A Low Power Balanced Security Control Protocol of WSN

Yu Jiang[1,2], Jin Wang[3], Lili He[2], Yuanbo Xu[2], and Hongtao Bai[4(✉)]

[1] Key Laboratory of Information System Security of Ministry of Education, TNLIST, School of Software, Tsinghua University, Beijing 100084, China
jiangyu2011@jlu.edu.cn
[2] College of Computer Science and Technology, Jilin University, Changchun 130012, China
helili@jlu.edu.cn
[3] Information Engineering College, Yangzhou University, Yangzhou 225009, China
jinwang@yzu.edu.cn
[4] Center for Computer Fundamental Education, Jilin University, Changchun 130012, China
baihongtao@263.net

Abstract. Wireless Sensor Network is limited to the energy. Low-power and network security need us to pay adequate attention when it comes to WSN environment. We proposed a new security control protocol in this article named WZ-lcp protocol to meet the needs. The protocol depends on the synchronization of key and time. The key stored with int bytes in the facility and changing with time synchronization. The experimental results on digital wireless gas network show that the proposed protocol ensures security without costing power-wasting and data collision.

Keywords: WSN · WZ-lcp protocol · Authentication · W2-TCP protocol

1 Introduction

WSN contains huge amount of information and value of scientific research. For there is a huge potential market for such appliances there are serious security challenges that have to be addressed in order to realize their true benefits. Recently, there are many researches about public utility automatic reading system. Some studies also design the remote reading system, but without considering the power factor and consumption of system. Few works are about the design and implementation of the low power security control protocol for the gas utility automatic reading system. Obviously, the WSN technology is definitely going to be applied to public utility reading system and have a

H. Bai—This work was supported in part from the National Natural Science Foundation of China (51409117, 51679105, 61672261, 61572228), Jilin Province Department of Education Thirteen Five science and technology research projects [2016] No. 432.

J.-H. Lee and S. Pack (Eds.): QShine 2016, LNICST 199, pp. 46–51, 2017.
DOI: 10.1007/978-3-319-60717-7_5

wide prospect cause WSN nodes have the ability of self organizing without center node and have wide distribution characteristics [1]. As energy is a limited factor in wireless sensor network, the low power security control protocol is of great significance. Fernndez-Mir et al. proposed the RFID protocol which is not only achieves control delegating but improves the scalability of the whole system. W2-TCP scheme is proved to have effect on the security [2]. However, an authentication is of necessity before a facility join in the network. Bandwidth and energy-saving are the two problems that mainly affect W2-TCP. Many researches have been conducted to provide a plan for WSN. The goal is to achieve the requirement that defend the attack which are as follows: (1) active attack (2) passive attack.

In this paper, we proposed a new security control protocol in this article named WZ-lcp protocol to meet the needs [3]. The protocol depends on the synchronization of key and time. The key stored with int bytes in the facility and changing with time. The experimental results on wireless gas network show that the proposed protocol ensures security without costing power-wasting and data collision.

2 The Proposed Protocol

2.1 Facility Authentication

The WZ-lcp protocol has the following processes.

Authentication Procedure :
Facility Fs, Gateway G
1）*Initialization*
F_s *initializes GNA,* $PRF_1(x)$, $PRF_2(x)$
F_s *gets a,b,c from G or database*
2）*Authentication*
F_s *builds the RJF:*
GNA is G's network address

$$\left.\begin{array}{l} a\ XOR\ GNA -> GNA_1 \\ b\ XOR\ GNA -> GNA_2 \\ c\ XOR\ GNA -> GNA_3 \end{array}\right\} \text{Triple Encryption Key Calculate}$$

$$\left.\begin{array}{l} GNA_1 XOR\ RJF\ from\ bth\ byte \\ GNA_2 XOR\ RJF\ from\ cth\ byte \\ GNA_3 XOR\ RJF\ from\ ath\ byte \end{array}\right\} \text{Triple Encryption}$$

3）*Join Network*
G gets RJF
G decrypts RJF with a,b,GNA
G allows F_s *to join network*

Every facility stores the following information: int a; int b; gateway's network address (GNA); PRF1(x) and PRF2(x). a, b ranges from 0 to 255, PRF1(x) and PRF2 (x) are the same. The facility gets a, b, GNA, PRF1 and PRF2 from the gateway or the database. After initializing, when the facility is going to join in the network, it should

broadcast a frame with the information the network needs named Request-Join-Frame (RJF). WZ-lcp uses a, b and GNA to encrypt the whole frame. Her we will describe how the encryption is going.

At first, the facility gets a, b and GNA,

$$a\,XOR\,GNA = GNA1$$

$$b\,XOR\,GNA1 = GNA2$$

Then the facility fills all frame to ensure the same length of all kinds of frames with random byte. GNA1 and GNA2 are used to encrypt the whole frame. WZ-lcp uses the XOR twice. First time GNA1 XOR the frame with bytes in length b until all the bytes in the frame are encrypted. Second time GNA2 XOR the frame with bytes in length a until all the bytes in the frame are encrypted (Fig. 1).

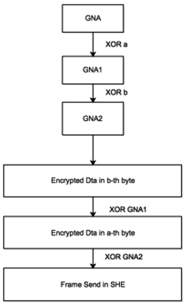

Fig. 1. Encryption in WZ-lcp.

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 is needs. A link is built to the facility in gateway [4].

The gateway sends a frame named Allow Join Frame which uses the same encrypting method. The facility gets AJF, decrypt the information and build a link to the gateway, either. Finally, the facility sends Confirm Join Frame to the gateway. The gateway adds the facility address to the facility table saved in the storage [5]. The whole authentication is shown in the (Fig. 2).

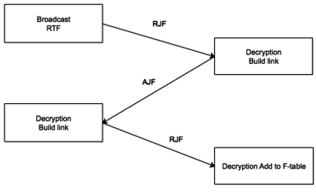

Fig. 2. WZ-lcp authentication process.

2.2 Keys Updating

Key Update Procedure
Gateway G, Fs, Fr

1) Preparations

Time synchronization Fs, Fr gets t

2) Updating:

Fs, Fr get $PRF_1(x)$,$PRF_2(x)$, $PRF_3(x)$

$a_{new}=PRF_1((b_{old}+t)mod256)$
$b_{new}=PRF_2((c_{old}+t)mod256)$
$c_{new}=PRF_3((a_{old}+t)mod256)$

3) Transport:

Fs, Fr send update frame to G

Conventional key update method transfers keys in secret ways. In this way the attackers cannot get the keys easily. But WZ-lcp protocol do not transfer any useful information in this process. The process of key updating is on the basis of time synchronization. In WSN network structures, time synchronization is important. The facility in the WSN should use the time synchronization to transfer data simultaneously. And in automatic reading system, time synchronization occurs repeatedly [6]. The key updating process is described as follows:

Step1: Each of the facilities has two different pseudo-random functions $PRF_1(x)$ and $PRF_2(x)$. At first we need to update a, b with the functions. Then get the time t. with (1), (2), (3) to update,

$$a_{new} = PRF_1((b_{old} + t)mod256) \tag{1}$$

$$b_{new} = PRF_2((c_{old} + t)mod256) \tag{2}$$

$$c_{new} = PRF_3((a_{old} + t)mod256) \tag{3}$$

Step2: As the keys has been updated, all the facilities need to send a frame to the gateway with the bit.

3 Security and Power-Saved Analysis

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

Table 1. Initialization storage cost

Cost of Storage		Function	Variable
W2-TCP	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-TCP scheme. X depends on the size of the RFID system. In W2-TCP, the authentication also needs data transmission for 3 times. But the calculation in W2-TCP is much more complex than WZ-lcp. 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. The gas meter reading system is a fundamental instrument in the house. Figure 3 shows the gas meter node.

Fig. 3. Gas nodes picture

In hardware, we try to choose those chips with lower consumption, richer resources. The outer circuit should be made up of low energy consumption components and the power should have large capacity and running stability. Otherwise, the system need low voltage and low frequency. In the designing of software, here are some instructions wo need to concern. First of all, MCU time is asked to reduce, we may try the way of interrupt. With this we hope the circulation can be avoided when querying, dynamic scanning through the event-driven way. Working efficiency should be guaranteed and the event of power on/off should be detected.

Tests are done to ensure the security of WZ-lcp protocol and the defense of both active and passive attacks. We then record a, b and the GNA in WZ-lcp in 4 times keys updating. The result in Table 2 shows the active attack is useless for WZ-lcp.

Otherwise, the passive attack is also useless in WZ-lcp for the key updating is quite frequently. According to the network protocol, when MCU starts to work, the time cost of joining network is tjoin_net $\approx$ 10 s, after that MCU will shut down RF transmitter and transfer to sleeping state immediately. Gas nodes wake up once an hour, the active time is no more than 4 s. The active energy consumption in an hour is 0.02284 mAh, the sleep energy consumption is 0.05392 mAh. The energy consumption of sensor module is 0.40033 mA. The energy consumption of power management module for one hour is 1.111×10^{-4} mAh. Finally, we can get the energy consumption of 0.9224533 mAh for a day and 336.695458 mAh for a year.

WZ-lcp is actually a protocol which balanced security and power perfectly. For it takes the advantages of W2-TCP scheme and uses the most applied authentication. Here we will list the advantages of WZ-lcp. At first, the authentication process is repeated for 3 times in data transmission, the repeated work is adopted in ZigBee and TCP/IP. Power and the bandwidth are saved at the same time. The process of the whole authentication requires only three keys and two functions and this can solve the problem of lacking storage and computing capacities. Besides, the XOR calculation is

Table 2. Encryption in WZ-lcp

DATA	GNA	a	b	c	t	GNA_1	GNA_2	GNA_3	$DATA_{enp}$
1F59D55800	77	5	34	8	9	1A	DD	D1	F58EDB6E01
1F59D55800	77	32	12	23	12	7D	A3	3C	EBFBEA0605
1F59D55800	77	6	5	34	24	D3	D4	B3	AB3B493FBC
1F59D55800	77	22	23	2	33	D2	66	B9	F58BABC142
1F59D55800	77	44	14	17	16	20	01	A2	D4373C9BC0
1F59D55800	77	26	33	28	59	F1	B8	F4	25FA61605A
1F59D55800	77	55	6	58	60	7C	F7	F9	71B6B176D5
1F59D55800	77	17	5	28	15	73	BC	8E	6215A29652
1F59D55800	77	59	2	45	48	BA	15	C7	CCB6BBBAB8
1F59D55800	77	0	4	39	11	90	18	92	453734C7FE

done for 3 times for security concerns. The XOR calculation is not a question for ARM and 8051 CPU. At last, WZ-lcp protocol can ensure the timeliness and consistency.

4 Conclusions and Further Work

In this paper, we proposed a new security control protocol in this article named WZ-lcp Protocol to meet the needs. The protocol depends on the synchronization of key and time. The key stored with int bytes in the facility and changing with time synchronization. The experimental results on digital wireless gas network show that the proposed protocol ensures security without costing power-wasting and data collision.

References

1. Song, S., He, L., Jiang, Yu., Hu, C., Cao, Y.: Wireless sensor network time synchronization algorithm based on SFD. In: Wang, R., Xiao, F. (eds.) CWSN 2012. CCIS, vol. 334, pp. 393–400. Springer, Heidelberg (2013). doi:10.1007/978-3-642-36252-1_37
2. Jiang, Y., Liang, Y., Cui, Y., et al.: Wireless digital gas meter with lower power consumption. In: 2010 Fifth International Conference on Frontier of Computer Science and Technology (FCST), pp. 192–197. IEEE (2010)
3. Xu, Y., Jiang, Y., Hu, C., et al.: A balanced security protocol of wireless sensor network for smart home. In: 2014 12th International Conference on Signal Processing (ICSP), pp. 2324–2327. IEEE (2014)
4. Lv, P., Lai, S.: A solution of hybrid TCP transmission in RFID reader network. In: 2006 IET International Conference on Wireless, Mobile and Multimedia Networks, pp. 1–4. IET (2006)
5. Li, J., Brassil, J.: On the performance of traffic equalizers on heterogeneous communication links. In: Proceedings of the 3rd International Conference on Quality of Service in Heterogeneous Wired/Wireless Networks, p. 33. ACM (2006)
6. Darsena, D., Gelli, G., Verde, F.: Non-cooperative superposition relaying for multicarrier cognitive networks. In: 2016 IEEE 27th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), pp. 1–6. IEEE (2016)