International Journal of Security and Its Applications
Vol. 10, No. 12 (2016), pp.1-12
http://dx.doi.org/10.14257/ijsia.2016.10.12.01

Research on Access Control and Encryption Transmission of 6LoWPAN

Fan Tongrang[1], He Bingchao[2], Zhao Wenbin[3*], Huang Xin[4] and Yu Tao[5]

[1,2,3,4] School of Information Science and Technology, Shijiazhuang Tiedao University, Shijiazhuang, Hebei 050043, China
[5] Institute of Network Science and Cyberspace, Tsinghua University, Beijing, 100084, China
[1]fantr@stdu.edu.cn, [3]zhaowb.email@qq.com*

Abstract

Based on research about network mobility, this paper analyzes the security requirements of internet of things and wireless network based on 6LoWPAN, and designs the security architecture based on 6LoWPAN network, especially for the frequent mobile handoff access and data multi-hop forwarding. The access authentication scheme and data encryption method are designed and implemented based on 6LoWPAN mobile switching. Through comparing with non-symmetric encryption and symmetric encryption, AES pre-shared key encryption scheme is determined to use for 6LoWPAN, and is compared with typical cryptographic algorithms on internet of things platform and Contiki operate system. In experiment, the lightweight security of IoT mobile communication is realized on CC2530 nodes, including the advanced encryption standard, the payload encryption of network data packet and wireless nodes access authentication. Security architecture for mobile switching scenarios are verified, the feasibility of proposed scheme is confirmed.

Keywords: *6LoWPAN, Mobile security, Access Authentication, AES Encryption, Pre-Shared Key*

1. Introduce

6LoWPAN technology enable wireless sensor network node to be equal and free to access to the Internet. At the same time, the Internet hosts can transparently access node of the Internet of things, it streamlined the part of the function of the IPv6 protocol, retain and simplifies necessary part, while clipping and delete non-essential part [1]. This has very important for achieving full integration of IoT and IPv6-based Internet. Mutual integration of Internet and IoT can form a real IP network, in order to obtain needed information through a terminal at any time and place. This is good prospect in future information society. The use of 6LoWPAN technology will effectively solve the problem of accessing the nodes of IoT perception layer to Internet, to achieve the sensor network peripheral nodes IP-based [2]. The IoT terminals are a large number of sensor nodes and wireless nodes, most of which have mobility. Currently, some research at home and abroad carry out a wide range of improving the mobility of the IoT in the access point switching delay and transmission efficiency of exploration, the terminal node usage scenarios is increasing, the performance is further improved.

Due to the limitations of personal area network technology, originally designed for its security is not adequate enough, IoT or low-power network terminal devices and data is highly easier to attack. Mainly reflected in the network using self-organization network and lack of proper authentication mechanisms, the local node in the connections between nodes without any restrictions, and the network is relying on wireless media, messages can be received by any node, which means that malicious users can copy or disguise a

ISSN: 1738-9976 IJSIA

normal node, cause such as denial of service attacks, or use traps to steal, tamper with data. Therefore, the safety design of the network is essential in this research. Security should be designed to correspond to the specific model of the network, corresponding to the reasonable scheme [3].

Based on previous research of mobility supported of the next-generation Internet [4] and the mobility optimization with 6LoWPAN [5], this paper proposes a 6LoWPAN mobile security communication architecture, which is based on wireless access authentication and data encryption.

2. Related Research

IPSec protocol [6] is a secure communication protocol for data security on Internet. It is an open standard architecture using encryption security services. Protocol provides active security protection through end-to-end security. However, IPsec is limited by the 6LoWPAN network, there exist some defects: such as the agreement is too complex and too many options; Encapsulating Security Payload (ESP) and Authentication Header (AH) larger [7], leading to the low efficiency of the data payload under the limitation of the maximum transmission unit of the 6LoWPAN network; Intensity of DES security algorithm is too low, SHA-1, MD5 is difficult to ensure data security; Key establishment and management mechanism is complex, and application layer requirements are difficult to achieve on the node, lacked of support for multicast and broadcast. The IPsec header compression scheme for 6LoWPAN is proposed in the literature [8]. The proposed scheme uses the AES-CCM (advanced encryption key chain packet mode), the underlying IEEE 802.15.4 protocol support encryption, has low overhead, to provide message authentication and privacy features. AES-CCM mode is opposite to ESP, does not require plaintext padding. Using AES-CCM is only applicable to the ESP, and does not apply to the AH method, using only the EID value 101.AES-CCM with IPsec security encryption can be used in multi group encryption mode, including the CBC-MAC(Cipher Block Chaining Message Authentication Code) mode [9]. Literature [10] made a detailed security analysis of the 6LoWPAN fragmentation mechanism, identified the two kinds of attack methods in 6LoWPAN design level. The author proposes two countermeasures against such attacks, namely the content link method and the split cache method. Based on each slice, if the node is able to identify the attack node, it can resist the attack of copied slices, however, even the security of the link layer only supports group authentication. For different types of attacks, such as phishing, wormhole, trap, black holes, flooding, overloading and forgery, thesis [11] provides some preventive measures and solutions, forming the intrusion detection system using different parameters detected and appropriate factors.

Constrained Application Protocol (CoAP) has now been standardized by IETF, and is applied to the communication level of various applications of resource constrained devices. In order to protect the transmission of sensitive information safely, CoAP using the data transport layer security protocol as the underlying security protocol, to carry out authentication and trusted transmission. DTLs was originally designed for a strong performance of devices and high bandwidth network, Raza *et al.*, [12] proposed an integrating DTLs and CoAP networking solutions, which DTLs header compression can optimize network energy consumption. Pedro *et al.*, [13] described the feasibility of EAP/PANA in the Internet of things, and provides an interactive EAP/PANA protocol implementation for the device equipped with Contiki system, called PANATIKI. A proposed and evaluated a new 6LoWPAN compression authentication header (AH) and ESP security header [14]. So that IPv6 on IEEE 802.15.4 wireless communications are protected. Based on the overall structural characteristics of the network topology, Xu Ke *et al.*, [15] construct the source address verification scheme based on IPv6 architecture. Extracting the source address of the data packet received from the terminal node and carrying out the verification test to ensure the reliability of the data source address. In the

preliminary study, based on the Contiki system, an optimized and efficient mobile switching scheme is designed in [16]. Author improved the process of RPL topology creation and maintenance in 6LoWPAN, and integrated the parameters of received signal strength and delay, to achieve the pre-switch mechanism. Based on mobile handoff, we finish the control of node access, while the Internet host access to authentication. And the AES encryption algorithm is realized in 6LoWPAN communication to complete data encryption. In the software and hardware testing environment for the overall program evaluation, test results show that the overall design of the communication program can achieve the desired purpose of this paper.

3. Mutual Access Control of 6LoWPAN

The topology structure of 6LoWPAN network is mainly tree structure, and it has strong mobility. Data transmission is mainly concentrated in the terminal node and the aggregation node, in the mobile case is between the access node and the mobile node, between Internet of Things gateways and local networking node.

3.1. Access Control of IoT Local Node

For strategies of access after mobile handover in local networking, using different pan ID control access. In the same domain, pan ID is the same, so it can't affect the normal communication process, when switching between different domains, we can use mechanism of register and authentication.

In the protocol of 802.15.4, it's used a 16 bit identifier to distinguish different network domains. The following code is used for configuration and modifies:

```
/* RF configuration */
#define IEEE802154_CONF_PANID 0x5409 /* PAN ID is 0x5409*/
#ifndef CC2530_RF_CONF_CHANNEL
#define CC2530_RF_CONF_CHANNEL 25    /* channel is 25 */
#endif /* CC2530_RF_CONF_CHANNEL */
#ifdef IEEE802154_CONF_PANID
#define IEEE802154_PANID IEEE802154_CONF_PANID
#else
#define IEEE802154_PANID 0xABCD    /*if PAN ID is undefined,   use 0xABCD */
#endif
/* if source ID and destination ID is same,   set PAN ID as compression bit */
if(p->fcf.dest_addr_mode & 3 && p->fcf.src_addr_mode & 3 &&p->src_pid == p->dest_pid)
 {
      p->fcf.panid_compression = 1;
      flen->src_pid_len = 0;
}
else
{
      p->fcf.panid_compression = 0;
}
… …
```

In the process of networking, we firstly judge whether the PAN ID in the broadcast message is consistent with the source PAN ID, if it is consistent, then it is compressed, and the communication is carried out. In which the channel 25 and 0x5409 is the experiment channel and PAN ID default values. PAN ID can be set by setting the value of 0xFFFF, through the discovery mechanism of automatic network to achieve ID PAN automatic configuration.

3.2. Access Control in Pre-Shared Key Domain

We can use the pre-shared key method to realize access authentication, that is, use a fixed key in trusted nodes, and send a random string in the reply message. For the access nodes, using the same encryption algorithm and key to encrypt the string. When the access nodes received the message, decrypt the cipher text and compared it with random characters, if the same then allows the node to access the network, or the communication will be cancelled. The certification process is shown in Figure 1:

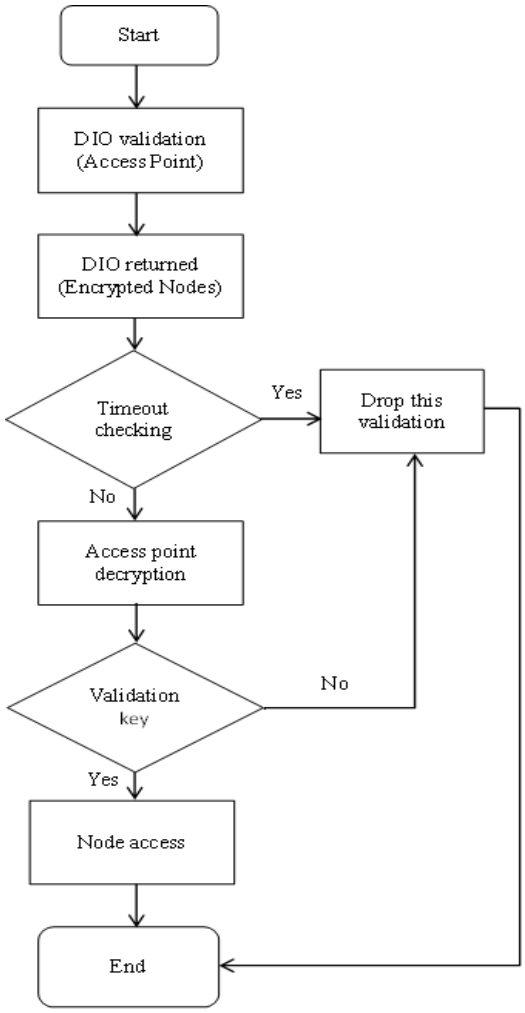


Figure 1. The Process of Access Authentication

To determine timeout operation, we should call timer of Contiki system and event driven timer, and set structure of timer, which contains the timer sequence, the timer pointer, time interval, and the calling process pointer. When the timer is timed out, the system will automatically call dropping function of the verification process, release memory and delete the corresponding stored string.

4. Encryption Algorithm of 6LoWPAN

4.1. Standard Encryption Algorithm

Authentication and MAC filtering can prevent malicious nodes connecting to the wireless network, but they cannot prevent them from blocking the data in transmission. If there are no secure encryption measures in data transmission process, the data will faced

with the risk of eavesdropping. Therefore, it is very necessary to carry out the transmission after encrypted data by using the appropriate encryption algorithm.

The comparison of several common encryption algorithms is shown in Table 1.

Table 1. The Comparison of Encryption Algorithm

Algorithm	Length	Speed	Security	Occupancy
DES	56bit	general	low	middle
3DES	56bit nesting	slow	high	high
IDEA	128bit	slow	high	high
RC4	variable	quick	lower	low
RC5	variable	variable	uncertainty	middle
AES	128bit,192bit, 256bit	quick	high	low

4.2. Encryption Algorithm of 6LoWPAN

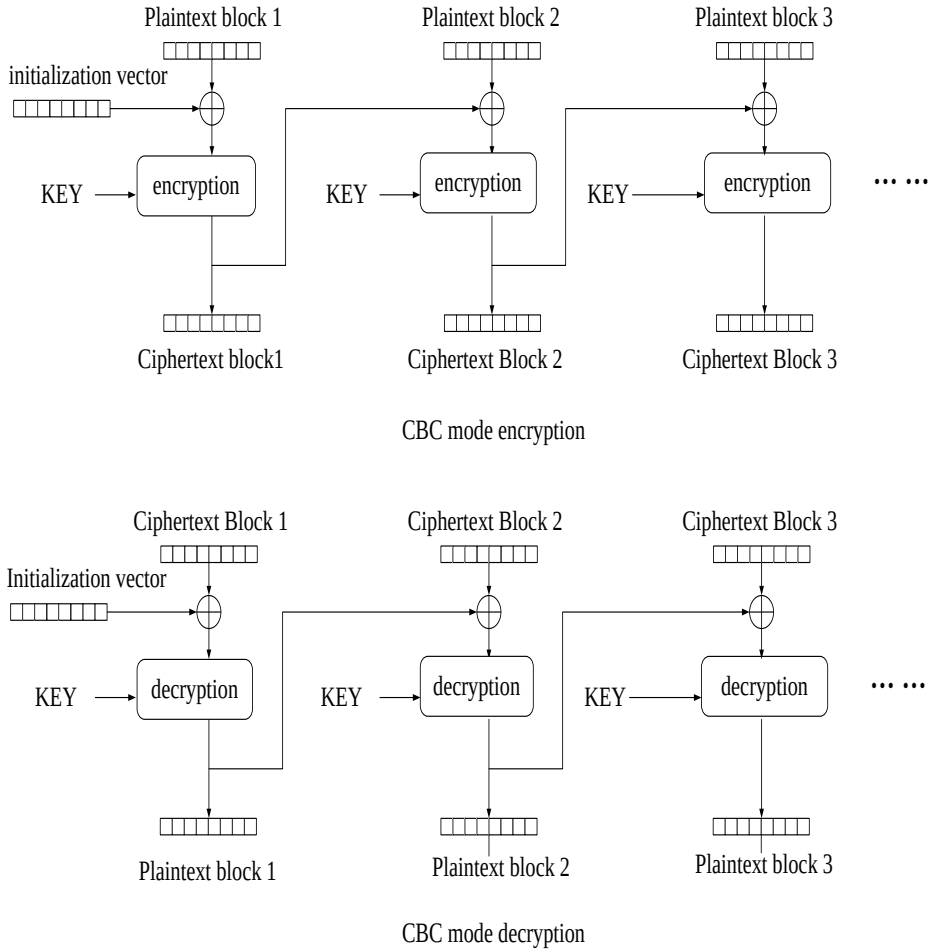


Figure 2. Encryption and Decryption Principle of AES-CBC Mode

The encryption and decryption method of CTR mode uses the stream key, which is beneficial to the parallel optimization of the operation. Random number, counter, and key are the parameters included in the CTR model. The random number and the count value can be regarded as a count value as a whole. As long as the algorithm selection is appropriate, the serial operation can be avoided.

CBC encryption principle:

Perform XOR the plaintext and the initialization vector, then, enforce encryption with the key. The resulting intermediate value will be used as the initialization vector for the next block.

CBC decryption principle:

For decrypting cipher text with key, Performing XOR the decrypted value and the initialization vector can get the plaintext.

In CBC mode, decryption is the inverse process of encryption. However, each data block encrypted in the encryption process is directly related to the previous generation of encrypted cipher text. Using UDP, 6LoWPAN network is faced to non-connected unreliable transmission. Therefore, if the packets are lost in the decryption process, will cause the risk that the decrypted plaintext is not in agreement with the encrypted plaintext, so the use of CTR mode is more reliable.

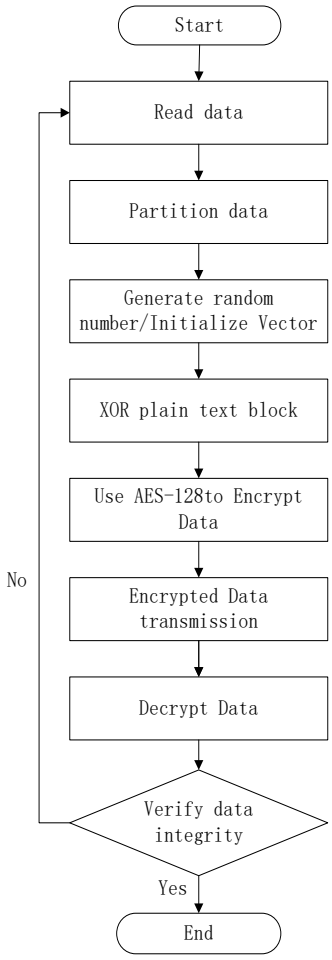


Figure 3. Encryption Process of Secure Communication

AES encryption processes in 6LoWPAN Communication is shown in Figure 3 specifically. According to the CC2530 data manual, CC2530 built-in random number generator, AES co-processor and the corresponding registers, which can provide resource sharing in cross layer? Compared to software implementation, the use of hardware assistance can effectively improve the efficiency of encryption and decryption, and reduce the operating pressure of the 8051 processor. Because of the AES co-processor can only

be used to handle an event at a time, so we need to configure some properties in the program for reasonable arrangements of resources.

Between the CPU and the coprocessor, Communication is realized with the following three SFR registers: Encryption control and status registers(ENCCS), Encrypt the input registers (ENCDI), Encrypt output register(ENCDO).

The starting position of the ENCCS register in the CC2530 is 0xB3, a total of 8 bits. Now set as shown in Figure 4.

0:ST	1-2:CMD[1:0]	3:RDY	4-6:MODE[2:0]	7:NULL

Figure 4. ENCCS Configuration

The first tag, ST, indicating that the startup process ID. The second tag, setting CMD start processing command. When ST is set to 1, 00, 01, 10 and 11, four values can take for tag2-3, represent the encryption blocks, decryption blocks, loading key and a random number or IV loading operation respectively. Tag4 indicates the decryption operation state, while the value is 0, that is running, a value of 1, said ready. Tag5-7 specify the current usage patterns, the use of 000 and 011 represent CBC mode and CTR mode respectively. Tag 8 is empty, filled by “0”.

5. System Testing and Performance Analysis

In system testing program, achieving deployment of the small test network topology, setting 6LoWPAN ordinary nodes and 6LoWPAN gateway in 6LoWPAN network domain area network and install Internet host node and gateway connecting then access it to 6LoWPAN network to test the connectivity and safety of the network. The network topology model of the test scheme is shown in Figure 5.

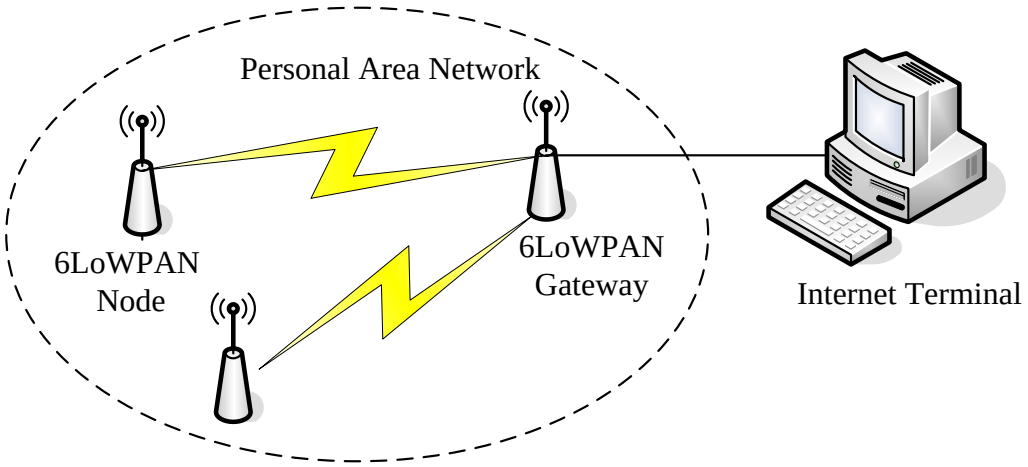


Figure 5. The Topology of System Testing

5.1. Access Control Testing

In the test of access control, the ID PAN and the channel value of the node are first configured, which are divided into two cases: the same PAN ID and the different PAN ID. In the first case, its domain switch authentication, you can achieve inter domain isolation, the nodes in the network of different inter domain deployment.

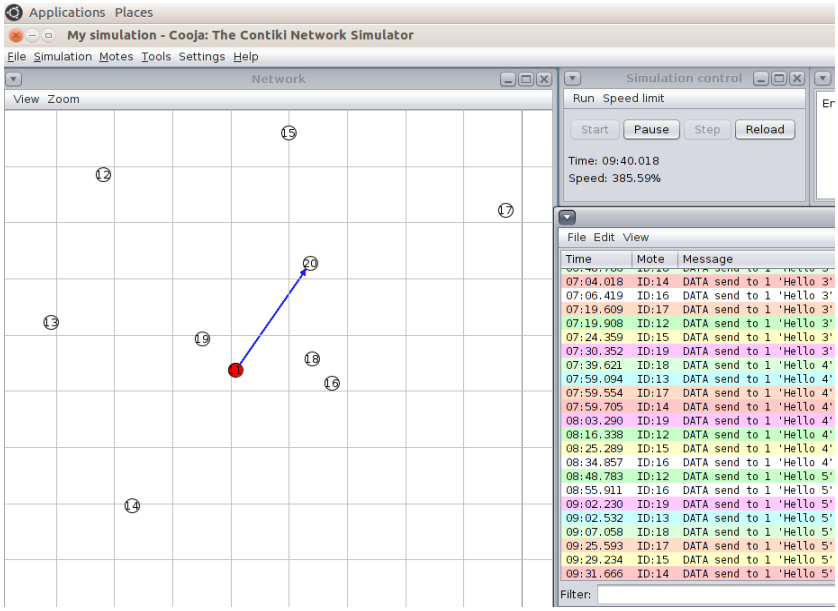


Figure 6. The Blocking of Normal Communication

Figure 6 shows the communication of multiple UDP client node and server node, and added the malicious nodes in the network, the malicious node by identifying the server node, and occupation the communication resources in a long-term, to prevent the other normal client nodes.

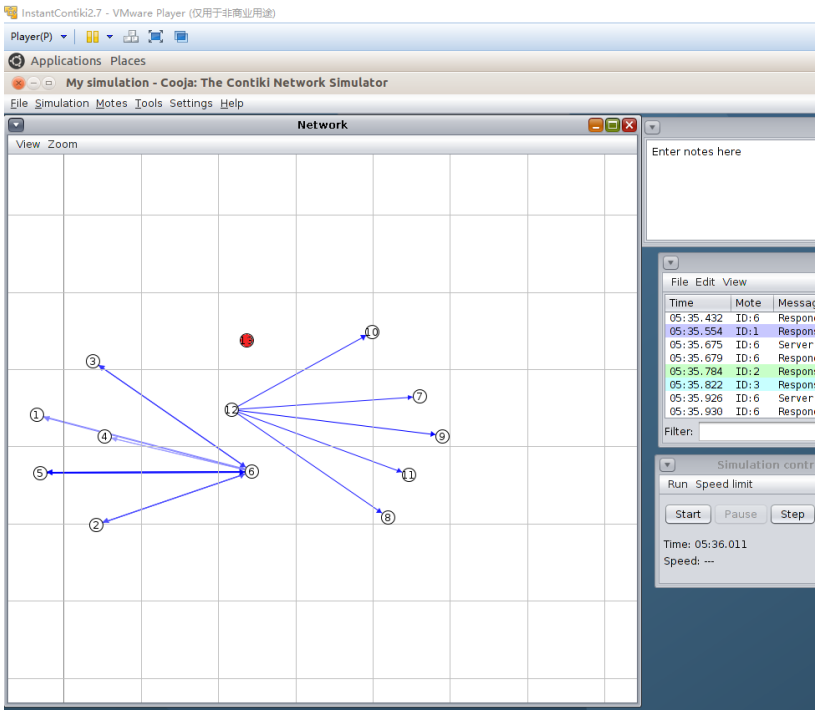


Figure 7. Access Control of Pre-Shared Key

Then add DIO, Dao nodes of RPL messages news into pre-shared key mechanism, using 128 bit AES CBC mode encryption. Without affecting the mobile switching efficiency, effectively limit the access authentication node. Print the current node status to the node output panel by calling the system print function make directly displayed refused

access request message possible. In Cooja, through the view option on the Network panel to open the traffic view between nodes, show as Figure 6.

The nodes in Figure 7 have the same pan ID and the same channel node and in good communication distance, which the node numbered 1 to 5, and 7 to 10 is UDP communications client, the node numbered 6 and 12 is server node. In the condition of not used authentication mechanism, the client node can communicate with any other server node. After use pre-shared key authentication, nodes can only communicate with the node use the same key authentication. Node 13 is the malicious node which initiates flooding attacks. In the authentication mechanism, the node can't join any network and can only initiate topology request broadcast message.

5.2. Mobility and Security Mechanism Testing

In the process of integration testing, add the authentication and encryption source code files to the project, encrypt before sending data, then sends the encrypted cipher text. After the node receives data packet, read the encrypted cipher text and decrypt according to the shared key. Finally, statistic the accuracy of encryption data transmission for validation, and comparison after add encryption algorithm, the differences in efficiency in 6LoWPAN network with before. With the effective data load transmitted in the unit time as evaluation index, compared with the data of 6LoWPAN node based on Contiki 2.7 in the same state. Test results are shown in Figure 9.

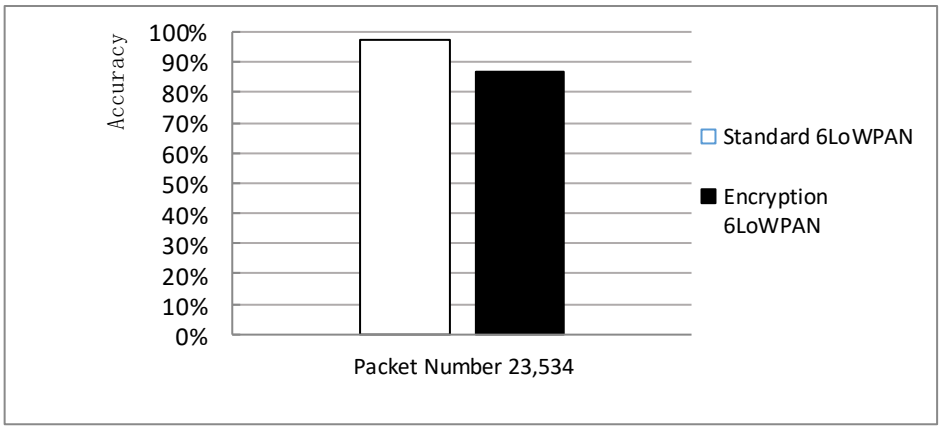


Figure 9. The Comparison of Data Transmission Accuracy Rate

In order to facilitate testing data transmission rate, it's useful to use simulator control network state and parameters, choose Cooja to simulate the network topology and mobility scenarios, import the encrypted node project file, and set the same time, tested 10 times for the two cases and taking the average value, the result shown in Figure 10.

Under the standard 6LoWPAN protocol, using resting mechanism and system timer time default, the data transmission rate close to 10 bytes per second, using encryption algorithm for data transmission, the average measured transmission rate is 917 bytes per second, the average rate drop about 5%, does not affect the normal communication of the 6LoWPAN network. It's in the normal fluctuation range in low-power wireless networks.

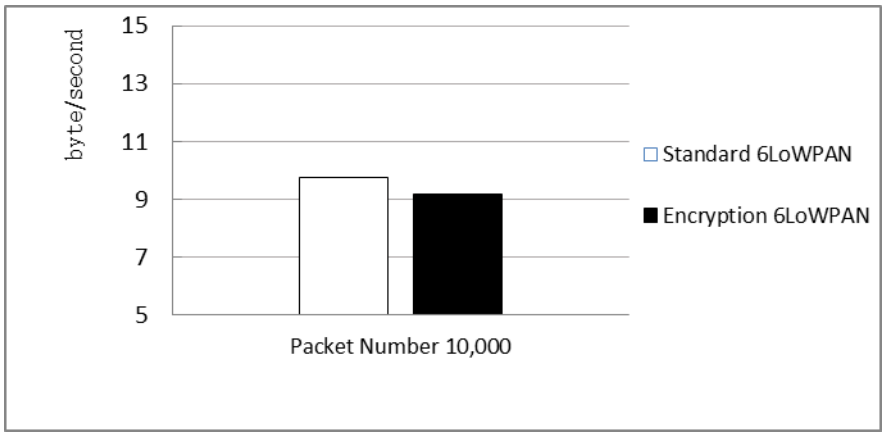


Figure 10. The Comparison of Node's Data Transmission Speed

6. Conclusion

In this paper, an encryption algorithm which is applicable in 6LoWPAN is designed, access authentication scheme and information security transmission function of 6LoWPAN network are proposed and implemented. In the process of 6LoWPAN node access authentication, using AES decryption of CBC mode, network data in the plaintext is encrypted. Using a pre-shared key authentication node can effectively isolate the malicious nodes outside the domain network. In the later data transmission process, using AES counter mode to send data block and encrypt. The performance and characteristics of standard data encryption algorithm are compared with the proposed data encryption, meanwhile, the data transmission of encryption algorithm is simulated, and the transmission accuracy and data throughput of proposed encryption algorithm is analyzed. In experiment, the feasibility of the control inter-domain access and pre-shared key authentication is tested. The results proved the proposed scheme can ensure the privacy of data without affecting the communication efficiency, so meet expected design goals.

Acknowledgment

This study is funded by the National Natural Science Foundation of China (#61373160).

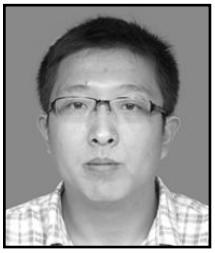
References

[1] J. W. Hui and D. E. Culler, "IP is dead, long live IP for wireless sensor networks", Proceedings of the 6th ACM conference on Embedded network sensor systems, ACM, **(2008)**, pp. 15-28.
[2] A. Terzis, S. Dawson-Haggerty, D. E. Culler, J. W. Hui and P. Levis, "Connecting low-power and lossy networks to the internet", Communications Magazine, IEEE, vol. 49, no. 4, **(2011)**, pp. 96-101.
[3] R. Wei, S. Jun, Y. Min and L. Yuliang, "Autonomous Security Adaptive Layer for IOT and T2T Anonymous Authentication Protocols in T2ToI", Computer Research and Development, vol. 48, no. z2, **(2011)**, pp. 320-325.
[4] L. Chuang and L. Lei, "Study on the next generation Internet architecture", Chinese Journal of Computers, vol. 30, no. 5, **(2007)**, pp. 693-711.
[5] Md. S Hossen, A. F. M. Sultanul Kabir, R. Hayat Khan and A. Azfar, "Interconnection between 802.15.4 Devices and IPv6: Implications and Existing Approaches", International Journal of Computer Science Issues, vol. 7, no. 1, **(2010)**, pp. 19-31.
[6] N. Doraswamy and D. Harkins, "IPSec: The new security standard for the Internet, intranets, and virtual private networks", Prentice Hall Professional, **(2003)**.
[7] Y. Zhang, X. Chen, J. Li and H. Li, "Generic construction for secure and efficient handoff authentication schemes in EAP-based wireless networks", Computer Networks, vol. 75, **(2014)**, pp. 192-211.
[8] K. Rantos, A. Papanikolaou, C. Manifavas and I. Papaefstathiou, "IPv6 security for low power and lossy networks", Wireless Days (WD), **(2013)**, IFIPIEEE, 2013, pp. 1-8.
[9] W. Zhao, and Z. Zhao, "Research on engineering software data formats conversion network", Journal of Software, vol. 7, no. 11, **(2012)**, pp. 2606-2613.

[10] R. Hummen, J. Hiller, H. Wirtz, M Henze, H. Shafagh and K. Wehrle, "6LoWPAN Fragmentation Attacks and Mitigation Mechanisms", Proceedings of the sixth ACM conference on Security and privacy in wireless and mobile networks, **(2013)**, pp. 55-66.
[11] A. Rghioui, A. Khannous and M. Bouhorma, "Denial-of-Service attacks on 6LoWPAN-RPL networks: Issues and practical solutions", Journal of Advanced Computer Science & Technology, vol. 3, no. 2, **(2014)**, pp. 143-153.
[12] S. Raza, H. Shafagh, K. Hewage, R. Hummen and T. Voigt, "Lithe: Lightweight Secure CoAP for the Internet of Things", Sensors Journal, IEEE, vol. 13, no. 10, **(2013)**, pp. 3711-3720.
[13] M. S. Pedro, M. L. Rafa and A. F. G. Skarmeta, "PANATIKI: a network access control implementation based on PANA for IoT devices", Sensors, vol. 13, no. 11, **(2013)**, pp. 14888-14917.
[14] J. Granjal, E. Monteiro and J. Sa Silva, "Enabling Network-Layer Security on IPv6 Wireless Sensor Networks", Global Telecommunications Conference (GLOBECOM 2010), IEEE, **(2010)**, pp. 1-6.
[15] H. Guangwu, C. Wenlong and X. Ke, "A distributed network source address authentication scheme based on IPv6", Chinese Journal of Computers, vol. 35, no. 3, **(2012)**, pp. 518-528.
[16] H. Bingchao, D. Shuling and F. Tongrang, "Neighbor discovery and integration of the Internet of things", Journal of the Hebei Academy of Sciences, vol. 31, **(2014)**, pp. 74-78.

Authors

Fan Tong-rang, born in 1965, Professor. Ph.D. School of Information Science and Technology, Shijiazhuang Tiedao University. Her main research interest includes network technology and Information processing. Email address: fantr@stdu.edu.cn; fantr2009@126.com.



Zhao Wen-bin, born in 1985, Ph.D. School of Information Science and Technology, Shijiazhuang Tiedao University. His major field of study is network technology and information processing. Email address: zhaowb.email@qq.com.

