Design of Embedded Secure Gateway Based on 6LoWPAN

Yuanyuan Zhou, Zhiping Jia, Xianli Sun, Xin Li, Lei Ju
School of Computer Science and Technology, Shandong University
Jinan, China,250101
Email: embed1988@126.com

***Abstract*-The paper proposes an embedded security gateway based on 6LoWPAN, which connects wireless sensor network with IPv6 network. Users can query current data of a certain sensor or historical data. The user authentication and SNEP security mechanism provide good secure guarantee to communication between networks; the address translation mechanism transforms an IPv6 address into a short address, which improves communication efficiency in 6LoWPAN network. The experimental results show that the design of gateway can realize communication authentication and security between the gateway and sensor node, and it balances performance and security.**
***Keywords*-6LoWPAN; gateway; network security; SNEP protocol.**

I. INTRODUCTION

Recently, low-rate wireless personal area network (LR-WPAN) has become a hot issue. It has the following characteristics: low data rate, low power consumption, and short communication range. IEEE 802.15.4 is a standard designed for LR-WPAN, and it mainly focuses on Wireless Sensor Networks (WSN). However, the standard only defines the PHY and MAC layers, and does not consider upper layers. In 2004, IETF established 6LoWPAN (IPv6 over low-power wireless personal area network) ([1]) work group, which devotes to research on how to realize the transmission of IPv6 packets on IEEE 802.15.4 and related problems. As IPv6 protocol stack can't run over 802.15.4 standard directly, 6LoWPAN adds an adaptation layer, which implements the seamless connection of MAC and network layer.

IEEE 802.15.4 defines two kinds of link addresses: IEEE EUI-64 addresses and 16-bit short addresses, from which 6LoWPAN can choose to forward and route packets in link layer. The maximum physical layer packet size of 802.15.4 protocol is 127 bytes, so the adaptation layer must provide the fragmentation and reassembly function for oversize IPv6 packets. Except for the MAC header and IPv6 header, the remaining space for upper-layer protocol is less, which leads to low fragmentation efficiency.

Sensor nodes are generally deployed in open environment, and messages are easy to be attacked in transmission process. Although IEEE 802.15.4 provides AES (Advanced Encryption Standard) security, the mechanism is comparatively loose. Moreover, the security mechanism in network layer (e.g., IPsec, security neighbor discovery) is too complex. So it is one of the significant problems in 6LoWPAN research to find a proper security mechanism.

In order to address the above-mentioned issues, we have proposed an embedded gateway design based on the 6LoWPAN, which provides an efficient, secure and trustworthy communication infrastructure between IPv6 networks and WSN. The technical contributions are as follows.

1) We define an address mapping table in the gateway which provides mapping between 16-bit IEEE 802.15.4 addresses and 128-bit IPv6 addresses. When an IPv6 packet is routed to the gateway from Internet, an IPv6 address is translated to a 16-bit short address, which is used for communication within WSN. The method improves fragmentation efficiency, transmission speed and use rate of packets.

2) In order to provide security in WSN communication, our proposed gateway design adopts SPINS (security protocols for sensor networks), which includes SNEP (secure network encryption protocol) and μTESLA (micro timed efficient streaming loss-tolerant authentication protocol). SNEP has the characteristic of low communication overhead. In our framework, we use the gateway, which has large store space and strong computing capability, to distribute and manage keys. With the SNEP protocol, the system realizes two-party authentication, data confidentiality, integrity as well as freshness. In our system, we concern only communication between an external user (in IPv6 network) and a particular sensor node (in WSN), without broadcast queries. As a result, we introduce only the SNEP protocol, instead of the full-fledged SPINS.

3) Besides, we build a web server in the gateway, which stores data periodically collected from sensor nodes. Users are able to query stored historical data, which allow operations such as event detection ([2]) in WSN. Furthermore, we maintain a user access authority table in the web server, which implements user authentication and access control services.

The paper is organized as follows: Section Ⅱ reviews the related work on WSN-IP network interconnection; Section Ⅲ interprets the access system of 6LoWPAN network and functions of the gateway in detail; Section Ⅳ evaluates the performance of the gateway on NS2 simulation platform and

978-1-61284-307-0/11/$26.00 ©2011 IEEE

analyzes experiment results; Section Ⅴ concludes the paper.

II. Related Works

For WSN-IP network interconnection, Adam Dunkels et al. proposes three approaches in [3], which are proxy architecture, DTN (Delay Tolerant Networks) overlays, and TCP/IP for sensor networks. In proxy architecture, a special proxy server is deployed between the sensor network and TCP/IP network. Generally, a gateway acts as the proxy server and can operate in two ways. In the first case, the gateway can be a relay to translate and forward packets from one network to the other. Reference [4] proposes a framework, in which every sensor node has a node ID and a virtual IP address assigned by the gateway; similarly, every host has an IP address and a virtual node ID. The gateway translates and transforms the received packets. However, it cannot support query for historical data. In the other case, the gateway operates as a front-end for sensor network. It collects data from sensors and stores information in a database for clients' query. In [5], once a sensor node detects that the physical information in a region exceeds the predefined threshold, it sends a message to the sink node. The gateway receives and stores the message in a database. In this method, it prevents illegal users from accessing data. However, it does not provide safety service at sensor end.

The DTN architecture in [3] is designed for fault-prone disturbed environment. DTN gateway forwards bundles between regions which share a common bundle layer that resides above the transport layer.

Directly employing TCP/IP protocol in sensor network allows seamless integration of the sensor network and TCP/IP network, without additional proxies or gateways. However, it also introduces some disadvantages. Reference [6] concludes that implementing the full IP protocol stack on sensor networks may not be feasible or desirable. The 6LoWPAN radically alters the calculation by introducing an adaptation layer that enables efficient IPv6 communication over IEEE 802.15.4. In [7], a gateway solution for IPv6 wireless sensor networks is proposed with 6LoWPAN technology.

The introduction of IPv6 to sensor networks brings advantages of IP network. However, it also raises some security issues. The 6LoWPAN working group published a draft ([8]) in 2010, which analyzes the security requirements, threats and key management methods in 6LoWPAN. It also points out that using IPsec (Internet Protocol Security) in 6LoWPAN still encounters many issues. In recent years, the research on key management in WSN has made some progress. Reference [9] surveys typical WSN key management schemes and protocols; and SPINS is one of the popular security framework protocols.

To address these disadvantages, this paper proposes an embedded secure gateway based on 6LoWPAN, by combining the proxy architecture and the TCP/IP interconnection. The gateway achieves direct communication between end users and sensor nodes, and enables users to query real-time sensor data and stored historical data. Besides, it introduces user verification mechanism and the SNEP protocol which implements communication security.

III. The Network Access Framework

Our proposed framework enables the interconnection of WSN and IPv6 network. As shown in Fig. 1, a complete access framework includes 6LoWPAN gateway, sensor nodes, web server, and IP users. First, an IP user connects to the gateway. Then, the gateway identifies the user, while only a legal user is permitted to submit query request about sensor nodes. Finally, the gateway sends processed query information to the WSN, and subsequently replies results to query users.

1) 6LoWPAN gateway: all packets from the two networks must be forwarded by it. The gateway deploys dual stack-traditional IPv6 protocol stack and 6LoWPAN protocol stack, as shown in Fig. 2. What's more, the SNEP protocol is introduced in IP layer to provide confidentiality and authentication service.

The gateway defines two tables: the address mapping table, achieves the two-way conversion between IPv6 addresses of sensor nodes and 16-bit short addresses; and the user access authority table, is responsible for verifying, authorizing and adding end users. Moreover, the gateway has two interfaces: the Internet interface is linked to outside routers; the serial interface is linked to the sink node. It also stores data periodically collected in the built-in web server.

2) Sensor node: each node works with 6LoWPAN protocol stack, and includes a security storage module which stores keys and message authentication information for communication. Each node has an IEEE EUI-64 address and a 16-bit short address.

3) End user: each user has his own user name and password. Trusted users can query node data by choosing a node address, or review historical data.

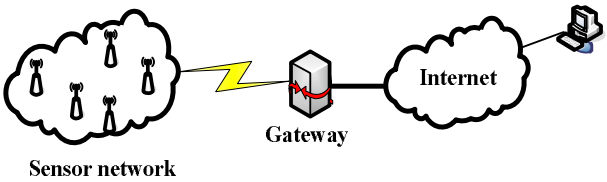


Fig. 1. Network access framework

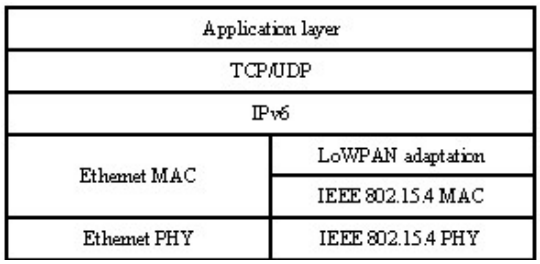


Fig. 2. Dual stack of the gateway

A. Gateway Architecture

Based on the design scheme in [10], the gateway software platform in the paper consists of TCP/IP protocol stack, web server, and the data query and security management part. The data query and security management part involves data analysis, query transformation and security management, as shown in Fig. 3. Our work on the gateway design is as follows: Firstly, adding a security module to the gateway. The module is responsible for assigning a master secret key shared between each node and the gateway, providing communication encryption and authentication. Secondly, the gateway stores an address mapping table, through which IPv6 addresses or short addresses can be converted in two-way. Thus, the delivery of packets in WSN is more efficient. Thirdly, the gateway can analyzes, processes, and stores the data periodically collected by sensor nodes, so users can learn about physical information in a certain period.

a) Address Translation

At first, an end user sends query request to the gateway. The packet is successively processed in gateway by a data analysis module (DAM), a query transformation module (QTM), and a security management module (SMM), before sent to WSN. The sensor data replied to the user are processed in a reverse procedure.

When the DAM receives the packet from a user, it uses built-in data extracting module to convert it to the web query, which is stored in a queue before sent to the QTM. For sensor reply, the DAM uses web reply module to send to the user.

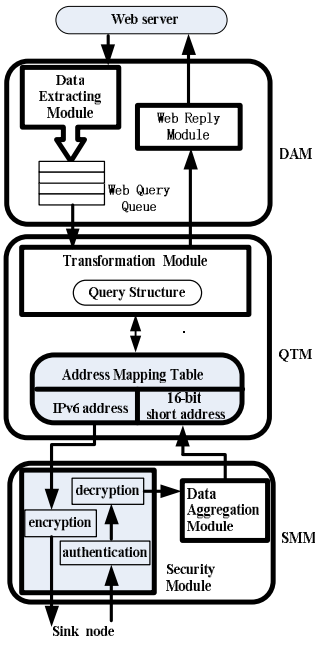


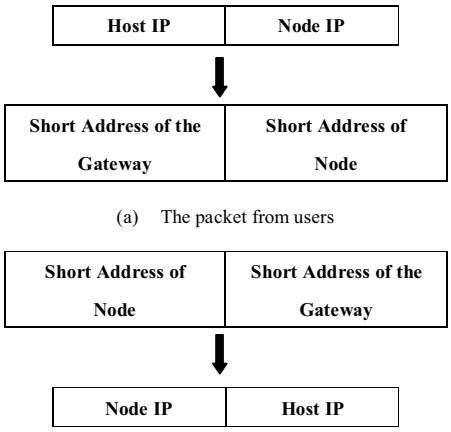
Fig. 3. The function modules of data query and security management part of the gateway.

The QTM includes a transformation module and an address mapping table. The transformation module transforms a web query from the DAM to a proper sensor query, and does reverse manipulation to sensor reply. The address mapping table records the 128-bit IPv6 addresses of sensor nodes and the corresponding 16-bit short addresses. When the gateway receives a user query targeting at a particular sensor node, it searches the table and translates the destination 128-bit IPv6 address of the node to a short address. Furthermore, the original IPv6 source address of the user is replaced by the short address of the gateway (refer to Fig. 4(a)). The gateway records the user address and sends the modified sensor query to the WSN. Similarly, when receiving a reply packet from the WSN, the gateway translates the source address to the node's IPv6 address, and translates the destination address to the user's IPv6 address stored previously (refer to Fig. 4(b)).

The advantages of using short addresses in the WSN are as follows: it eliminates encapsulation in network and transport layer, reduces packet header and improves utilization of the packet; when receiving packets with compressed IPv6 header, intermediate nodes only needs to process and forward packets in adaptation layer without header decompression, so node power consumption is reduced and the speed of routing packets is improved.

b) Security Management

The security management module (SMM) consists of a security module and a data aggregation module. The sensor query from QTM is first passed to the security module. The security module uses the SNEP protocol to encrypt packets before sending them to the sink node, and authenticate the reply packets from sensor nodes. Unsafe packets are directly deserted and safe packets are decrypted. The packets are aggregated in the data aggregation module before sent to QTM. The detailed description of the security protocol and implementation of the encryption algorithms are presented in Section III-B.



(a) The packet from users

(b) The packet from sensor nodes

Fig. 4. Source address and destination address translation

c) Web Server

We create a web server in the gateway, which stores the data periodically collected from sensor nodes. Users can query these data at any time. In the applications such as environmental monitoring, these data can be used for event detection in the WSN. Due to the sophisticated environment and unreliability of sensor nodes, the administrator cannot ensure whether an event has happened or not, based only on abnormal data received at a particular moment. Instead, all data in a period of time are needed because of the temporal correlation of an event. The web server also stores a user access authority table, which stores users' authentication information. It prevents illegal users from accessing the gateway and controlling sensor devices, and sets administration rights for different users.

B. SNEP Protocol

The system adopts SNEP (secure network encryption protocol) to implement two-party authentication, data confidentiality, integrity as well as freshness. SNEP is a proprietary protocol of WSN with low communication overhead. It takes security guide model with pre-shared master key, assuming that each node has a master key shared with the base station, and other keys are derived from the master key.

SNEP only stipulates the protocol implementation process, but doesn't provide any concrete algorithms. Given the strict resource restraint in WSN, a proper encryption algorithm should make a good compromise between security intensity and other factors. Reference [11] shows that the RC5 algorithm is more suitable to WSN, with the characteristics of simplicity, high efficiency and small code size. So we use RC5-CTR to achieve encryption.

The gateway acts as a trusted network entity. Before communication, the gateway assigns each sensor node a master key χ shared with the gateway. Some independent keys can be derived from χ with Pseudo-Random Function (PRF) F based on communication directions: $K_{GS}=F_{\chi}$ (1) and $K'_{GS}= F_{\chi}(2)$ denote the encryption key and the MAC (message authentication code) key of the gateway, respectively; and $K_{SG}= F_{\chi}(3)$ and $K'_{SG} = F_{\chi}(4)$ denote the encryption key and the MAC key of a sensor node, respectively. All the keys are shared between the communication parties, i.e. the gateway and a sensor node. Each of the communication parties has a counter, and its value will increase by one when sending or receiving a message. Because of the different counter values, the same message will be encrypted to different ciphertexts, which provides semantic security and weak data freshness. The encrypted data have the following format: $E=\{D\}_{<K,C>}$, where D is the data, K is the encryption key, and C is the counter as the initialization vector in CTR mode. The count is set long enough to prevent repeat in node lifetime.

SNEP uses the message authentication code to realize data integrity and two-party authentication. In order to reuse the encryption algorithm, we choose CBC-MAC (in [12]) to generate the message authentication code. The formula of computing the message authentication code has the following format: $M=\mathrm{MAC}(K',C \parallel E)$, where K' is the MAC (message authentication code) key, C is the counter and E is the encrypted data. The whole process of communication between Gateway G and Node S is as follows:

$$G \to S : \{D\}_{<K_{GS},C_G>}, \mathrm{MAC}(K'_{GS}, C_G \parallel \{D\}_{<K_{GS},C_G>}); \quad (1)$$

$$S \to G : \{R\}_{<K_{SG},C_S>}, \mathrm{MAC}(K'_{SG}, C_S \parallel \{R\}_{<K_{SG},C_S>}). \quad (2)$$

Where D denotes the query from the gateway, and R denotes the replied data from the senor node; C_G and C_S denote the counter value of the gateway and the sensor node, respectively.

Before the sensor query is sent to WSN, the security management module operates as follows: encrypting the message with the encryption key K_{GS} and gateway counter C_G, generating the message authentication code (MAC) with MAC key K'_{GS}, and sending the ciphertext and MAC to node S. Node S decrypts the sensor query if the message authentication code is correctly verified. When the node replies to the gateway, similar encryption, authentication and decryption operations are performed. SNEP adopts the ciphertext authentication method that the receiver will directly desert a message without decryption, if the message is not correctly verified. This method speeds up the authentication process. The following example shows that how the gateway guarantees communication security with encryption and authentication.

Assuming that there is an attacker A in the WSN, which tries to get plaintext from a captured ciphertext. Because every message is encrypted with different counter values, even if A has had several ciphertexts of the same message, it cannot infer the corresponding plaintext. If a normal node B continuously sends to the gateway several messages, one of which is captured by A and is sent repeatedly, the gateway can judge according to the counter values whether received messages are sent in order by B, which restrains the replay attack. When receiving a forged message, the gateway knows the message has been modified by computing the message authentication code.

IV. Experiment Simulation

We use NS2 (Network Simulator, version 2, [13]) to evaluate the performance of our proposed gateway architecture. In a simulation area with $100 \times 100 m^2$, five sensor nodes (label from N1 to N5) and a gateway (N0) are randomly distributed. During the simulation time of 900 seconds, a randomly chosen sensor node sends packets with different length to the gateway with an interval of 0.2 seconds, in order to test the average delay. The average delay denotes the average time interval of delivering packets from the sender to the receiver. The lower curve in Fig. 5 shows that delay increases with increased packet length. When the packet length exceeds 127 bytes, the fragmentation and reassembly of packets also take up some time, so the delay increases with a higher degree. We use RC5 and CBC-MAC algorithms to implement encryption and authentication in SNEP. Although introducing the security mechanism increases overhead, the upper curve (denotes the

average delay with SNEP) in Fig. 5 shows the performance of the gateway is still in good level. By comparing the two curves, we conclude that SNEP doesn't bring much increase to the network delay, and it also proves that SNEP is a low-overhead security protocol. So it is feasible to adopt SNEP in gateway and WSN.

To test the security function of the gateway, we set the following simulation environment as shown in Fig. 6: N1 acts as the sink node; N2 to N4 are normal nodes and N5 is a malicious node. N2 to N5 keep sending request packets to N1. By analyzing the generated trace file, the results are shown in Fig. 7: nodes N2 to N4 receive response packets from N1, but N5 cannot. The reason is that N5 does not have the shared key with the gateway and it cannot be authenticated, so N1 does not respond to its data request. On the contrary, N2 is authenticated successfully by the gateway with shared keys, and then the gateway assigns a temporary communication key for it and N1. So N1 receives and responds to the packets from N2 with the temporary key. Communications with N3 or N4 adopts the similar way.

The experiments prove that the design of gateway is able to achieve communication authentication and security in WSN. Specially, it balances the gateway performance and security at the same time.

V. Conclusion

The paper designs a 6LoWPAN-based gateway, which defines several novel function modules. With the gateway, users not only directly communicate with sensor nodes, but also query historical data in the web server. The user access authority table identifies and authorizes users; the address mapping table translates IPv6 addresses to short addresses, which improves communication efficiency; SNEP is adopted to implement encryption and authentication of wireless communication. The experiment uses NS2 to simulate the delay and security performance of the gateway, and the result shows that the gateway can realize communication security and good performance at the same time.

Acknowledgment

This research is sponsored by the Natural Science Foundation of China (NSFC) under grant No. 61070022, 60903031, and the Natural Science Foundation of Shandong Province, No. 2010ZR2010FM015.

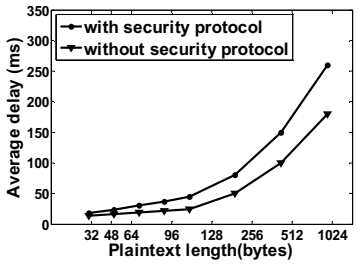


Fig. 5. Average delay

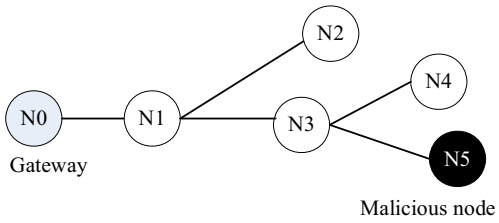


Fig. 6. Node distribution

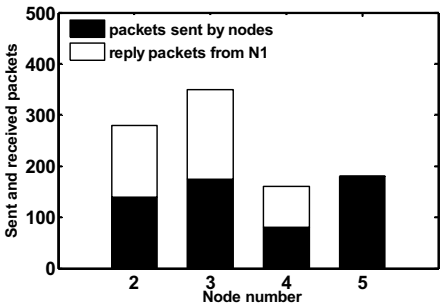


Fig. 7. Node communication authentication

References

[1] G. Montenegro , N. Kushalnagar, J. Hui, D. Culler, *Transmission of IPv6 Packets over IEEE 802.15.4 Networks,* RFC4944, http://www.ietf.org/rfc/rfc4944.txt，September,2007.

[2] Donglei Cao, Jiannong Cao, Peihong Jin, *A Fault-Tolerant Algorithm for Event Region Detection in Wireless Sensor Network*s, Vol.30, No. 10, pp.1770-1776, Oct. 2007.

[3] A. Dunkels, J. Alonso, T. Voigt, H. Ritter and J. Schiller, *ConnectingWireless Sensornets with TCP/IP Network,* in proceedings of the second International Conference on Wired/Wireless Internet Communications(WWWIC2004), Frankfurt, Germany, Feb.2004.

[4] K.A. Emara, M. Abdeen, M. Hashem, *A gateway-based framework for transparent interconnection between WSN and IP network,* the IEEE Region 8 EUROCON 2009 Conference, Saint-Petersburg, Russia, pp.1775–1780, 2009.

[5] Weiren Shi, Jie Zhang, Yunjian Tang, Chao Huang, *Design and implementation of wireless sensor network gateway,* Computer Application, Vol.26, No.11, pp.2525-2527, Nov.2006.

[6] M. Zuniga, B. Krishnamachari, *Integrating future large-scale wireless sensor networks with the Internet,* USC ComputerScience Technical Report CS 03-792, 2003.

[7] Gopinath Rao. S, Zeldy Suryady, Usman Sarwar, Mazlan Abbas, *A Gateway Solution for IPv6 Wireless Sensor Networks,* 2009 International Conference on Ultra Modern Telecommunications, St. Petersburg, Russia, pp.1-6, Oct. 2009.

[8] S.Park,K.Kim,E.Seo, *IPv6 over Low Power WPAN Security Analysis*, draft-daniel-6lowpan-security-analysis-04.txt, Mar.2010.

[9] Zhong Su， Chuang Lin， Fujun Feng, and Fengyuan Ren, *Key Management Schemes and Protocols forWireless Sensor Networks,* Journal of software, Vol.18, No.5, pp.1218-1231, May 2007.

[10] Kwang-il Hwang, Jeongsik In, NhoKyung Park, Doo-seop Eom, *A Design and Implementation of Wireless Sensor Gateway for Efficient Querying and Managing through World Wide Web,* IEEE Transactions on Consumer Electronics, Vol.49, No.4, pp.1090—1097, Nov.2004.

[11] A. Perrig, R. Szewczyk, V. Wen, D. Culler, J.D. Tygar, *SPINS: security protocols for sensor networks,* Proceedings of ACM MobiCom'01, Rome, Italy, pp.189–199, Jul.2001.

[12] D. Whiting, R. Housley, and N. Ferguson, *Counter with CBC-MAC (CCM),* RFC 3610, http://datatracker.ietf.org/doc/rfc3610/,Sep.2003.

[13] *The Network Simulator - ns-2*, http://www.isi.edu/nsnam/ns/.