$ by computing the value of the hash chain to authenticate the *adv* message broadcast from the candidate cluster heads and to authenticate the legal identification of the candidate cluster heads to prevent malicious nodes as cluster heads.

Ordinary nodes authenticate the identification of candidate cluster heads, and choose the nearest cluster heads with the shared keys to join the cluster. The *join_req* message of ordinary nodes to join the cluster contains b and uses $K_{[b]}$ to compute MAC, and the cluster head can find the keys shared with each ordinary node to authenticate the identification of ordinary nodes, so as to prevent malicious nodes joining the cluster.

The cluster member nodes encrypt the message the monitoring data send to the cluster head with the shared key $K_{[b]}$ by the two, guaranteeing the confidentiality of the monitoring data while authenticating the message source. It is significantly important for some specific applications requiring the high confidentiality of the monitoring data. The message the cluster heads send to the base station (5) also uses the shared key $K_{ID_j,BS}$ by the cluster heads and the base station for encrypting data. The message used in the next loop that the base station sends to the cluster head node(6) uses the key shared by the cluster heads and the base station for the key set $KS_{ID_i,C+1}$ encryption while guaranteeing the communication authentication and confidentiality between the cluster heads and the base station.

If the cluster head does not send aggregated data to the base station in the current round, it can directly send the new key request message *NKS_req* for the next cycle to the base station, which uses the key shared by the base station and the cluster to compute MAC for the authentication. A command message that the cluster head node broadcasts to members uses the μTESLA broadcast authentication scheme, using the OHC_{CH_i} key generated in cluster formation stage to compute MAC and release the key for the authentication operation for the cluster head broadcast.

All the above security mechanisms have one premise that a node in the network cannot be captured by attackers. Once an attacker captures a node and if the attacker has enough resources, it can obtain all keys used in the security mechanism, and the network security will be severely damaged. In fact, many current protocols for the security of WSNs cannot respond well to node capture problems. Reference [12] provides the definition of node capture: attackers successfully control the nodes in a network after the network deployment. Generally, once an attacker finds a node and uses its own tools (notebook computer, cable and so on) to access node data or load new data to the node, it is a serious blow to the network's secure operation.

When the network is deployed in a hostile environment, it is possible to capture nodes. Many researchers have studied intrusion detection systems in sensor networks [13-15], and these studies mainly focus on how to find and locate captured nodes. The SA-LEACH assumes that the network uses one intrusion detection technology, and with its help the cluster heads find and locate the ID of a captured node and send the ID to the base station. The base station also can find and locate the ID of the captured cluster head node. The base station periodically announces the IDs of the captured nodes throughout the network, and all other nodes delete the keys shared with the captured nodes from the memory to remove the captured nodes out of the network.

Without considering the premise of node capture, the SA-LEACH can prevent the attacker from becoming cluster heads and broadcast authentication in the cluster. If there is the problem of node capture, the intrusion detection technology can be introduced into the network, periodically removing captured nodes to effectively guarantee the network security.

4.2. Comparison with other Protocols

The SA-LEACH protocol in this paper is to strengthen the security of the clustering protocol. The original LEACH scheme almost has no considerations for security, and it only uses the periodical changes of the cluster head identification to increase the difficulty for attackers to attack cluster-heads [16], but it cannot prevent malicious nodes from becoming cluster heads since it does not provide the identification authentication for the candidate cluster heads.

1. Comparison between the SA-LEACH and SLEACH.

Each node in the SLEACH protocol uses two keys: one is shared with the base station, and the other is the latest key generated by the base station on the one-way hash chain. The SLEACH protocol uses the key shared with the base station for computing a message authentication code, and ordinary nodes can authenticate broadcast messages of cluster heads to authenticate the legitimate cluster heads with the help of the base station and join to form a cluster. However, the SLEACH does not provide a mechanism for ordinary nodes to prove identification to cluster heads, and this will make it possible for malicious nodes to join the clusters. The SLEACH does not introduce the broadcast authentication of cluster heads after the cluster formation, and it cannot guarantee the authentication of broadcasting commands or querying information of cluster heads in the cluster.

2. Comparison between the SA-LEACH and Sec-LEACH.

Compared with the Sec-LEACH, the SA-LEACH protocol has two advantages: first, the SA-LEACH introduces the cluster head authentication in the cluster formation stage, preventing malicious nodes from becoming cluster heads while the Sec-LEACH uses the SLEACH to authenticate candidate cluster head identification, and its biggest disadvantage is that it needs candidate cluster heads in a cluster formation stage to send broadcast messages to the base station. The LEACH protocol network model assumes that the network deployment area is far from the base station, which makes the authentication of the Sec-LEACH on candidate cluster heads during the cluster formation stage more energy. However, the SA-LEACH authentication does not require the candidate cluster head to send directly broadcast messages to the base station in a cluster formation stage for the identification authentication of candidate cluster heads, and the candidate cluster heads broadcast adv messages locally within the network, then the base station broadcasts RNs. All nodes receive only RNs to authenticate the identification of candidate cluster heads, greatly reducing the energy consumption due to the cluster head status authentication. Secondly, the SA-LEACH introduces authenticated broadcast inside the cluster in the stabilization stage. Each cluster head computes one-way hash chain OHCCHi used in the current round for calculating the MAC value in the cluster formation stage, and the agreed value in cluster formation stage selects candidate cluster heads to broadcast the adv message of its status as the cluster head to the nodes around, and so the cluster head in stabilization stage can realize the cluster broadcast authentication with the help of OHCCHi . If the Sec-LEACH needs to broadcast within the cluster, it has to calculate MAC values respectively for each cluster member, and send the same message repeatedly (different MAC values), and it costs more energy than one broadcast (the energy consumption of node wireless communications is much higher than other operations).

3. Comparison between the SA-LEACH and L-LEACH.

Compared with the L-LEACH, the SA-LEACH has the following advantages. Firstly, the L-LEACH requires grouping nodes before the network deployment, and the nodes in the same group form a cluster deployed in a grid area, and the cluster members remain stable through the whole network operation. This has some limitations. However, the SA-LEACH finds and forms clusters through sharing keys, and the nodes and the network topology can change dynamically, meeting the basic requirements of the wireless network deployment. Secondly, the L-LEACH requires determining the maximum number of broadcast in clusters each round during the network operation before the network deployment, and it is a harsh and abnormal requirement. Before the network deployment, the protocol requires each node to maintain OHC agreed value for all other members in the same group (cluster), increasing the storage cost of nodes. During the network operation, each round finally needs to specially separate time for cluster heads to announce OHC agreed value used in its next re-election as cluster-head, increasing the cost and complexity of the protocol. In the SA-LEACH, the newly elected cluster heads broadcast the required OHC in the cluster in the cluster formation stage each round, and then inform the cluster members. Whether the storage cost for members to maintain the agreed value or the protocol complexity is relatively low, and it is a more reasonable choice.

4.3. Simulation Analysis

The Sec-LEACH and SA-LEACH algorithm are performed respectively in the Matlab to get the comparison relationship between the network lifecycle and energy consumption.

1. Lifecycle

The death time of the first node (first_dead), the death time of half of nodes (HND) and the death time of the last one (LND) in the simulation process of network operation in 10000 rounds are used to measure the network's lifecycle. The number of broadcast of cluster heads in the cluster is 4 during the stabilization stage in each round which can be seen from Table 1.

Table 1. Lifecycle Comparison Between the Sec-LEACH and SA-LEACH.

Algorithm	First_dead	HND	LND
Sec-LEACH	3122 rounds	4323 rounds	10000 rounds
SA-LEACH	3258 rounds	4451 rounds	0 round

From the data above, it can be seen that the SA-LEACH reduces more energy than the Sec-LEACH, and extends lifecycle longer with more effective energy. After 10000 rounds, there are two nodes still alive in the SA-LEACH network.

2. Comparison of total number of death nodes

When the network runs respectively after 1000, 2000, 3000, 4000, 5000, 6000, 7000, 8000, 9000 and 10000 rounds, the total number of death nodes in the Sec-LEACH and SA-LEACH are shown in Table 2. It should be noted that in the simulation process there is no consideration for the communication cost the network sends data, but for extra communication cost in strengthening security in the two protocols.

Table 2. Relationship Between total number of death nodes and simulation rounds in the Sec-LEACH and SA-LEACH.

Simulation Rounds	1000	2000	3000	4000	5000	6000	7000	8000	9000	10000	1000	2000	3000
Sec-LEACH	0	0	0	42	78	96	97	98	99	100	0	0	0
SA-LEACH	0	0	0	29	72	94	97	97	98	98	0	0	0

It can be seen from Table 2 that in each round of the network operation the total number of death nodes of the SA-LEACH is always less than the Sec-LEACH

3.Relationship between the total number of death nodes and the distance of the base station from the network deployment area

When the simulation program runs after 4000 rounds, suppose the number of broadcast is 4 in the cluster in the network operation which can be seen from Table 3.

Table 3. Relationship between the Total Number of Death Nodes and the Distance of the Base Station from the Network Deployment Area (4000 rounds).

Distance of the base station from the network center	125 m	150 m	175 m	200 m	225 m	250 m
SA-LEACH	29	29	39	41	46	49
Sec-LEACH	42	42	43	50	56	60
Percentage of Less Death Nodes	13	13	4	9	10	11

From the simulation results, it can be seen that when the distance of the base station from the network deployment center area changes from 125 to 250 meters, the number of death nodes of the SA-LEACH protocol is smaller than the Sec-LEACH run after for 4000 rounds, and therefore the SA-LEACH performs better than the Sec-LEACH in saving communication energy consumption.

4. Comparison of the number of death nodes with different broadcast times

From the previous analysis, suppose the broadcast number in the cluster the two protocols in the stabilization phase is 4, but that will also have some application of stable phase cluster radio frequency may be less. In order to further analyze the energy advantage of the SA-LEACH broadcast authentication in clusters, the energy consumption comparison is made for f 1 to 5 times of the broadcast in the cluster of each round for the SA-LEACH and Sec-LEACH. The simulation program runs based on the parameter of 250 meters from the base station to the network deployment center area and total 4000 rounds of network operation.

The simulation results can be seen from Table 4.

Table 4. Comparison of the Number of Death Nodes with Different Broadcast Times (4000 rounds).

Cluster Head broadcast times in the cluster	1	2	3	4	5
SA-LEACH	27	42	44	46	48
Sec-LEACH	30	50	54	56	58
Percent of Less Death Nodes	3	8	10	10	10

From the simulation results, it can be seen that as the broadcast time increases from 1 to 5, the total number of death nodes of the SA-LEACH and Sec-LEACH increases with the increase of broadcast time, and no matter how the number changes in the cluster, the total number of death nodes of the SA-LEACH is smaller than the Sec-LEACH the after 4000 rounds, which further illustrates the advantage of the SA-LEACH in energy consumption.

5. Conclusions

The network security technology is an important part of the network technology. Without enough security, the network has no future.

In order to strengthen the security of the cluster-based communication protocol in wireless sensor networks, this paper introduces the SA-LEACH. In the cluster formation phase, certification for candidate cluster head broadcast messages is introduced to effectively prevent malicious nodes from becoming cluster head nodes, effectively prevent to join the cluster; introduced the authentication, and the identification certification during nodes joining clusters can prevent malicious nodes from joining clusters. In the stable phase, the certification mechanism for cluster head broadcast messages of each member node in the clusters is introduced to stop attackers from broadcasting bogus news to cluster members. The simulation results show that the SA-LEACH scheme balances the node load with less energy consumption and improves network security at the expense of network reasonable computational and communication cost. In the situation that the long distance from the base station to the network deployment, the SA-LEACH is much better in terms of energy consumption, it can better meet the needs of sensor network applications. Future work will be to further improve the SA-LEACH to be suitable for multiple levels of the network topology.

The future work will be how to further improve the SA-LEACH further to apply it to multilayer network topology.

Acknowledgements

This research is supported by the Fundamental Research Funds for the Central Universities No. 2010B07014.

References

[1]. Wencheng Yang, Yiying Zhang, Kee Bum Kim et al., SCAF: A Secure Cluster-Based Architecture Formation Scheme for Wireless Sensor Network, in *Proceedings of the 4th IEEE International Conference on Circuits and Systems for Communications*, 2008, pp. 843-847.

[2]. Kun Zhang, Cong Wang, Cuirong Wang, A Secure Routing Protocol for Cluster-Based Wireless Sensor Networks Using Group Key Management, in *Proceedings of the 4th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM '08)*, 2008, pp. 1-5.

[3]. A. S. Poornima, B. B. Amberker, Protocols for Secure Node-to-Cluster Head Communication in Clustered Wireless Sensor Networks, in *Proceedings of the Conference on Contemporary Computing Second International (IC3'09)*, Noida, India, August 17-19, 2009, pp. 434-444.

[4]. A. C. Ferreira, M. A. Vilac, A. L. B. Oliveira, E. Habib, H. C. Wong, and A. A. F. Loureiro, On the security of cluster-based communication protocols for wireless sensor networks, in *Proceedings of the 4th IEEE International Conference on Networking (ICN'05),* Vol. 3420, 2005, pp. 449–458.

[5]. Leonardo B. Oliveira, Hao C. Wong, M. Bern, Ricardo Dahab, A. A. F. Loureiro, Sec-LEACH - A Random Key Distribution Solution for Securing Clustered Sensor Networks, in *Proceedings of the Conference on 5th IEEE International Symposium on Network Computing and Applications (NCA'06),* 2006, pp. 145–154.

[6]. Sajid Hussain, Firdous Kausar, Ashraf Masood, An Efficient Key Distribution Scheme for Heterogeneous Sensor Networks. in *Proceedings of the Conference on International Conference on Wireless Communications and Mobile Computing,* pp. 388-392.

[7]. J. Deng, R. Han, S. Mishra, Security Support for In-Network Processing in Wireless Sensor Networks, in *Proceedings of the Conference on 1st ACM Workshop on Security of Ad Hoc and Sensor Networks*, October 2003.

[8]. H. Chan and A. Perrig, PIKE: Peer Intermediaries for Key Establishment in Sensor Networks in *Proceedings of the 24th IEEE Annual Joint Conference on Computer and Communications Societies*, Mar. 2005.

[9]. Elson J., Time Synchronization Services for Wireless Sensor Networks. Dissertation Proposal, Dept of Computer Science, *University of California,* Los Angeles, April 2001.

[10]. Ganeriwal S, Kumar R, Srivastava M. B., Timing-Sync Protocol for Sensor Networks, in *Proceedings of the 1st Int'l Conference on Embedded Networked Sensor Systems (SenSys'03),* November, 2003, pp. 138-149.

[11]. Van Greunen J., Rabaey J., Lightweight Time Synchronization for Sensor Networks, in *Proceedings of the 2nd ACM Int'l Conference Wireless Sensor Networks and Applications (WSNA'03)*, 2003, pp. 11-19.

[12]. Carl Hartung, James Balasalle, Richard Han, Node Compromise in Sensor Networks: The Need for Secure Systems, Technical Report CU-CS-990-05, *Dept of Comp Sci, Univ of Colorado at Boulder,* January 2005.

[13]. Vijay Bhuse, Ajay Gupta. Anomaly Ontrusion Detection in Wireless Sensor Networks, *Journal of High Speed Networks*, Vol. 15, January 2006, pp. 33- 51.

[14]. Misra, S. Abraham, K. I. Obaidat, M. S. Venkata Krishna, P. Intrusion Detection in Wireless Sensor Networks: The S-Model Learning Automata Approach, in *Proceedings of the IEEE International Conference on Wireless and Mobile Computing*, 1 2-14 October 2008, pp. 603-607.

[15]. SaniKommu Madhavi, An Intrusion Detection System in Mobile AdHoc Networks, in *Proceedings of the International Conference on Information Security and Assurance,* 2008, pp. 7-14.

[16]. Xiaofang Li, Lizhong Xu, Huibin Wang, Jie Song and Simon X. Yang, A Differential Evolution-Based Routing Algorithm for Environmental Monitoring Wireless Sensor Network, *An International Journal of Sensors*, 2010, Vol. 10, Issue 6, pp. 5425-5442.