A BALANCED SECURITY PROTOCOL OF WIRELESS SENSOR NETWORK FOR SMART HOME

Yuanbo Xu[1], Yu Jiang[1], Chengquan Hu[1], Hui Chen[2], Lili He[1], Yinghui Cao[1]*
1. College of Computer Science and Technology, Jilin University, Changchun 130012, China
2. Meteorological Information and Network Center of Jilin Province, Changchun 130062, China
jiangyu2011@jlu.edu.cn

ABSTRACT

The Smart Home is based on the Wireless Sensor Network (WSN) and Embedded System (ES). The most important parts of the Smart Home are low-power and high-security. And it is very vulnerable to various attacks ether an active or passive one in WSN. We shed light upon some existing security flaws in W2 and ZigBee. Some are quite useful to defend the various attacks, but don't suit for the Smart Home. We propose that a new balanced security WZ-lcp protocol which can achieve our requirements. First, in every facility we store two int which can be used as the keys for the authentication, and also can be changed with the time. Second, we do time synchronization to update keys. Finally the proposed scheme achieves balanced and security without costing power-wasting and data collision.

Index Terms--Smart Home, WZ-lcp, Authentication, W2

1. INTRODUCTION

In the era of information technology, the elderly and disabled can be monitored with numerous intelligent devices. Sensors can be implanted into their home for continuous mobility assistance and non-obtrusive disease prevention. Modern sensor-embedded houses, or smart houses, cannot only assist people with reduced physical functions but help resolve the social isolation they face [1] In China, electronics giants are selling various kinds of smart home appliances and have also joined hands to create standards for linking networked home appliances. While there is a huge potential market for such appliances, both in China and around the world, there are serious security challenges that have to be addressed in order to realize their true benefits [2].

There are various kinds of attacks in Smart Home Environment (SHE). We have studied the security of ZigBee and W2 scheme in RFID, which are most applied for SHE. Using the benefits both they own, we propose a new balanced delegation protocol—WZ-lcp.

* Corresponding Author

2. PRELIMINARY AND RELATED WORK

1.1. Security in RFID and ZigBee

In RFID, there are some useful protocol to defend the attacks and ensure the security of the users. The most famous protocol is named W2. In [3], Sharaf pointed out these flaws and later modified the W0 scheme by applying the TCP/IP three-way handshake protocol [4] in the secret update and session termination. It is useful to introduce a counter in the delegated readers. Such a delegated mechanism will be effective in ensuring controlled delegation and scalability property. At the opposite of this mechanism, the proposal [5] has the advantage of supporting controlled delegation without needing a counter on the tag's side. Fernndez-Mir et al.propose the RFID protocol that not only achieves controlled delegation but also improves the system scalability [6].W2 scheme is proved to have effect on the security. But in W2, before a facility join in the network, an authentication is necessary. This will waste 3 times transmission in SHE, the possibility for a facility to join or rejoin in is so large. So the bandwidth and power-saving are the main problem for the W2.

In ZigBee Standard [7], because of the different purposes, the protocol is mostly used for industrial, aerospace, monitoring. There is nearly no special protocol for ZigBee to defend the attacks. If having a facility that meets the ZigBee Standard, an adversary can join any ZigBee Standard Networks (of course the band should be known by the facility, but it is quite easy for an experienced adversary). Also the adversary can do some active attacks easily.

1.2. Related work

Many researches have been conducted to provide a scheme for WSN. The goal is to achieve the requirement that defend the Active Attack and the Passive Attack, which are described as follows:

(a) The Active Attack

An adversary uses the sniffer to catch the frames transformed in SHE. Then try to explain the useful information to make the security of the whole protocol means nothing to the adversary. With these information, the adversary can make a new facility in SHE, easily join the networks and get the more information they need and do some attacks such as Dos attack.

(b) The Passive Attack

978-1-4799-2186-7/14/$31.00 ©2014 IEEE

An adversary just catch the frames, do not use any explanation just transfer the same frames in a huge number. This kind of attack can make the congestion of network. As we all know, the gateway in SHE do not have the powerful computing capabilities. The passive attack may cause the death of the whole system.

In one word, the Active Attack is to get the meaning of the frame in SHE, use the information that maybe have the owner's secret. And the Passive Attack is just trying everything to damage your system. Both two kinds of attack cause huge threat to WSN.

3. THE PROPOSED PROTOCOL

Based on the W2 and ZigBee security protocol, we propose a new security protocol, WZ-lcp(W2-ZigBee Low Cost Protocol)which has the ability of W2 to defend our networks in WSN and also owns the network mechanisms same as ZigBee [8].

Firstly, let's describe the SHE in our WZ-lcp for WSN: This SHE has a gateway and many facilities, every facility (include the gateway) has a network address with the length of 1 bytes. And every facility has limited calculation and storage. In the gateway, there is a facility table to record the network address of every facility in the networks. Once a facility want to join in the networks, it should be authenticated by the gateway. Even if the facility is linking to another facility, the authentication should be sent to the gateway and make the gateway decide whether the facility should join in SHE. We assume the gateway is absolutely safe.

The WZ-lcp is depicted as follows:

3.1. Facility Authentication

Initialization:

Every facility (include the gateway) should save int a, int b, and the gateway's network address (GNA), and has two different Pseudo-Random Function $PRF_1(x)$ and $PRF_2(x)$. a, b is from 0 to 255, and the $PRF_1(x)$ and $PRF_2(x)$ has the same range both for its input and output. The facility can get the a, b, GNA, PRF_1 and PRF_2 from the gateway (using Dimensional Code Scanning in our SHE) or from the DateBase (do not recommend because of the timeliness of the keys).

Authentication:

After the initialization, once the facility want to join in the network, it should broadcast a frame named Request-Join-Frame (RJF) with the information that the network needs (Such as ZigBee, BlueTooth,). The WZ-lcp uses a, b and GNA to encrypt the entire frame. The encryption is described as follows:

Step1:

The facility gets a, b and GNA, uses a XOR GNA, which we name GNA_1. Then use b XOR GNA_1, which we name GNA_2.

Step2:

The facility uses the random byte to fill the all frame to make sure different kinds of frames has the same length.

Step3:

The facility uses GNA_1, GNA_2 to encrypt the whole frame. In our design, WZ-lcp uses the XOR, but not only one time from the beginning. We do the XOR twice. First time we do the GNA_1 XOR the frame from the b-th byte until all the bytes in the frame is encrypted (of cause for a loop). Second time we do the GNA_2 XOR the frame from the a-th byte until all the bytes in the frame is encrypted (also for a loop). All the encryption is shown in Figure 1;

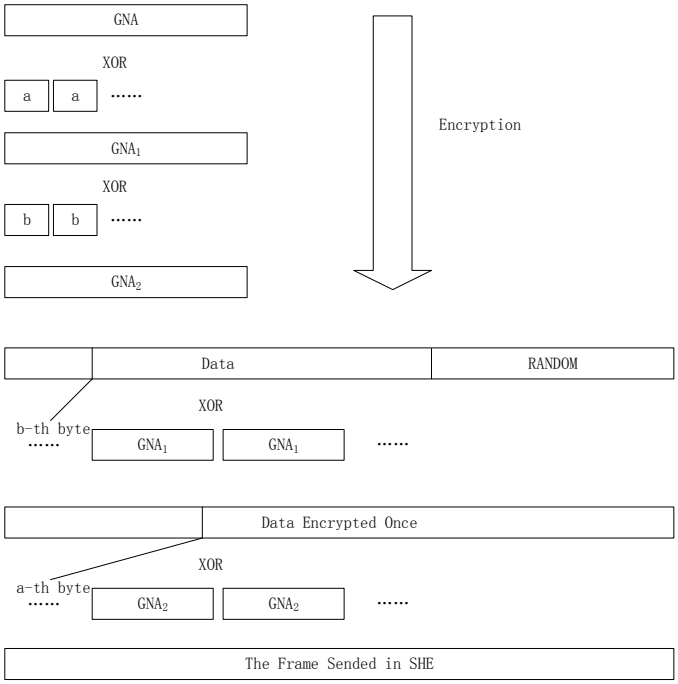

Figure 1. Encryption in WZ-lcp.

The facility broadcasts the RJF, all the facility in the band can get it. But only the gateway can save a, b, and GNA and have the ability to allow one facility to join in the networks. So it can use a, b, and GNA to decrypt the RJF. Then it can get the information that it should know (such as the network address of the facility). And build a link to the facility in gateway.

The gateway sends a frame named Allow-Join-Frame (AJF), which uses the same encryption. The facility get the AJF, do the decryption and build a link to the gateway too. Finally the facility send Confirm-Join-Frame (CJF) to the gateway. The gateway add the address of the facility to the facility table saved in its storage. So the Authentication is done. The facility join in SHE. The whole authentication is shown in Figure 2.

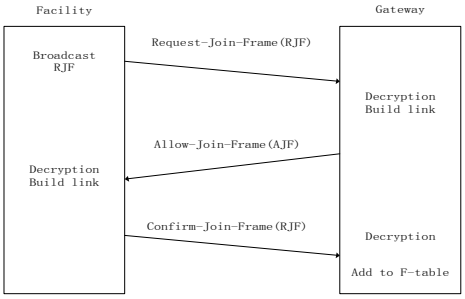

Figure 2. Authentication in WZ-lcp.

3.2. keys updating

Traditional keys update mechanism transports the keys in a secret ways. So the adversary cannot get the keys easily. But WZ-lcp do not transport any useful information in the Keys Updating. And also cost no more bandwidth waste in SHE. The keys updating is based on the time synchronization. In any wireless sensor networks, the time synchronization is quite an important part of the system. The facility in the WSN should use the time synchronization to transmit data in the same time. And in SHE, the time synchronization is also a recurrent event. The Keys Updating is described as follows:

Preparations:

Once the networks in SHE is founded, if in a period of time (in our design, one hour), no other facility join the networks. The gateway started a time synchronization. The time synchronization is done based on SFD [9]. This approach of time synchronization has the accuracy of 0.1s, which is quite enough for WZ-lcp.

Updating:

After the time synchronization, the gateway can receive a frame that the progress is finished. And every facility also know the time synchronization is finished. So they start the keys updating just finished the synchronization together.

Step1:

Every facility has two different pseudo-random Function $PRF_1(x)$ and $PRF_2(x)$. We update a, b by using them. Get the seconds of time, t. using (1), (2) to update.

$$a_{new}=PRF1((bold+t)mod256) \quad (1)$$

$$b_{new}=PRF2((aold+t)mod256) \quad (2)$$

The pseudo-random with the same seeds also get the same results. So we get the new keys.

Step2:

After the keys updating, all the facilities should send a frame to the gateway with the bit Updating changed and encrypted in a_{old}, b_{old} to the gateway.

The gateway check the all the facility in its table until all the facilities' frames with Updating bit changed are received. Then the gateway start to send a frame named Updating-Over-Frame (UOF) to every facility encrypted in a_{old}, b_{old}. After the UOF is received, the facility deletes the a_{old}, b_{old} and start using a_{new}, b_{new}. The keys updating is over. All the facilities in SHE use the new keys to protect the information. The keys updating is shown in Figure 3.

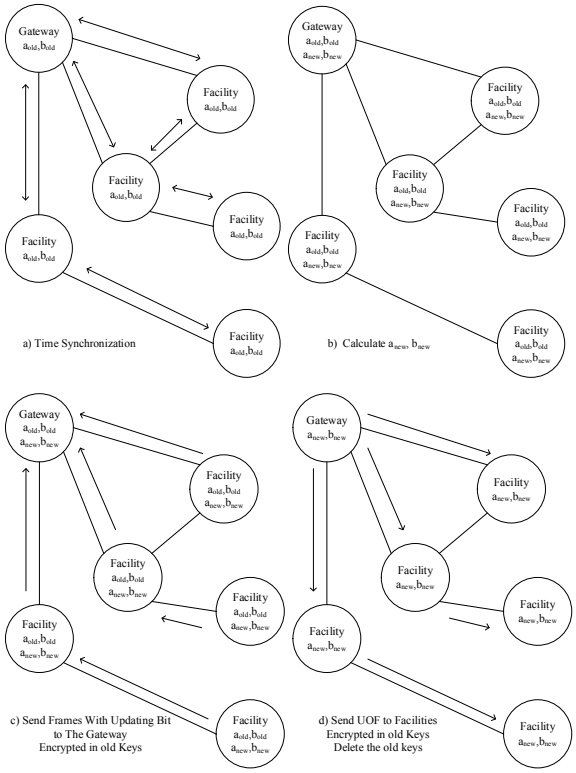

Figure 3. Keys updating in WZ-lcp

4. SECURITY AND POWERSAVED ANALYSIS

Compared to W2 scheme, there are some advantage in WZ-lcp. W2 scheme needs the facility to store more variables and hash functions. Table 1 shows the cost of storage both in W2 and WZ-lcp when initializes.

TABLE 1. Initialization Storage Cost

Cost of Storage		Function	Variable
W2	Tag	4	3
	Reader	4	4+X
WZ-lcp		2	2

X means the reader should store an array of variables to ensure the security in W2 scheme. X depends on the size of the RFID system.

After initialization W2 needs to update both the functions and the variables and the old variables is also needed so cannot be delete. WZ-lcp costs less storage than W2 with only 2 variables and 2 functions.

In W2, the authentication also needs data transmission for 3 times. But the calculation in W2 is much more complex than WZ-lcp [1].

The keys updating in W2 transmits the key encrypted. Although cracking in the frames is nearly impossible, the security is worried by a lot of people [10]. WZ-lcp don't transmit the key to update. The time synchronization is a new way to update the keys.

In order to prove the effectiveness of WZ-lcp, we choose ZigBee protocol to test and verify. We add the authentication and the encryption in ZigBee's APL. Firstly, we use 10 nodes

to verify the connectivity in WZ-lcp. The experiment shows that the WZ-lcp can found the WSN based on ZigBee.

We also do some test to ensure the security of WZ-lcp to defend the active attacks and passive attacks. Use sniffer to catch the frames. We record a, b and the GNA in WZ-lcp in 4 times keys updating. We seize the data part (5 bytes) of the frame in Table 2. The result shows that the active attack is useless for WZ-lcp.

TABLE 2. Encryption in WZ-lcp

DATA	GNA	a	b	T	GNA_1	GNA_2	$DATA_{enp}$
EA C3 54 B2 47	C9	3	37	4	CA	EF	CF E6 71 97 62
EA C3 54 B2 47	C9	9	13	19	C0	CD	E7 CE 59 BF 4A
EA C3 54 B2 47	C9	212	46	13	1D	33	C4 ED 7A 9C 69
EA C3 54 B2 47	C9	98	5	57	AB	AE	EF C6 51 B7 42

The passive attack is also useless in WZ-lcp because the key updating is quite frequently. The huge frames send by an adversary cannot occur in a little period of time.

Consider the particularity of SHE, we try to find balanced point in security and power-saved. WZ-lcp is a protocol with high security and low power. It takes advantage of W2 scheme and uses the most applied authentication. The superiority is following:

- The authentication is done in the 3 times of data transmission, which is widely used in most of the data transmission protocol like ZigBee and TCP/IP. The authentication wastes no more frame in WZ-lcp, and saves the power and the bandwidth.
- The authentication needs only 2 keys and 2 functions. Meet requirements of the smart home for storage capacity and calculations. The facility in SHE is consist of ARM and 8051 CPU, which are always lack of storage and computing abilities. The traditional authentication uses the matrix and array, causing the pressure on the facility in SHE, also the power-waste.
- The encryption uses the XOR calculation and be done two times for security. The adversary can only get the frames looks like useless. No matter how many frames an adversary can get, there is no useful information to explain the frame. Just in case the information was stolen by the adversary, the keys updating is quite easy for WZ-lcp.
- The XOR calculation is quite easy for ARM and 8051 CPU. And it can also be done by hardware (use logic circuits, etc.). This will cancel the calculation in the maximum extent.
- The time synchronization is necessary for any wireless networks protocol. WZ-lcp uses the time for the variable for the keys updating. Ensure the timeliness and consistency. Compared to the W2 in RFID, WZ-lcp uses less variable and less calculation, no counters, and no keys implicit transmission. The security is quite enough for SHE and reduce the power-wasting.

5. CONCLUSIONS AND FURTHER WORK

This article has demonstrated the attacks in security of Smart Home Environment. Additionally, we propose WZ-lcp scheme to enhance the security and defend against the active and passive attacks in SHE. WZ-lcp tries to find the balance between the security and the power-cost. So we takes advantage of W2 scheme in RFID and networks mechanism of ZigBee. As a consequence, with little cost in power, storage and ability of calculation of the facilities in SHE, WZ-lcp stop an adversary from attacking SHE and destroying the networks. Our PZ-lcp can distinguish the malicious facilities by the authentication and the keys updating based on time synchronization.

Therefore, we conclude that WZ-lcp meets the security and power requirements by the authentication and the keys updating. Furthermore, our future work is to improve WZ-lcp in WSN in our lab, with no more cost in the facilities.

ACKNOWLEDGMENT

We are grateful to the support of young teacher's innovation foundation of Jilin University.

REFERENCES

[1] M. Chan, D. Esteve, C. Escriba, and E. Campo, "A review of smart homes - Present state and future challenges," Computer Methods And Programs In Biomedicine, vol. 91, no. 1, pp. 55-81, Jul, 2008.

[2] R. Volner, P. Bores, V. Smrz, and T. Tallinn Univ, "A Product Based Security Model for Smart Home Appliances," Bec 2008: 2008 International Biennial Baltic Electronics Conference, Proceedings, Proceedings of the Biennial Baltic Electronics Conference, pp. 221-222, 2008. M. Sharaf. RFID

[3] Mutual Authentication and Secret Update Protocol for Low-Cost Tags. proceedings of the Trust, Security and Privacy in Computing and Communications(TrustCom), 2012 IEEE 11th International Conference on,IEEE 2012.

[4] W. Stevens, TCP /IP Illustrated, Volume 1: The Protocols,Addison-Wesley, ISBN 0-201-63346-9, 1994.

[5] D. Molnar, A. Soppera, and D. Wagner. "A scalable, delegatable pseudonym protocol enabling ownership transfer of RFID tags." In Selected Areas in Cryptography, Springer, 2006, pp. 276-290.

[6] A. Fernndez-Mir, R. Trujillo-Rasua, J. Castella-Roca, et al. "A scalable RFID authentication protocol supporting ownership transfer and controlled delegation" [M]. RFID Security and Privacy. Springer, 2012, pp.147-162.

[7] J. Yick, B. Mukherjee, and D. Ghosal, "Wireless sensor network survey," Computer Networks, vol. 52, Aug 22 2008, pp. 2292-2330.

[8] L. Herrera, A. Calveras, and M. Catalan, "two-way radio communication across a multi-hop wireless sensor network based on a commercial IEEE 802.15.4 compliant platform," in Eurosensors Xxv. vol. 25, G. Kaltsas and C. Tsamis, Eds., ed, 2011.

[9] S. Song, L. He, Y. Jiang, C. Hu, and Y. Cao, "Wireless sensor network time synchronization algorithm based on SFD," Communications in Computer and Information Science. pp. 393-400.

[10] L. Peizhuo, and L. Shengli, "A solution of hybrid TCP transmission in RFID reader network," IET Conference Publications. p. 65.