ISSN : 0974 - 7435 Volume 10 Issue 23

2014

BioTechnology

An Indian Journal

FULL PAPER

BTAIJ, 10(23), 2014 [14223-14229]

Network security encryption mechanism design based on the wireless router

Renshang Zhang*, Jun Mi
Shanxi University of Finance and Economics, Taiyuan, Shanxi, (CHINA)
E-mail: zhangrenshang@163.com

ABSTRACT

In the traditional network, cryptographic keys management technology has been highly developed in many fields including generation, updating, maintenance, management and destruction. However, the wireless router network can not use traditional network asymmetric key system, the traditional key management techniques can not apply to wireless router network either. The paper explores how to progress the cryption design based on random cryptographic keys pre-distribution model.

KEYWORDS

Encryption mechanism1; Wireless router2; SPIN agreement3.

OVERVIEW OF THE CRYPTOGRAPHIC KEYS MANAGEMENT

Encryption provides confidentiality, integrity, security and other basic services for network,and cryptographic keys management system is responsible for generating and maintaining cryptographic keys used in the encryption process. Compared with other security technology, encryption technology has been highly developed in traditional security field. But in resource-constrained wireless sensor networks, encryption algorithms faces the problem of how to accomplish the encryption operation in a very limited memory space, and how to minimize energy consumption and computation time. Facing the situation of severely limited resources, encryption algorithm which is based on public cryptographic keys is considered not suitable for being used in the wireless sensor networks[1]. The wireless sensor network is a distributed self-organization, and it is a network of no central control,and therefore third-party authentication mechanisms can not be adopted[2]. Up to now, the research of cryptographic keys management is mainly focused on encryption for symmetric cryptographic keys.

There are two cryptographic keys management scheme in the wireless sensor networks. They are single cryptographic key scheme and multi-key solutions[3]. Single cryptographic key scheme refers to all the nodes share a symmetric cryptographic key to encryption the wireless sensor networks, and it is the simplest management form of the wireless sensor network. Single cryptographic key scheme is the most efficient and most achievable in cryptographic keys management mechanisms of wireless sensor network. Moreover, the support for the basic functions of the network is also the most comprehensive. But, the disadvantages are also obvious. Once cryptographic keys compromise, the security system of the entire network will be non-existent, which is a huge threat to unguarded wireless sensor networks.

Multi-key security scheme is much better than single cryptographic key scheme. In simple terms, multi-key scheme refers to using different cryptographic keys on different nodes, and using different cryptographic keys on same node at different timing points. Compared with the single cryptographic key scheme, the multi-key scheme is more rigorous, even if individual cryptographic keys leaking out, it will not cause a devastating destroy to the security system. Although with improved security, problems follow, Multi-key scheme will sacrifice storage capacity and computing power of some sensor nodes and uses it for cryptographic keys management[4]. To reduce the effect, the location-based random cryptographic keys pre-distribution model can be applied.

Random key pre-distribution model is mainly based on the principles of probability aiming to improve the anti-trapping capacity of the entire network, and is modified by incorporating the location information. The base station will choose a very large pool of keys for the entire sensor network when using a random password key pre-distribution model for deployment. The size of key pool to some extent, determines the level of network security. After that, each sensor node needs to choose an equal number of keys randomly. Password keys owned by any two nodes have shared probability, which will be the connectivity rate PIN communication, each node firstly declares its keys, and records all nodes with whom it had shared the key. If there is a shared key between two nodes, a secure link established to communicate.

Network Security Routing Protocol

The work flow

In this paper, SPIN agreement is used as a basis for routing protocols. By analyzing and improving it, the wireless router network security routing protocol is made. Basic work flow of SPIN works as follows:

In a SPIN protocol-based network, each node has a unique address, and each node also save the address information for neighboring nodes. When sending out data, according to the recipient and address information, each node selects Address from their store address table as the destination address.

Wireless sensor networks is more complicated. It is determined by a number of sensors. However, all of its mode of operation are almost the same as the sensor nodes, and SPIN protocol mode is the single-hop route. Therefore, the use of a relatively simple model in the relationship between nodes can be represented in the working relationship between nodes. The working process is shown in 1, and a specific network node relationship shown in Figure 2:

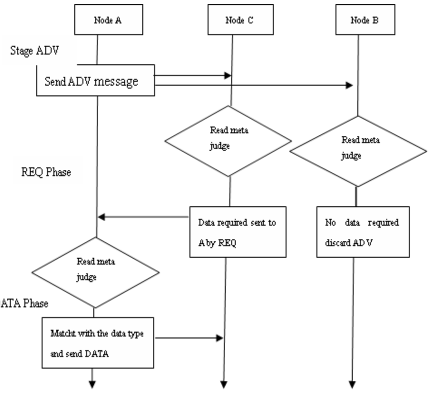


Figure 1 : The workflow of SPIN protocol

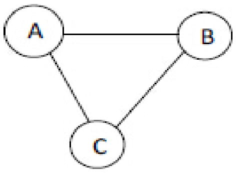


Figure 2 : The nodes' relationship of SPIN

Sensor node A gets the data, sends it out, B and C are neighboring node of A.

A sends out a broadcast of ADV.

B and C receive ADV message and determines whether to accept according to the message type.

Discard ADV if it is not required by B. If C needs, then send REQ message out.

A node receives REQ message sent by C, then send DATA message out.

The message format may be expressed as:

ADV (ADV, Address, meta)

REQ (REQ, Address, meta)

DATA (DATA, Address, meta, data)

ADV, REQ, DATA represent message indication code, determines the message type;meta represents meta data, though wich determines whether meta data is needed; Address indicates the target address; data indicates that the data deeded to be sent by node.

Security analysis

The SPIN protocol is a wireless sensor networks routing protocol of high performance. The characteristics of data centric accord with the requirements of the work of sensor networks. Although SPIN protocol is widely used, SPIN protocol does not take into account the network security problem, which will be analyzed in this paper.

(1) Potential safety hazard concerning the confidentiality

The SPIN routing transmits information through broadcast, and the data is sent to the target node after two handshake. But the node information in the network is not encrypted, and the whole network information depends on the plaintext transmission. Once node is compromised, the information in the whole network will be intercepted,which makes SPIN protocol is the biggest potential safety hazard. In addition, the nodes lack of identity authentication mechanism in the network, so they cannot guarantee the authenticity of sources.

(2) Communication security risk

As the SPIN routing is a communication method using active sending form rather than passive query form, the malicious nodes often blocking the channel, interfere with the normal communication and consume the energy of the node by sending out frequent mass data packet, such as flooding attack, denial of service attack etc. In addition, the selective forwarding attacks in wireless sensor networks are a relatively difficult to guard against attacks.

(3) Hidden threats of the energy consumption

The SPIN protocol transfers messages through the path length to determine routing. It is the routing selective method that makes a message delivery task excessively focused on the part of the nodes, which make the energy consumption intensify. With the features of slightly longer path and further distance, the sensor node has sufficient energy. But because of the far distance, the sensor node is failed to support more work, with almost no loss of the energy. In addition, because there is no energy control mechanism, the whole network almost has no prevention ability against the attack technique aimed at node energy. Once the node energy is exhausted, the entire network function will suffer loss and even paralyzed.

These security risks that make SPIN protocol's normal operation in the network has been seriously threatened,if these security risks can not be eliminated, the wireless sensor networks which works in the SPIN protocols can not reliably complete the task.

Analysis

SPIN protocol based on consultating delivery sends data down until they reache the sink node. But two biggest issues in the SPIN protocol make the application a huge flaw.

Firstly, the"date blind spot"problem can't be solved,which means date can not be sent down when neighboring nodes are not interested in the data. Taking Figure 5 for example,when A has only and has B,C, two neighboring nodes, A can only send messages to B,or C. However,if B and C are not interested in the message obtained by A,so B and C will not feedback on the message of A. Then A can not sent out the data which forms a blind data spot is.

Besides, message repeating. is also a problem. Since SPIN uses the way of the interest negotiation to transmit, but don't take into account the problem of the flow of the node transmitting the date, thereby, a large amount of date message is repeatedly transmitted. Still use Figure 5 as an example, when node A sends data to node C,C sends data to outside, the ADV message that C send will still be sent to A and shared neighboring nodes of A and C, which causes unnecessary wasting of energy and network resources.

THE DESIGN OF ENCRYPTION MECHANISM MODULE

Encryption mechanism module is a fundamental part of the whole security mechanism, and is divided into four parts, respectively the key distribution, identification distribution, process of key negotiation, and process of encryption. Among them, key distribution and identification distribution are completed by the coordination of node and base station when the network is formed, while key negotiation and the encryption process are completed by the mutual coordination when node is working, the process shown in Figure 3.

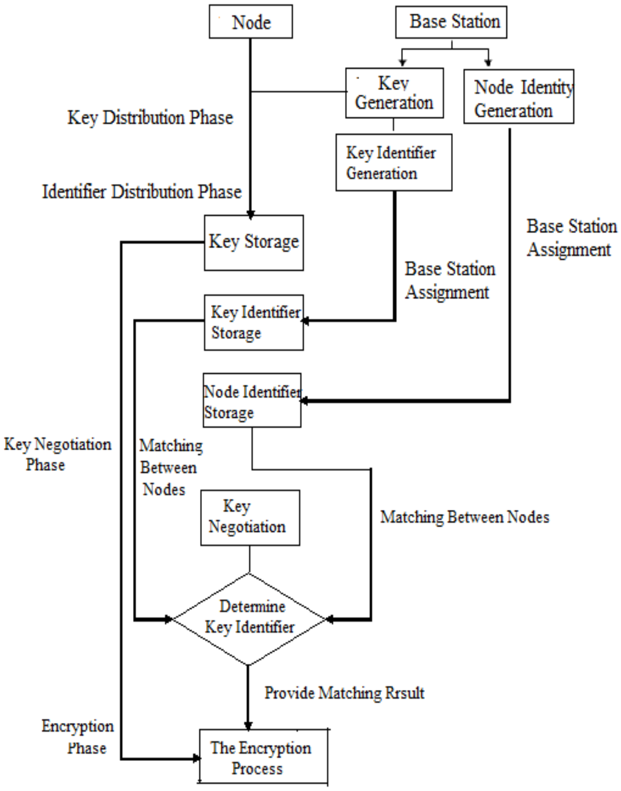


Figure 3 : Encryption process

Key distribution mechanism

Trust management based R-SPIN security router locating-based selects random key pre distribution model to carry out key distribution. Because the computing power of wireless sensor network node is limited, the whole process of key generation needs to be finished at the base station. After the deployment of wireless sensor networks, the formation of node neighbor relationship, base station starts the key distribution process. The formation of the node neighbor relationship between nodes is based on the mutual distance relation, which will not be discussed a lot.

Key distribution is done at the base station. Firstly, the base station generates a large key pool for the entire network. After the large key pool generation is completed, the nodes in the network will select some equal number key randomly from the key pool to form sub key pool independently, and ensures the probability of shared keys between neighboring nodes is not less than P, the formula is as (3).

$$P = \frac{c_s^i c_{s-i}^{2(k-i)} c_{2(k-i)}^{k-i}}{(c_s^k)^2} \quad \textbf{(1)}$$

Where, S, key pool size formed by base station, I, the number of nodes between the shared keys, K,key number selected by nodes except for the number of shared key. P is the key to ensure the network security. The higher the P, the more number of shared keys between nodes, the metter the connectivity of the network. But it relatively means S of key pool reduces, and the worse its security becomes. Vice versa, the node selects the key, it will store the selected keys in local, preparing for the encryption use in the process of communication.

Identifing distribution mechanism

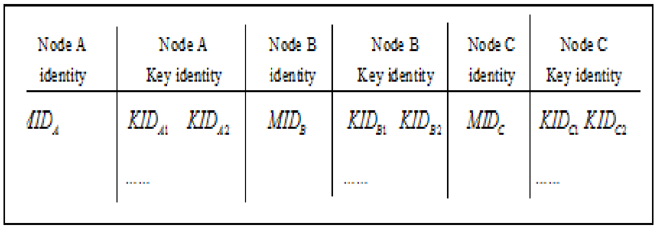
Identifying distribution can be divided into key identifier KID and node identity MID. The following will make a concrete analysis to the two kinds identification distribution and they effects.

(1) definition and role of key identification KID

After the base station generates the key, it will assign a key identification number for each key, called KID. This KID number, as the key in the network identification, is unique and can not be changed after assignment. In order to ensure key’s secret characteristic, in the entire network, when needing to negotiate key, key is matched through the KID number.

After the node selects the key, the key will be stored in local, and announce the selection KID number of key. At the same time, it accepts KID sent by other nodes. When the node receives the adjacent node sent by KID number, it will generate an adjacent key identification table in local. Take the relationship between nodes in the 2 graph as an example, it will be shown in TABLE 1 that the neighboring key identification table generated by node.

TABLE 1 : The neighbor key identification table of node A



Node A identity	Node A Key identity	Node B identity	Node B Key identity	Node C identity	Node C Key identity
MID_A	KID_{A1} KID_{A2}	MID_B	KID_{B1} KID_{B2}	MID_C	KID_{C1} KID_{C2}
	……		……		……

When a node needs to negotiate keys with other nodes, it needs to select KID number which need to negotiate shared key nodes from neighbor key identifier table of their own storage, and sends it to the node, to complete the key negotiation process.

(2) The definition and function of node identifier MID

In the wireless sensor network, as we couldn’t use the asymmetric key mechanism, it cannot achieve the node identity authentication to the asymmetric key mechanism. So here we use the unique node identifier to identify the node identity to ensure security.

In the network deployment process, the base station allocates a node number for each node, called the MID. This KID number, as the node in the network identification, is unique and can not be changed after assignment. When the nodes are deployed, the neighbor relationship is determined, nodes can release their MID to the neighbor nodes, at the same time accept the MID information sent by other neighbor nodes. When the node receives the MID signal, it will generate a neighboring relation table in local, recording all the adjacent MID number, as shown in Figure 4.

The KID number, as the node in the network identification, is unique and can not be changed after assignment. When the network’s deployment completed, the nodes between the neighbor nodes can record MID number of the other side. When they transfer information between nodes, the nodes judge the source from data sent by MID. MID, because it can not change, can prevent from the nodes in the network deliberately falsifying of MID for disguising to other nodes. Once the malicious nodes try to pretend to be other identity and modify MID, while at this time the neighbor nodes don’t store disguised MID. Then the neighbor nodes may reduce its trust evaluation to the source node because MID is abnormal, in order to guarantee the security.

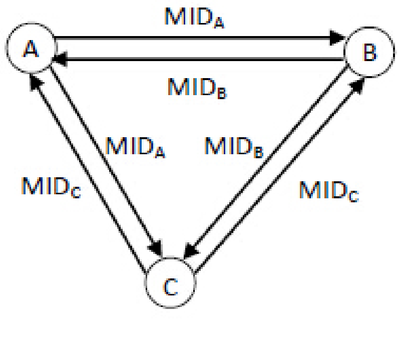


Figure 4 : The node's MID announced sketch map

The key negotiation process

R-SPIN security router based on trust management use encryption mechanism in the communication process, to prevent information from being leaked out during transmission. Take node relationship of Figure 2 for as an example to explain key negotiation process, when a node needs to communicate A with C, key negotiation process is as follows:

Firstly, node A and C need to establish communication relation, and has reached agreements to transmit encrypted data, which is the premise of two nodes need to negotiate key. If no agreement between two nodes achieved, key negotiation can’t work.

It needs to have key negotiation after node A and C establish communication. As one party needs to get the data, node C firstly needs to query his neighbor key identification table. When querying key identification table, key identifier KID need to find their own and key identifier KID stored by A. If a same KID is found to exist, we should randomly select a key identification applicated for A, and send the KID to A. When node A receivs the KID, A will compare it with key identifier stored for its own, and if a matched key is found, key negotiation is successful, and the process of key matching is finished. Then with this identified KID key to encrypt, is completed the transfer process, as shown in Figure 3-3.

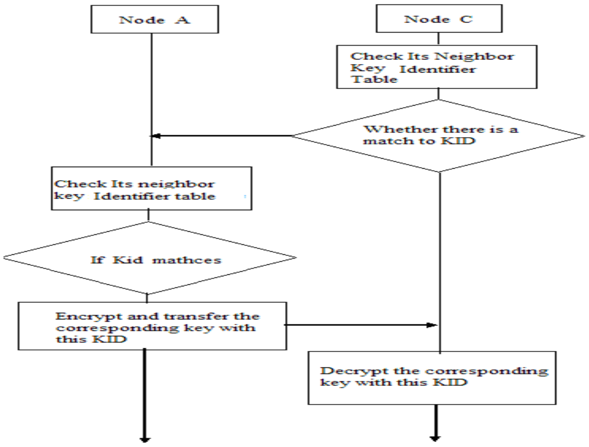

Node A
Node C
Check Its Neighbor Key Identifier Table
Whether there is a match to KID
Check Its neighbor key Identifier table
If Kid mathces
Encrypt and transfer the corresponding key with this KID
Decrypt the corresponding key with this KID

Figure 5 : Agreement process of key

The encryption process

Since the complex encryption algorithm is not available, so here we selected RC5 encryption algorithm. In this paper, the process of RC5 algorithm omitted the process that key is formed into key group, and we use "key" to represent the actual calculation process.

Firstly, the encryption process will divide plaintext block into A, B two groups. Then we use the operation result of group A or group B, again as the second discrepancy. For irregular digit, it will be padded with 0. Among them,+ represents encryption operations, and- represents the decryption operation, ⊕represents the XOR, < < < represents left circle, > > >represents cyclic shifts, one round of encryption and decryption process as shown in Figure 6.

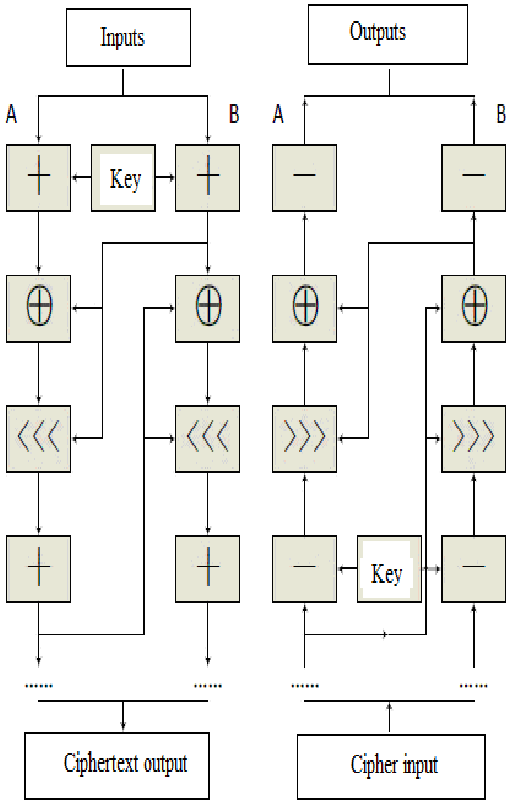


Figure 6 : One encryption and one decryption

For the key it can choose 16 bit, 32 bit or 64 bit. Choosing a different digit key means that consumption of energy consumption and storage requirements are different.

RC5 is a encryption algorithm with variable key numbers and variable numbers of rounds of encryption. The encryption key number and number of is proportional to rounds safety performance. In order to ensure the confidentiality in condition of sufficient energy and ensure the node lifetime requirements when lack of energy, we use two kinds of encryption round number set. When the node energy is sufficient, encryption round number can perform more than 10 rounds. When the node energy consumption is too high, the encryption round will implement 6 rounds.

According to the analysis of the security of RC5 algorithm, after the encryption round has implemented 6 rounds, it can guarantee that certain safety. It can also ensure that the network has a degree of confidentiality when the energy consumption is too high.

In short, the design of encryption mechanism mainly solves the problem of plaintext transmission by wireless router network. By designing the model of random key pre distribution based on position and unique identification, it can ensure the confidentiality of node transmission and the authenticity of node identity. In order to solve the problem of network security, we need the trust mechanism and the state judge technology. All these technologies need to be further explored.

REFERENCES

[1] Gan Guo; Packet aggregation method in wireless sensor networks, Journal of chongqing university of posts and telecommunications (Natural Science), **18(03)**, 402-405 **(2006)**.

[2] Wang Zhen; Security issues and challenges in wireless sensor networks, Computer CD software and application, **13(13)**, 150 **(2012)**.

[3] Zhao Haixia; The study of secure routing in wireless sensor networks, National University of Defense Technology, **(2013)**.

[4] Li Quanquan, Li Chenghai, Li Bingbing, Zhao Yongjun; Research on wireless sensor network and its military application, Winged Missiles Journa, **9(09)**, 76-80 **(2012)**.

[5] Sun Yuyan, Liu Zhuohua, Li Qiang, Sun Limin; A security framework for internet of things based on 3G access, Journal of Computer Research and Development, **47(l)**, 327-332 **(2010)**.

[6] Yang Ruiqiang, Zhang Fusheng, Hu Yongzhi; Attack and defense of the network layer in wireless sensor network, Wu Xian Hu Lian Ke Ji, **3(03)**, 6-7 **(2013)**.

[7] Jing Haixia, Hu Xiangdong; Analysis on security problems of routing protocols in wireless sensor networks, Ordnance Industry Automation, **26(07)**, 33-35 **(2007)**.

[8] LvYuanfan; Research on key management mechanismin wireless sensor, Hunan University, **(2010)**.

[9] Jing Haixia, Hu Xiangdong; A location-based key management scheme for wireless sensor networks, Communications Technology, **40(11)**, 311-313 **(2007)**.

[10] Xu Chen, Cao Lei, Zhang Guo-An, Gu Jinyuan; Overview of multiple sink routing protocols in wireless sensor network, Application Research of Computers, **27(03)**, 816-823 **(2010)**.

[11] Q.Xue, A.Ganz; Runtime security composition for sensor networks, Vehicular Technology Conference,VTC 2003-Fall, 2003 IEEE 58th, **5**, 2976-2980 **(2003)**.

[12] D.Sanchez, H.Baldus; A deterministic pairwise key pre-distribution scheme for mobile sensor networks, Proc.Of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks, 277-288 **(2005)**.