Compression Method for IPSec over 6LoWPAN

Huqing Wang[1,2], **Zhixin Sun**[3]
[1] College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing 210003, China
[e-mail: wanghuqing@njupt.edu.cn]
[2] College of Communication and Information Engineering, Nanjing University of Posts and Telecommunications, Nanjing 210003, China
[3] Key Laboratory of Broadband Wireless Commnunication and Sensor Network Technology, Ministry of Education (Nanjing University of Posts and Telecommunications), Nanjing 210003,China
*Corresponding author: Huqing Wang

Received January 8, 2017; revised November 21, 2017; accepted December 10, 2017; published April 30, 2018

Abstract

This paper focuses on a header compression method for the Authentication Header (AH) and Encapsulation Security Payload (ESP) for application to 6LoWPAN. Based on the context, an extendible compression method is developed by analysing each field of the AH and ESP. The method is carried out by resetting the AH and ESP header compression formats, adding a MOD field, and setting different working modes. Authentication, encryption, and a mixture of certification and encryption are provided as flexible options. In addition, the value of the original IPv6 extensible header ID (EID) field can be retained, while the number of occupied NHC_ID values can be decreased for future extendibility. The experimental results show the feasibility and validity of the current compression method. By comparison with other solutions, the new mechanism is demonstrated to be advantageous in terms of compression ratio, flexibility and extendibility.

Keywords: 6LoWPAN, IPSec, WSN

http://doi.org/10.3837/tiis.2018.04.023 **ISSN : 1976-7277**

1. Introduction

With wireless sensor networks (WSNs) being applied for sensitive information transmission in some areas, such as military, medical treatment, intelligent building and industrial control, network security must be considered to ensure the security of the network and data transmission. The IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) adaptation layer is an intermediate layer between the network layer and the MAC layer. 6LoWPAN is an efficient extension of IPv6 into the wireless embedded domain that enables end-to-end IP networking and features for a wide range of embedded applications [1]. It mainly solves the problem of excessive IPv6 data package headers, which must be compressed, and facilitates the fragmentation and reassembly of the IPv6 data package on IEEE802.15.4 to better conform to the IEEE802.15.4 standard. Sensor nodes that use 6LoWPAN can directly communicate with IPv6-enabled hosts and, for example, sensor data processing can be performed by standard servers. Thus, 6LoWPAN greatly simplifies the operation and integration of WSNs in existing IT infrastructures. To defend against data collection and dissemination of private information by an attacker, the 6LoWPAN working group has focused on security since its establishment [2]. IP Security (IPSec) defines AH and ESP. AH provides data integrity and authentication, while ESP provides data confidentiality, integrity and authentication. IPSec belongs to the mandatory configuration for IPv6 and can achieve end-to-end security protection. In addition, the IPSec security protocol is already available to IPv6-enabled Internet hosts.

This paper presents a new IPSec protocol for the header compression mechanism applied to 6LoWPAN. The method is carried out by resetting the AH and ESP header compression formats, adding a MOD field, and setting different working modes. The proposed protocol provides authentication, encryption, and a mixture of certification and encryption as flexible options. In addition, the value of the original IPv6 extensible header ID (EID) field can be retained, while the number of occupied NHC_ID values can be reduced for future extendibility. The experimental results show the feasibility and validity of the proposed compression mechanism. By comparison with other solutions, the proposed mechanism is demonstrated to be advantageous in terms of compression ratio, flexibility and extendibility.

The paper is organized as follows. Section 2 describes related work regarding existing security solutions for 6LoWPAN networks. Section 3 introduces background knowledge on IPSec and 6LoWPAN. Section 4 presents the IPSec-based 6LoWPAN solution, including the AH and ESP protocol header compression method. Experimental results are presented in Section 5. Finally, future trends are forecasted in Section 6.

2. Related Work

A secure network environment can promote the development of application fields. The key security technology of 6LoWPAN has become an overarching concern for scholars worldwide. Methods for securing communications in low-power nodes can be applied to several layers of the TCP/IP stack: each has its own advantages and drawbacks. In the link layer, two common security methods are the Access Control List (ACL) [3] and pre-defined security suite. In the former, only nodes in the ACL are considered credible nodes and data frames from these nodes can be received, whereas data frames from other nodes will be filtered. This method can provide only limited secure service and does not guarantee the confidentiality of the network.

Furthermore, every device must maintain its own ACL and there is no perfect method for maintaining the ACL, especially in a power-loss state. A pro-defined security suite can ensure confidentiality, message integrity and access control. However, key management is difficult such methods [4]. Many scholars have investigated shared keys to solve this problem in the data link layer. However, for WSNs, this approach results in new problems, such as difficulty in resisting replay attacks from stolen equipment. Transport Layer Security (TLS) is used to provide confidentiality and verify data integrity between two communication applications. The compression algorithm, encryption algorithm and message authentication algorithms used can be designated through the TLS connected state. High-level protocols can be transparently distributed over TLS. However, TLS is generally used over the reliable Transmission Control Protocol (TCP), and in a resource-constrained WSN, the transport layer uses the User Datagram Protocol (UDP) instead of TCP. Datagram Transport Layer Security (DTLS) attempts to expand the existing TLS framework to make it compatible with UDP [5]. However, DTLS has not yet been satisfactorily deployed and cannot be widely used at present. Some scholars have proposed applications of intrusion detection systems [6], but no detail intrusion detection method suitable for 6LoWPAN currently exists.

The methods discussed above play a role in promoting 6LoWPAN security. However, they cannot be widely used because they are difficult to implement. Therefore, more attention has focused on the network layer.

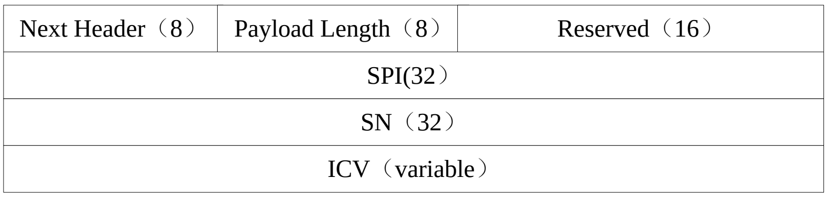
IPSec, as a standard component of IPv6 security, provides three kinds of protection for the network layer: authentication, data integrity and confidentiality through AH, ESP, and Internet Key Exchange (IKE), respectively. With 6LoWPAN, WSN and traditional IP networks are more tightly integrated. Therefore, it is natural to research how to inherit and realize IPSec in 6LoWPAN. Granjal [7] and Raza [8] extended a header compression method for the AH and ESP protocols to the 6LoWPAN adaptation layer and analysed its influence on data transmission rates when using encryption algorithms such as AES, 3DES, SHA1 and SHA2. Granjal's secure compression scheme is based on LOWPAN_HC1, while Raza's is based on LOWPAN_IPHC. For different network topologies, using different compression schemes in different sensor nodes increases the code complexity [9]. Moreover, due to resource constraints, some nodes may load only a specific compression scheme to reduce the amount of embedded code. However, this will affect the interconnections between nodes. Considering that LOWPAN_HC1 is highly effective for link-local unicast communication, but insufficient for most practical uses of IPv6 in 6LoWPAN, while LOWPAN_IPHC supports multicast routing and can effectively compress the global routing address and the multicast address, a new compression scheme based on LOWPAN_IPHC is proposed in this paper. In the plan that was proposed by Raza, NHC_ID is set to different values when compressing the AH and ESP header and the remaining two values of EID are occupied: 5 for AH and 6 for ESP. To reduce the occupations of EID and NHC-ID, on the basis of the development trend of investigating the use of the protocol field in IPv6, in this paper, we propose a new AH and ESP header compression scheme. The scheme is carried out by resetting the AH and ESP header compression formats, increasing the MOD field, and setting different working modes. It provides users with flexible selections of authentication and encryption, or a mixture of certification and encryption. In addition, the original EID value of 6 can be retained and the number of occupied NHC_ID values can be reduced for extensive future use.

3. Background

IPSec is an Internet security protocol that works in the network layer to protect IP security, which was proposed by the international organization IETF. IPSec provides encryption and /or authentication for all traffic, so that the upper-layer application can be protected. When a firewall or router uses IPSec, the user's system and the server system do not require any changes. Even if the terminal system uses IPSec, the upper-layer software and application are not affected. IPSec belongs to the mandatory configuration of IPv6. Since it was first proposed in 1995, it has become more mature. The research of Granjal *et al*. shows that IPSec has good application prospects in WSNs [10].

3.1 AH and ESP

IPSec contains two secure protocols: AH and ESP. Fig. 1 shows the AH format.



Next Header（8）	Payload Length（8）	Reserved（16）
SPI(32）		
SN（32）		
ICV（variable）		

Fig. 1. AH Format

The sequence number (SN) is 32-bit unsigned integer that can be used to resist replay attacks. When a new security association (SA) is established, the sequence number counter is initialized to 0. The sender increments the sequence number counter for this SA and inserts the low-order 32 bits of the value into the SN field. The SN value increases by one for each package sent. The authentication data are a variable-length field, and the total length must be an integral multiple of 32 bits whose specific value is the Message Authentication Code (MAC) produced by the selected authentication algorithm. Using this field, data integrity authentication can be achieved. However, AH does not provide confidentiality.

Fig. 2 shows the ESP format.

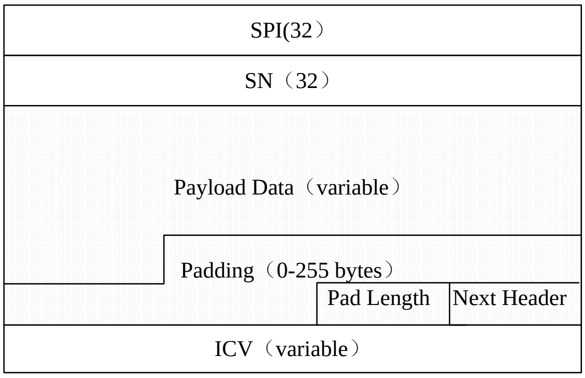


Fig. 2. ESP Format

ESP provides confidentiality, including encryption of the message and the traffic limit. Generally, low-computational-complexity encryption algorithms (such as symmetric cryptography algorithms) are selected. As an optional feature, ESP can also offer authentication and anti-replay-attack capacity, such as AH.

In addition to the overlapping functions of data integrity maintenance and defence against replay attacks, ESP can provide confidentiality. This paper combines AH with ESP when implementing IPSec compression in the 6LoWPAN network.

3.2 Transport mode and tunnel mode

AH and ESP have two working modes: transport mode and tunnel mode. Transport mode provides end-to-end security services, as shown in **Fig. 3**, while tunnel mode provides end-to-middle security services, as shown in **Fig. 4.**

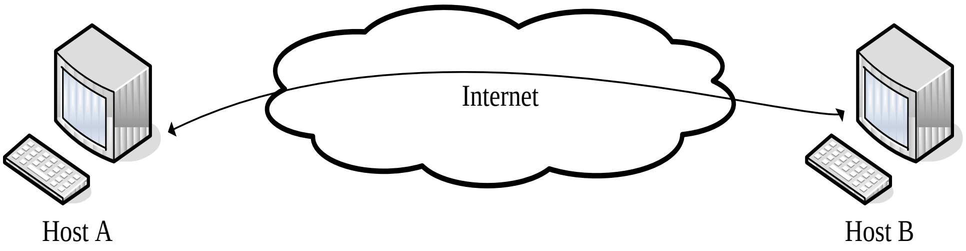


Fig. 3. End-to-End Security

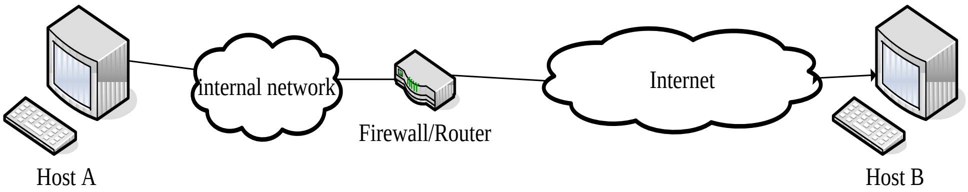


Fig. 4. End-to-Middle Security

In transport mode, two terminal nodes can be in the same internal network or in external networks. As long as the two terminals share a protected key, the AH authentication and ESP encryption processes are secure. The application scenarios of tunnel mode generally consist of the following: (1) the remote terminal provides their identities to the firewall; (2) the remote terminal accesses the internal network; and (3) the requested server does not support IPSec services. The protection target in AH is the payload, while in ESP, it is the entire IP packet.

Transport mode provides IPSec service for all applications, thereby simplifying the security operation of the application layer. This working mode is also efficient. The CPU cost can be reduced with a small increase in the IP data package length. However, transport mode is unable to resist traffic analysis. In tunnel mode, the original IP header, including the destination address, is encapsulated, so that intermediate routers cannot obtain the destination address. To supply sufficient information to routers, a new IP header is placed in front of the original IP data package. This results in low efficiency, which is impractical in the context of 6LoWPAN. However, tunnel mode can resist flow analysis based on the destination address. Tunnel mode operates between the external host and a security gateway or between two security gateways. The internal host burden can be reduced and the key distribution task can be simplified by reducing the number of required keys.

Based on this analysis, tunnel mode increases the data package length. Considering the maximum transmission unit (MTU) in the 6LoWPAN frame, this paper focuses on the compression application of IPSec transport mode in 6LoWPAN.

4. IPSec compression over 6LoWPAN

An important characteristic of 6LoWPAN is the load size limitation provided by the underlying protocol IEEE 802.15.4. The MTU under IEEE 802.15.4 is 127 bytes, which includes the control field and security header, so the data payload is more limited. The fixed header of IPv6 is 40 bytes and the upper-layer protocol header (such as UDP or TCP) occupies a limited space; therefore, the rest of the data load is smaller. Only 81 bytes are available for transmitting data on the Internet into an IEEE 802.15.4 frame. Some large datagrams can be transferred by segmentation and reassembly over the lower-layer protocol. However, in the 6LoWPAN network, packing an entire IPv6 package into one IEEE 802.15.4 frame would be highly efficient. Although some segmentation is normal, massive data segmentation will lead to higher battery consumption and occupy the limited transmission tunnel of IEEE 802.15.4. Therefore, datagram compression is particularly important.

4.1 IPSec compression scheme over 6LoWPAN

This section proposes an extensible compression scheme for IPSec over 6LoWPAN. The process diagram of the proposed compression scheme is shown in **Fig. 5.** When an IP packet is received, based on demand, the scheme defines the format of IPSec header compression encoding and adds the MOD field to set different working modes.

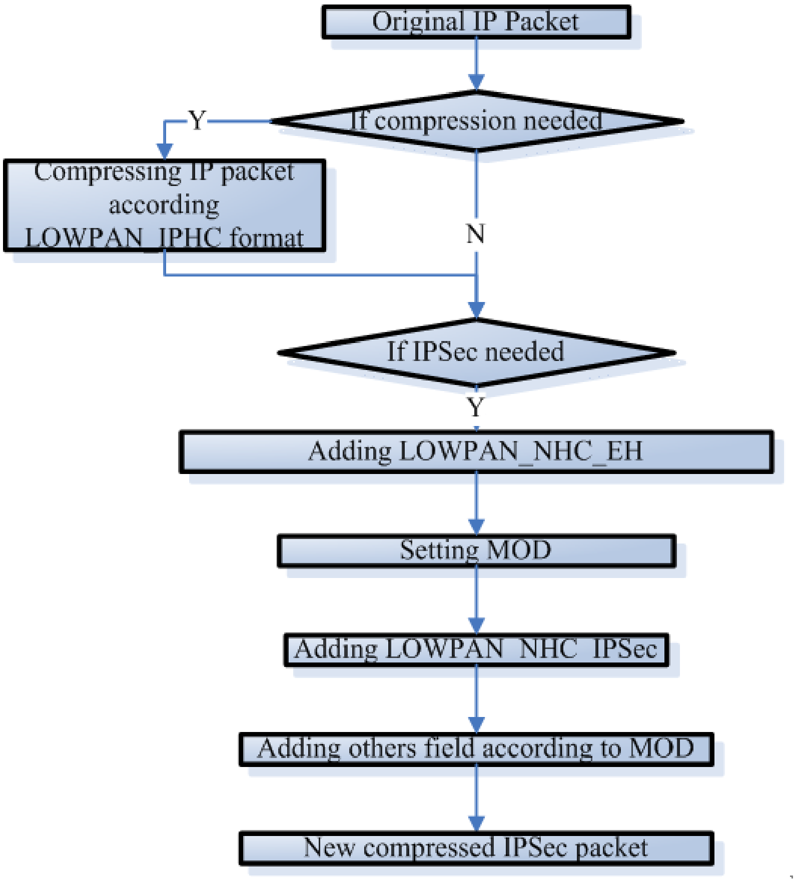

Original IP Packet
If compression needed
Y
Compressing IP packet according LOWPAN_IPHC format
N
If IPSec needed
Y
Adding LOWPAN_NHC_EH
Setting MOD
Adding LOWPAN_NHC_IPSec
Adding others field according to MOD
New compressed IPSec packet

Fig. 5. Compression Process

RFC6282 [11] two proposes context-aware header compression mechanisms: the LOWPAN_IPHC encoding for IPv6 header compression and the LOWPAN_NHC encoding for the next-header compression. The LOWPAN_NHC encoding is shown in **Fig. 6**.

NHC-ID(variable）	Next Header

Fig. 6. LOWPAN_NHC Encoding

In particular, the previously defined NHC encoding format for IP extension headers is shown in **Fig. 7**.

1110	EID	NH

Fig. 7. LOWPAN_NHC_EH

LOWPAN_NHC_EH can be used to encode both AH and ESP extension headers. NHC encodings for the IPv6 Extension Headers consist of an NHC octet, where three bits (bits 4, 5, 6) are used to encode the EID. There are eight possible values for the EID, but six are specified by RFC6282. The remaining two slots (101 and 110) are currently reserved. As we combine AH and ESP, it makes sense to use one of these unassigned slots. We propose using reserved slot 101 for the IPSec, AH, ESP or combined AH and ESP header. The newly increased MOD field will distinguish these headers from one another.

Definition 1: IPSec header compression encoding LOWPAN_NHC_IPSec:

1101	MOD	SPI	NH

Fig. 8. LOWPAN_NHC_IPSec

The first four bits in LOWPAN_NHC_IPSec represent the NHC-ID. These are set to 1101 to define IPSec.

When MOD = 00, the slot is reserved. When MOD=01, authentication-only mode is selected. If MOD=10, encryption-only mode is selected. When MOD=11, the authentication and encryption combined mode is selected.

When SPI=0, the default SPI for the sensor network is used and the SPI field is omitted. When SPI=1, every node has its own preferred security association (SA) and the SPI is carried inline; this does not mean that all nodes use the same SA.

When NH=0, the next header field in AH or ESP will be used to specify the next header and is carried inline, and when NH=1: the next header field in AH or ESP is skipped, and the next header will be encoded using LOWPAN_NHC.

4.2 Different compression modes of MOD

1. Authentication mode

When MOD is set to 01, it works in AH authentication mode. The compression scheme is similar to that proposed in [8]. Ideally, the AH can be compressed from 24 bytes to 16 bytes, including LOWPAN_NHC_EH (1 byte), LOWPAN_NHC_IPSec (1 byte), SN (2 bytes) and authentication data (ICV) (12 bytes). The compression ratio can be up to 1/3.

2. Encryption mode

When MOD is set to 10, it works in ESP encryption mode. As shown in the shaded part of **Fig. 2**, ESP already provides encryption for the Payload Data, Padding, Pad Length and Next Header fields. Therefore, these fields cannot be compressed in the 6LoWPAN layer. These fields are always carried inline. Ideally, the compressed ESP header includes the following fields: LOWPAN_NHC_EH (1 byte), LOWPAN_NHC_IPSec (1 byte), SN (2 bytes), Payload Data (variable length), Padding (0~255 bytes), Pad Length (1 byte), and Next Header field (1 byte). Thus, its size can be decreased by 4 bytes.

3. Hybrid authentication-encryption mode

When MOD is set to 11, it works in hybrid authentication-encryption mode. Ideally, the compressed IPSec header includes the following fields: LOWPAN_NHC_EH (1 byte), LOWPAN_NHC_IPSec (1 byte), SN (2 bytes), Payload Data (variable length), Padding (0~255 bytes), Pad Length (1 byte), Next Header field (1 byte) and authentication data (ICV) (12 bytes). Thus, its size can be decreased by 4 bytes.

4.3 Necessity of setting MOD

The next header field in the original IPv6 is omitted in RFC6282 and the NH field in LOWPAN_IPHC indicates whether the next header is encoded using LOWPAN_NHC. In **Fig. 6**, the variable length of NHC_ID is determined by the perceived frequency with which that format is used. However, the numbers of NHC_ID bits and any remaining encoding bits should respect the octet alignment. For example, NHC_ID for UDP is set to 11110, which is 5 bits and NHC_ID for the extensible header is set to 1110, which is 4 bits. The next header in IPv6 has 8 bits, with values from 0 to 255. This field identifies the next-level protocol, including the IPv6 extension header. Several values have been assigned; the unassigned values are quite limited. RFC 1700 [12] shows the detailed assignment:

0 reserved;

1~54 assigned;

55~60 unassigned;

61~100 assigned;

101~254 unassigned;

255 reserved.

The total number of unassigned values is 160 and the number of assigned values is 96, which is 37.5% of the total number of values. By 2017, Ref. [13] shows that the assigned numbers have increased substantially:

0~142 assigned;

143~252 unassigned;

253~254 for testing;

255 reserved.

The total number of unassigned values is 110 and the number of assigned values is 146, which is 57.03% of the total.

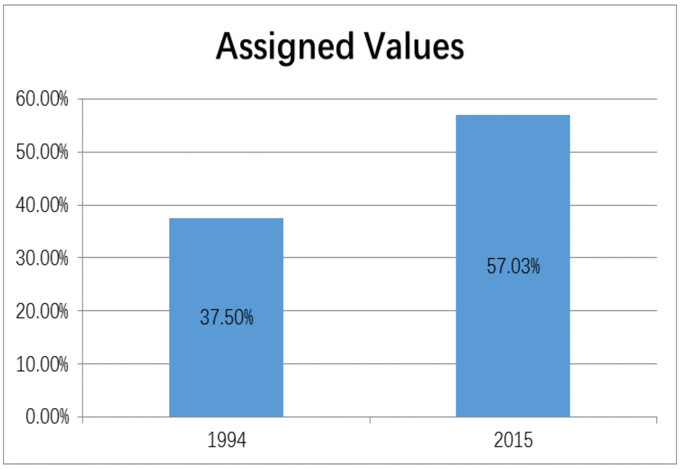


Fig. 9. Ratios of Assigned Values

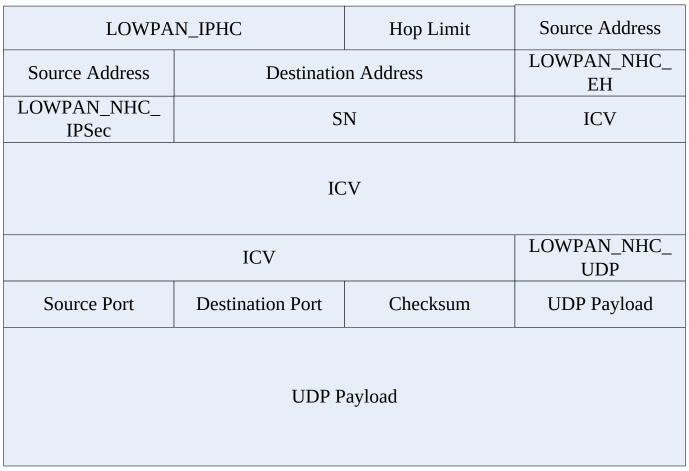
RFC6282 makes a specific provision for the EID. Three bits are used to encode the EID, with eight possible values, from 0 to 7. Six are specified and the remaining two (101 and 110) are reserved.

Based on the above analysis, when studying the IPSec compression scheme for 6LoWPAN, we should consider the situation in which NHC_ID and EID may run out of possible values. In the future, we should reduce the occupancy of these values.

5. Implementation and Analysis

5.1 Implementation and Experimental Setup

To evaluate the effect of the new IPSec compression scheme for 6LoWPAN, a simulation is conducted using the Contiki system in the Cooja environment. Two sky-type wireless sensor network nodes are set up to conduct simple UDP communications, and IPSec is employed in the network layer for security. We define MOD as 01. The compressed UDP data package with the AH authentication protocol is as follows.



LOWPAN_IPHC		Hop Limit	Source Address
Source Address	Destination Address		LOWPAN_NHC_ EH
LOWPAN_NHC_ IPSec	SN		ICV
ICV			
ICV			LOWPAN_NHC_ UDP
Source Port	Destination Port	Checksum	UDP Payload
UDP Payload			

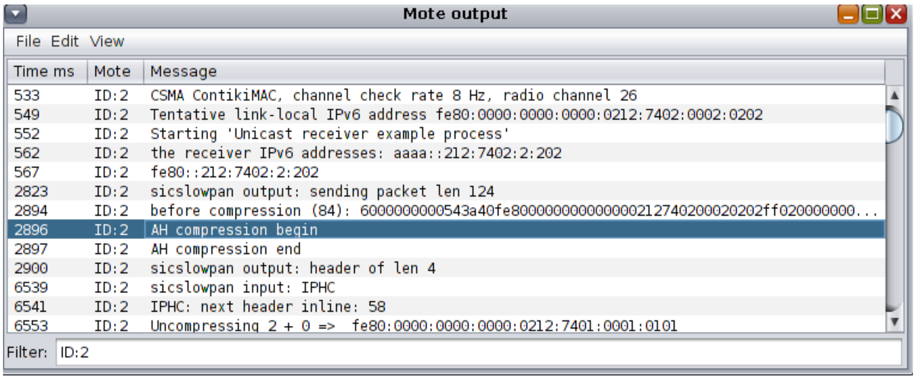
Fig. 10. A Sample NHC Compressed UDP Packet, Secured with AH

According to Fig. 7, we define LOWPAN_NHC_EH:

#define LOWPAN_NHC_EH 0Xeb

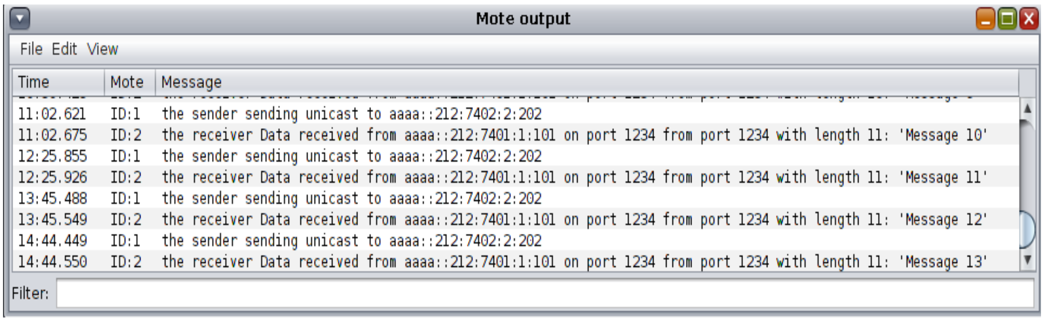
SHA1 is used for authentication in AH.

After AH compression, two nodes can transmit data successfully. Fig. 11 and Fig. 12 show the experimental processes.



```
Time ms  Mote  Message
533      ID:2  CSMA ContikiMAC, channel check rate 8 Hz, radio channel 26
549      ID:2  Tentative link-local IPv6 address fe80:0000:0000:0000:0212:7402:0002:0202
552      ID:2  Starting 'Unicast receiver example process'
562      ID:2  the receiver IPv6 addresses: aaaa::212:7402:2:202
567      ID:2  fe80::212:7402:2:202
2823     ID:2  sicslowpan output: sending packet len 124
2894     ID:2  before compression (84): 6000000000543a40fe800000000000000212740200020202ff020000000...
2896     ID:2  AH compression begin
2897     ID:2  AH compression end
2900     ID:2  sicslowpan output: header of len 4
6539     ID:2  sicslowpan input: IPHC
6541     ID:2  IPHC: next header inline: 58
6553     ID:2  Uncompressing 2 + 0 =>  fe80:0000:0000:0000:0212:7401:0001:0101
```

Fig. 11. Experimental Process A



```
Time       Mote  Message
11:02.621  ID:1  the sender sending unicast to aaaa::212:7402:2:202
11:02.675  ID:2  the receiver Data received from aaaa::212:7401:1:101 on port 1234 from port 1234 with length 11: 'Message 10'
12:25.855  ID:1  the sender sending unicast to aaaa::212:7402:2:202
12:25.926  ID:2  the receiver Data received from aaaa::212:7401:1:101 on port 1234 from port 1234 with length 11: 'Message 11'
13:45.488  ID:1  the sender sending unicast to aaaa::212:7402:2:202
13:45.549  ID:2  the receiver Data received from aaaa::212:7401:1:101 on port 1234 from port 1234 with length 11: 'Message 12'
14:44.449  ID:1  the sender sending unicast to aaaa::212:7402:2:202
14:44.550  ID:2  the receiver Data received from aaaa::212:7401:1:101 on port 1234 from port 1234 with length 11: 'Message 13'
```

Fig. 12. Experimental Process B

5.2 Memory Footprint

We use the SHA1 and AES implementations for AH and ESP, respectively. The ROM and RAM footprints of our new IPSec implementation are listed in Table 1.

Table 1. Memory Footprint

System	ROM footprint (KB)		RAM footprint (KB)	
	overall	overhead	overall	overhead
Without IPSec	33.1	----	8.1	----
AH with HMAC-SHA1-96	36.9	3.8	9.0	0.9
ESP with AES-CBC	41.5	8.4	8.5	0.4

5.3 Analysis of the proposed scheme

According to the experimental results, the correctness and feasibility of this scheme are confirmed. Next, it is compared with Ref. [7] and Ref. [8] to analyse the characteristics of the scheme, as shown in **Table 2.**

Table 2. Performance Comparison

	Ref. [7]	**Ref. [8]**	**Proposed scheme**
Compression theory	LOWPAN_HC1	LOWPAN-IPHC	LOWPAN-IPHC
IPSec working mode	transport and tunnel mode	transport mode	transport mode
Whether ESP and AH are combined or not	NO	NO	YES
NHC_ID	Not mentioned	AH and ESP take values 1101 and 1110, respectively	AH combined with ESP takes one value: 1101
EID scalability	——	AH and ESP take values 5 and 6, respectively, all EID values are used	AH combined with ESP, which is set to 5, retains the EID value of 6 for future extensions
Header compression ratio（AH）	30.7%	33.3%	33.3%

By comparison, the following main characteristics of this scheme are identified:

（1）It adopts the latest LOWPAN-IPHC compression theory, and the next header adopts the LOWPAN_NHC compression theory. LOWPAN-IPHC can support multicast routing, whereas the improved LOWPAN_HC1 compression scheme cannot effectively compress the global routing address and multicast address, and therefore, it cannot be used for the LOWPAN networks and Internet applications involving mutual visits. LOWPAN_NHC can support any next header, whereas improved LOWPAN-HC2 compression theory only supports UDP, TCP and ICMPv6, and cannot support other types of expandable headers.

（2）It selects IPSec transmission mode to reduce the amount of data traffic.

（3）It combines AH with ESP, because they have some functional overlaps. According to the provisions of RFC6282, the NHC_ID field, which is used to compress next protocol header, should be set to 1101 and take one value.

（4）According to the provisions of RFC6282, EID values 5 and 6 are not used. In this paper, EID values 5 and 6 are also reserved for future extensions.

In conclusion, this scheme maintains a high compression ratio, which is no less than that of Ref. [8]. In addition, it provides users with the convenience of freely choosing security solutions and improves the extensibility.

6. Conclusions

WSNs will be an integral part of the Internet, and IPv6 and 6LoWPAN are the protocol standards that are expected to be used in this context. IPSec is the standard method for securing Internet communications. The security problem stemming from the use of 6LoWPAN with IPSec in the network layer is discussed in this paper. We proposed a new AH and ESP header compression scheme. Through simulation experiments, the new scheme is demonstrated to be feasible and valid. Compared with other schemes, it shows superior performance, a high compression ratio, and is more flexible and scalable.

In future work, we plan to investigate a lightweight key management protocol for IPSec-6LoWPAN.

Acknowledgments

This research was supported by the National Natural Science Foundation of China under Grant (No. 61373135, 61170276, 60973140), the Major Natural Science Foundation of the Jiangsu Higher Education Institutions of China (No. 12KJA520003), the Natural Science Foundation of Jiangsu Province under Grant (No.BK2009425), the construction project of Jiangsu Province advantage discipline “Information and Communication Engineering”.

References

[1] PE. Figueroa, JA. Perez and I. Amezcua, “Performance evaluation of lightweight and secure protocol for wireless sensor networks: A protocol to enable Web services in IPv6 over low-power wireless personal area networks,” *International Journal of Distributed Sensor Networks*, Vol. 13, No, 6, pp. 1-8, Jun 2017. Article (CrossRef Link)

[2] C. Hennebert and JD. Santos, “Security Protocols and Privacy Issues into 6LoWPAN Stack: A Synthesis”, *IEEE Internet of Things Journal*, Vol. 1, No. 5, pp. 384-398, Oct 2014. Article (CrossRef Link)

[3] Chang S Y and Hu Y C, “SecureMAC: Securing Wireless Medium Access Control Against Insider Denial-of-Service Attacks,” *IEEE Transactions on Mobile Computing*, Issue: 99, Apr 2017. Article (CrossRef Link)

[4] H. Nicanfar, P. Jokar, K. Beznosov and VCM Leung, “Efficient Authentication and Key Management Mechanisms for Smart Grid Communications,” *IEEE Systems Journal*, Vol. 8, No, 2, pp. 629-640, Jun 2014. Article (CrossRef Link)

[5] M. Tiloca, C. Gehrmann and L. Seitz, “On improving resistance to Denial of Service and key provisioning scalability of the DTLS handshake,” *International Journal of Information Security*, Vol. 16, No. 2, pp. 173-193, Apr 2017. Article (CrossRef Link)

[6] Veeraputhiran A and Sankararajan R, “Feature based fall detection system for elders using compressed sensing in WVSN”, *Wireless Networks*, pp. 1-15, Jul 2017. Article (CrossRef Link)

[7] J. Granjal, E. Moteiro and JS. Silva, “Enabling network-layer security on IPv6 Wireless Sensor Networks,” *IEEE Global Telecommunications Conference (GLOBECOM 2010)*, Dec 2010. Article (CrossRef Link)

[8] Raza S, Duquenoy S, Chung T and Yazar D, “Securing Communication in 6LoWPAN with Compressed IPSec,” *7th IEEE International Conference on Distributed Computing in Sensor Systems (DCOSS)*. Barcelona, SPAIN, Jun 2011. Article (CrossRef Link)

[9] CH. Ling, CC. Lee, CC. Yang and MS. Hwang, “A secure and efficient one-time password authentication scheme for WSN,” *International Journal of Network Security*, Vol. 19, No. 2, pp. 177-181, Jan 2017. Article (CrossRef Link)

[10] M. Bouaziz and A. Rachedi, "A survey on mobility management protocols in Wireless Sensor Networks based on 6LoWPAN technology," *Computer Communications*, Vol. 74, pp. 3-15, Jan 2016. Article (CrossRef Link)

[11] J. Hui and P. Thubert, "Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks," *RFC6282*, Sep 2011. Article (CrossRef Link)

[12] J. Reynolds and J. Postel, "Assigned Numbers," *RFC1700*, Oct 1994. Article (CrossRef Link)

[13] http://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml#protocol-numbers-May 2017, accessed 30/07/2017.

Huqing Wang is currently pursuing a PHD degree in the field of network security at Nanjing University of Aeronautics and Astronautics. Her current research interests include network security and IoT.

Zhixin Sun is a professor and PhD supervisor .He has around twenty years both teaching and research experience. He is the dean of School of Modern Posts & Institute of Modern Posts in Nanjing University of Posts and Telecommunications. His current research interests include network security, IoT and video information processing.