Key management schemes using routing information frames in secure wireless sensor networks

V A Kamaev¹, A G Finogeev², A A Finogeev², D S Parygin¹

¹ Volgograd State Technical University, 28, Lenina Ave., Volgograd, 400131, Russia
² Penza State University, 40, Krasnaya Str., Penza, 440026, Russia

E-mail: kamaev@unix.cad.vstu.ru, alexeyf@unigeev@gmail.com

Abstract. The article considers the problems and objectives of key management for data encryption in wireless sensor networks (WSN) of SCADA systems. The structure of the key information in the ZigBee network and methods of keys obtaining are discussed. The use of a hybrid key management schemes is most suitable for WSN. The session symmetric key is used to encrypt the sensor data, asymmetric keys are used to encrypt the session key transmitted from the routing information. Three algorithms of hybrid key management using routing information frames determined by routing methods and the WSN topology are presented.

1. Introduction

The protection of corporate information systems from security threats is the basis for the implementation of any IT project, including Supervisory Control And Data Acquisition (SCADA) systems [1]. SCADA systems use wired or wireless sensor networks (WSN) as a transport medium for collecting telemetry data and sending commands to actuators [2]. Most such systems are not directly connected to the Internet, but they are connected to industrial business and information systems, to the communication maintenance manufacturers and consultants from the external networks. The uses physical isolation of the critical SCADA system will be at risk of need to receive information from the outside world. The introduction of such measures generates new ways of information security violations, which are more difficult to manage [3]. For example, the Stuxnet virus passed through APCS firewalls using indirect ways, such as USB keys and CDs, or via protocols that firewalls were configured to miss. Therefore, the purpose of the security of SCADA systems is to implement architecture that increases resistance the sensor network, communications, devices and dataframes [4].

The current trend of building a transport network for SCADA systems data acquisition determines the use of wireless self-organizing networks with features of the equality of nodes, dynamically changing topology, self-repair after failures, etc. The ZigBee technology provides a good basis for the construction of reliable WSN for data collection [5]. WSN are gradually replacing the wired network and are used in industry for control of technological equipment [6], in the housing sector to control the heat supply [7], lighting, air-conditioning and ventilation [8], to commercial account of energy and water consumption, in the fire security systems, home automation systems, medical monitoring, etc.

For the protection from other types of impacts, experts use hardware and software methods for a multi-layer protective model for the components of the SCADA system and security information interaction with public wireless data transmission. The task of ensuring the sensor networks security is shifted to prevent data leaks from the system [9], intrusion detection and attack [10], etc.
2. Key management for data encryption in the WSN SCADA systems

Modern cryptographic data protection is based on the encryption using a symmetric key or an asymmetric private/public key. Special codes are used for authentication of the elements of the SCADA system and nodes of the sensor network, the hash functions are used to control the integrity of transmitted data. In any complex information system, there is a lot of secret information that requires protection against compromising that leads to the implementation of key management systems.

If cryptographic algorithms to protect information are developed well enough, the procedures for secure creation, keys use and management are problematic tasks. There are two problems:

- How to generate keys with the necessary cryptographic properties?
- How to send the keys safely to the participants of the information interaction in WSN?

The complexity of key management in wireless sensor networks is determined by the absence of any fixed routes data due to self-organization, spontaneous connections during routing and random nature of information interactions. The main objective of key management is to provide participants of information interaction with key data in wireless sensor networks for implementing the confidential exchange of information via a secure communication channel. The key-management procedures that should be implemented in the control system are as follows:

1. Registration of network nodes as the interaction participants.
2. Synthesis of cryptographically strong keys.
3. Transmission and distribution of keys between nodes of a WSN of the SCADA system.
4. Managing connections between the exchange participants and the keys.
5. Keys replacement.
6. Key recovery in case of accidental destruction.
7. The planned or compromised destruction of the keys.

3. The extended keys structure of the WSN ZigBee technology

The confidentiality mechanism in the WSN ZigBee specification is the encryption and protection of key data when establishing a trust between interacting partners, both at the stage of installation of keys and data transfer process [11]. The security framework is governed by the IEEE 802.15.4 standard, where security is provided by means of special profiles. Specification ZigBee Pro Feature Set supports data encryption, determines changes in the keys distribution and encryption. An additional encryption protocol can be used at the application level when exchanging data cannot be decrypted by any other node in the network, despite the fact that they all have a common network key.

The security system is based in accordance with the ZigBee specification on the AES symmetric encryption algorithm with 128-bit keys, which may be associated with the network (network key – NK) or channel (link key – LK). The key synthesis is based on the use of the master key (MK), which controls their compliance. The initial master key must be obtained through a secure environment.

The control centre keys to which other nodes trust the distribution of keys is assigned to the ZigBee network. Each node in the network must be pre-loaded with the address of the control center keys to get the NK and session keys for the LK connection. During configuration or reconfiguration of the network, the center control key enables/disables the connection for new devices, i.e. working with access control lists (ACLs). Typically, the control center also serves as the coordinator of the WSN, but it may be associated with the server. In the WSN ZigBee standard uses three types of keys:

1. The master key, which is used as an original shared secret code between two nodes in the procedure of generating the session link key.
2. The network key (NK) provides security at the network layer and each node of the network has its own one. These keys are used when disconnecting and re-connecting nodes to the network. The center may periodically update the network key, and broadcast to all nodes in the new key.
3. Session LKs provide a secure unicast transmission of frames between nodes at the app level.

As the ZigBee security is based on symmetric keys, the sender and the recipient of the data frame must have the same shared key. There are three methods of transfer switches for the participants of the information exchange: (i) pre-installation, (ii) transmission from the centre of keys management, (iii)
the synthesis of keys by the participants of the interaction. In case of pre-setting, the keys are placed in
the nodes or PLC in advance in the process of firmware of the device. In the second case, the centre
of key management sends the keys to the devices. In the third case, one of the participants generates its
own keys before information exchange and sends it to the partner. Using the symmetric exchange, the
participants are sent the same key (shared key) to encrypt/decrypt that causes the following problems:

- the need for secure transmission of keys to each subscriber via a secret or secure channel;
- the complexity of key management, which means the quadratic growth of the number of keys
  that are to generate, transmit, store and destroy for each pair of nodes in the sensor network.

To solve these problems, an asymmetric encryption scheme with public key is used in network
systems. The use of asymmetric algorithms eliminates the problem of key distribution in the system,
but raises the problem of validating the received keys and their source authentication, especially in
wireless networks. The technology of an electronic digital signature is used when the message
previously is subjected to the hash, using the private key, and the other party, using the public key, can
verify the authenticity of the recipient signature. Such a scheme of joint application of asymmetric
encryption is used in the RSA cryptosystem, where the sender is first added to the message's digital
signature.

Although this method solves the problem of symmetric schemes associated with the initial transfer
of the key to the other party, such systems are demanding in the length of the keys, computing
resources and the performance of the whole network, which does not allow it to be applied in sensor
networks. Therefore, the hybrid encryption system for the use in WSN is of greater interest, as it
combines the advantages of an asymmetric system with the performance of symmetric cryptosystems.
The key structure used in the ZigBee standard, should be supplemented by a special type of key
(asymmetric key – AK), which will be used to encrypt a symmetric session key connection (figure 1).

The MK, NKs and special AK keys are long term and session keys have typically a short lifespan.

4. Key management protocols in WSN

In SCADA systems with a small number of monitoring objects WSN with centralized control is the
most common network, which has a topological structure of the "star" or "cluster tree." This network
uses a coordinator associated with the server, where it is logical to install the key management system.

The task of key management is more complicated in networks with a large number of controlled
objects. Such networks include full or partially decentralized structures where multiple coordinators
are responsible for separate areas of monitoring and interact with each other through routers. To
provide secure information interoperability of sensor nodes, industrial controllers and a zone
coordinator, there are tasks of ensuring secure communications between coordinators and routers.

Key management protocols can be divided into three groups: protocols of pre-placement keys;
arbitration protocols with a third trusted party; autonomous protocols. Protocols of pre-placement keys
can reduce the service traffic in a sensor network, since the keys are placed in the firmware in advance
when configuring sensor nodes. In arbitration protocols, the third-trusted party is used for generating,
distributing, installing and maintaining the keys, established by the coordinator or the associated
server. In the process of information exchange, the third-trusted party plays some roles (see figure 2).
The key controlling system generates, stores and distributes keys, produces accounting, network
addressing and configuration of sensor nodes, and is responsible for their authorization.

The autonomous protocols work on the scheme of a self-distribution pair of identical keys between
communicating parties. In the first case, the disadvantages are the keys transmission to other party via
an wireless communication channel. In the second case, the drawback is the computational
complexity of the algorithms of generating the keys pair, the encryption/decryption complexity and the
need for a key generation node authentication that leads to additional time and energy of sensor nodes.
Therefore, the system of a hybrid encryption is the most effective one, where pairs of asymmetric keys are used to encrypt the symmetric key before passing it to the interaction participants with the transmission initiator authentication by signature. But it does not exclude the growth of routing traffic.

5. Hybrid key management in the WSN ZigBee technology

In traditional wireless networks, the problem of data protection is ensured by the services at the program level. Sensor networks do not differ from other types of wireless networks in terms of security. They are vulnerable to passive listening attacks and active falsification attacks, as the wireless network is available to the public. Limited energy, computational power and memory nodes are not capable of providing powerful data protection. These restrictions narrow the use of cryptographic mechanisms and protocols at the data link and physical layers of the network model that requires the implementation of an architectural component security at the network and application levels.

6. Autonomous hybrid key management with dynamic routing

Reactive dynamic routing protocol Ad hoc On Demand Distance Vector (AODV) is used in mesh topology sensor networks and sets a route from the source to the destination by broadcasting queries [12]. When one of the touch nodes is going to send data, it sends a broadcast request to create a route (Route Requests – RREQ). The WSN routers broadcast frame relay and make an entry for the node in their routing table. "Logical distance" from the requester to the current position is also written in the frame. The recipient will receive some RREQ frames with different "logical distances" and sends a reply (Route Reply – RREP) to the device, from which the package with a minimum "logical distance" came. RREP is transmitted on the shortest chain until the source. Thus, the response is returned to the optimal path, and generates a vector of the direct route for the frame transmission. If the connection is unreliable, then the node may send a receipt confirmation of a route to the destination (RREP-ACK).

The key-management procedures should be integrated into the routing protocol to reduce the service traffic. It needs to add the appropriate fields in the route frames RREQ and RREP to write the keys and hash functions in them. The encryption and authentication methodology will be as follows:

1. The sender generates a random session key, which encrypts and prepares the data frame to send.
2. The sender sends a broadcast request to create the RREQ route and obtain the public key from the recipient to encrypt the session key.
3. The receiver generates a random pair "public key-private key" for the RSA algorithm and sends the public key to the sender together with the RREP route reply. To authenticate the receiver, the hash of the frame with the public key is computed, encrypted by a key known to both parties.
4. The sender encrypts the session key with the public key and sends it to the recipient along with the encrypted session data frame key. To authenticate the sender and verify the data in the frame, the...
hash function of the encrypted frame is computed, which is passed along or together with the frame data, or together with a confirmation receipt of the RREP-ACK route with a bad link quality.

5. The recipient decrypts the session key and the hash function, checks the authenticity of the sender and the integrity of the encrypted frame. Further, he decodes the frame data and deletes the key.

7. The arbitration scheme of hybrid key management in the hierarchical routing process

Another routing method of cluster topology in ZigBee networks is hierarchical routing. When building a cluster tree of the ZigBee network [13], the coordinator, and then the attached routers assign address ranges to child devices in a hierarchical manner. Each node can determine whether the recipient address of the data frame belongs to its "child" branches or is in the other part of the network.

In such sensor network topology and method for hierarchical routing, it is advisable to use the arbitration key management protocol, where on a network coordinator or a related server of the SCADA system, the role of the trusted certification center in a hybrid encryption is implemented. The arbitration method of a hybrid key management for the transmitted data encryption will be as follows:

1. The joined nodes to sensor networks receive addresses for the branches of the cluster tree from the coordinator or the router in accordance with the ranges.

2. Each newly joining node generates a random pair "public key-private key" by the RSA algorithm and sends frames with the public key, the address and the calculated hash as a digital signature the center key management that records the public keys and digital signatures sensor nodes.

3. The source sends a request to the key management center for the generating of the session key for the symmetric data encryption and the frame receiver address for the same key transfer.

4. The management centre authenticates the source, generates a session connection key, finds the public keys of the source and destination in the keys database, encrypts the session key with.

5. The encrypted session key is sent to the source and destination, where the authenticity of the key management center is also verified and the session key is decrypted using the stored private key.

6. The source encrypts the frame using the session key, destroys the key and sends the frame to the recipient who decrypts it with the same key and then destroys it.

8. The arbitration scheme of the hybrid key management in the WSN Many-to-One routing

The third type of routing in the ZigBee network takes into account the specificity of information flows, which are transmitted from a plurality of end nodes to one or more coordinators. This type of routing is called Many-to-One Routing. When using this mechanism, the central coordinator periodically sends a broadcast request (SINK_ADVERTISE) to all nodes. When the node receives the SINK_ADVERTISE request, it sends the Route Record frame back and waits for a receipt confirming the route. Thus, the coordinator receives the full information about the route to the source node and uses it to send a receipt confirmation of the route and the subsequent receipt of a data frame. With the receipt, the coordinator can send any additional information to the node.

The technique for the encryption of data frames and the sender authentication is as follows:

1. The central coordinator sends the SINK_ADVERTISE broadcast request and waits for the Route Record staff in response.

2. The sensor node receives the SINK_ADVERTISE request, generates a random pair "public key-private key" by the RSA algorithm, forms the Route Record frame adding a public key, then calculates and adds a hash function to authenticate the frame and sends the frame to the coordinator.

3. The coordinator receives the frame with the routing information, the source address, its hash function and the public key. Then it generates a session connection key and encrypts it by the received public key. Then, the coordinator adds the session key to the route supporting receipts, calculates the hash function to his authentication using the public key and sends the frame back to the source.

4. The sensor node decrypts the session key using the private key, authenticates the sender by calculating and comparing the hash function.

5. Then the frame is encrypted, using the session key, and sent to the coordinator.

6. The coordinator decrypts the received frame by the same key and destroys it.
9. Conclusion
The advantage of these approaches is the use of existing routing procedures for the simultaneous exchange of key information that allows reducing energy consumption during the information transmission. However, it is required the consumption of network nodes as well as the additional energy for the generation, storage and destruction of keys, the calculation of hash functions, etc. The size of transmitted frames with routing information also increases.

The main disadvantage of key management methods in the hybrid and asymmetric encryption is the possibility of a successful attack to spoof the public key or nodes, where the pair keys for the asymmetric encryption are generated, which leads to a compromise of the entire sensor network. The process of the asymmetric public key obtaining is vulnerable to attack, in which the attacker interferes with the interaction between the sender and the receiver, and can modify the traffic between them. Therefore, the open asymmetric key must have a digital signature to authenticate its sender. Today, there is no such system, in which it would be possible to guarantee the authenticity of the public key.

In the next step, the session key is encrypted using the asymmetric encryption algorithm and the asymmetrical public key of the recipient. The encrypted session key is attached to the frame routing which also includes the added electronic signature. The entire data packet is transmitted to the recipient via the unprotected WSN, and, of course, it is also subjected to sniffer attacks.

To solve these problems, it is possible to abandon the cryptographic encryption of session keys by high computational complexity algorithms, but instead carry out covert transfer of open or encrypted key information by the steganographic methods. Despite the fact that the cryptographic security mechanisms are a prerequisite for the security of sensor networks today, other methods also require the intensive study. The examples are steganography to hide the fact of classified information transfer, the use of the timestamps and synchronization technologies in the generation and disclosure of key information, the intrusion detection and prevention in the sensor network, etc.

Acknowledgments
The reported study was funded by RFBR according to research projects No. 16-07-00031_a, No. 15-07-01720_a, No. 16-37-50017_mol_nr, No. 15-57-54033_Vet_a and the Russian Ministry of Education in scope of the base part (project 2586 of task N 2014/16).

References
[1] Zhao G 2011 Network protocols and algorithms (Penza: PSU) 3(1) 46–63
[2] Kim HJ 2012 Int. J. of Distributed Sensor Networks (Hindawi Publishing Corp.) 8(11) pp 1–10
[3] Kravets A G, Bui N D and Al-Ashval M 2014 Communications in Computer and Information Science (Springer IPS) 466 371–382
[4] Bolshakova O N and Chusavittina G N 2016 Proc. 3d Int. Conf. on Information technologies in science, management, social services and medicine (Tomsk: TPU) pp 122–126
[5] Finogeev A G, Maslov V A, Finogeev A A and Bogatyrev V E 2011 Proc. VSTU (Actual problems of management, computer science and informatics in technical systems) (Volgograd: VSTU) 3(10) 73–81
[6] Kizim A, Matokhina A and Nesterov B 2015 Communications in Computer and Information Science (Springer IPS) 535 354–366
[7] Finogeev A G, Dilman V B, Maslov V A and Finogeev A A 2011 Applied Informatics (Moscow: Market DS) 3(33) 83–93
[8] Sokolov A, Tyukov A, Sadovnikova N, Zhuk S, Khrzhanovskaya O and Brebels A 2015 Communications in Computer and Information Science (Springer IPS) 535 462–473
[9] Banokin P I 2016 Proc. 3d Int. Conf. on Information technologies in science, management, social services and medicine (Tomsk: TPU) pp 106–109
[10] Frolov S G and Demin A U 2016 Proc. 3d Int. Conf. on Information technologies in science, management, social services and medicine (Tomsk: TPU) pp 74–76
[11] ZigBee Specification Overview http://www.zigbee.org/Specifications/ZigBee/Overview.aspx
[12] Rivest R L, Shamir A and Adleman L 1978 *Communications of the ACM* (New York, NY: ACM) **21**(2) 120–126

[13] *ZigBee cluster library specification* http://www.zigbee.org/zigbee/en/spec_download/spec_download.asp?AccessCode=1351395201