IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified

Vol. 6, Issue 2, February 2017

IPsec the Realm for Secure Communication in Internet of Things

Ms. Aishwarya Ashok Akul [1], Prof. Mrs. Snehal Bhosale[2]

Student (ME), Electronics and Telecommunication, R.M.D Sinhgad school of Engineering, Pune, India [1]

Professor, Electronics and Telecommunication, R.M.D Sinhgad school of Engineering, Pune, India [2]

Abstract: Internet of Things (IoT) provides many services in Industrial, Medical, commercial areas etc. Therefore, implementing secured communication in the IoT is essential among many other issues. An IPv6 network interconnects multiple computers and a large number of smart devices. IPsec is secured network therefore it is reasonable to explore the option of using IPsec as a security mechanism for the IoT. Smart devices are generally added to the Internet using IPv6 over Low-power Wireless Personal Area Networks (6LoWPAN). Therefore, to provide security for the IoT IPsec mechanism and IPsec extension of 6LoWPAN is important. In this paper, we discussed such a 6LoWPAN/IPsec mechanism and its extension of this approach. We describe our 6LoWPAN/IPsec mechanism with IEEE 802.15.4 link-layer security. This paper shows that IPsec is a feasible option for securing the IoT in terms of packet delivery, packet size, energy consumption, memory usage, processing time and network lifetime.

Keywords: Internet of Things; 6LoWPAN; IPv6; IEEE 802.15.4 Security.

I. INTRODUCTION

Smart devices are connected using a wireless IEEE 802.15.4 network. A router can be used to connect an IEEE 802.15.4 network to the Internet to enable IPv6 communication between smart devices and Internet hosts. However, IPv6 packets traveling on IEEE 802.15.4 networks use header formats as defined by IPv6 Over Low-power Wireless Personal Area Networks (6LoWPAN) to conserve the bandwidth resources. The router has to compress and decompress IP packets when transmitting packets to ensure compatibility with the existing Internet. A 6LoWPAN relies on 802.15.4 security mechanisms. The node participating in the communication process at the link layer needs to be trusted. The communication can use multiple numbers of hopes as well- as nodes to communicate. A key which is used in communication is to protect all the respective communication. This key is used in the network to secure data transfer on a hop-by-hop basis. This mechanism prevents, as long as the key is kept secure, unauthorized access to the IEEE 802.15.4 network. When the IEEE 802.15.4 network is isolated, in the context of the IoT such an approach fails to provide end-to-end (E2E) security in terms of authentication, non repudiation, confidentiality and integrity. That's why; additional or alternative mechanism is required.

IPsec is a security extension to the IP protocol for the security services. Thus, it seems reasonable to explore the option of using IPsec in the context of 6LoWPAN networks. This paper represents a 6LoWPAN/IPsec extension and viability of this approach. This 6LoWPAN/IPsec is an extension to implement true E2E secure communication between smart devices and Internet hosts. We define header compression format for the IP security related IPv6 Extension Headers: Authentication Header (AH) and Encapsulating Security Payload (ESP). A particular focus of this paper is on the comparison of 6LoWPAN/IPsec security with IEEE 802.15.4 link layer security.

II. RELATED WORK

We present study related to the security in IoT. After reviewing works aiming at designing cryptographic algorithms for constrained devices, we discuss the link layer and network layer at which security can take place in IP-based IoT.

A. Securing the IoT at the link layer

IPsec communication among smart devices uses 6LoWPAN [1], which in turn build on the IEEE 802.15.4 [2] link layer. IEEE 802.15.4 link-layer security is the current state of security solution for IP-connected IoT. IEEE 802.15.4 defines the data encryption/decryption and integrity verification. Advantages of this network protocol independence for the cryptographic functions by currently used 802.15.4 radio chips. Link-layer security provides hop to hop security where each node in the communication path has to be trusted and where neither the host authentication nor the key management is supported. This single pre-shared key is used to protect all communication between the nodes. Furthermore, messages leaving the IEEE 802.15.4 network and continuing to travel on an IP network are not protected by link-layer security mechanisms. Therefore, in many solutions, a separate security mechanism is added to protect data traveling between Internet hosts and routers.

Example is ArchRock PhyNET [3] that applies IPsec in tunnel mode between the router and Internet hosts. Roman et al. [4] proposed key management systems for the sensor network which is applicable to link-layer security.

B. Securing the IoT at the network layer

The IPsec [5] protocol, mandated by IPv6, provides End to End security for the IP communication. Like TLS solutions, it includes a key exchange technique and provides authentication in addition to confidentiality and integrity. Operating at the network layer, it can be used with any transport protocol, including potential future ones. Furthermore, it ensures the integrity and confidentiality of transport-layer headers and integrity of IP headers, which cannot be carried out with higher level solutions as TLS. For these reasons, the research community [6–8] and 6LoWPAN standardizations groups consider IPsec a potential security solution for the IoT. Granjal et al. [9] discussed the use of IPsec for 6LoWPAN. In that study, they analyze the execution times and memory requirements of cryptographic algorithms that they proposed for a 6LoWPAN over IPsec integration.

III.BACKGROUND

In this section, we give an overview of technologies. We give information of 6LoWPAN [3], IEEE 802.15.4 security [2] and IPv6 [10].

A. Overview of 6LoWPAN

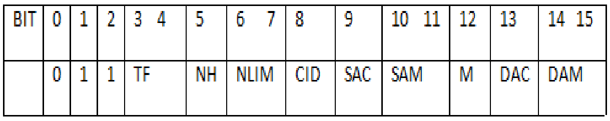
The Low-power Wireless Personal Area Networks idea originated from that "the Internet Protocol should be the smallest objects, and that low-power objects which is having limited processing capabilities should be able to participate in the Internet of Things.

The 6LoWPAN is couple between the IEEE 802.15.4 and IPv6 i.e. between two different networks. The most important difference is the size of IEEE 802.15.4 supports only 127 octet’s packet size wherever IPv6 packet supports 1280 bytes, where the solution proposed by using 6LoWPAN an adaptation layer that optimize IPv6 packets through fragmentation and assemble by the IEEE 802.15.4 link layer. This new layer is located at the Routers that control flow of incoming and outgoing packets from the 6LoWPAN. This all packets of 6LoWPAN nodes share the same address prefix of IPv6.

Frames in 6LoWPAN use four types of headers:

1) No 6loWPAN header (00): In that any frame that does not follow 6loWPAN specifications that will be discarded.
2) Dispatch header (01): It is used for multicasting and IPv6 header compressions.
3) Mesh header (10): It is used for broadcasting.
4) Fragmentation header (11): It is used to fragment long IPv6 header to fit into fragments of maximum 128-byte length. The 6LoWPAN provides header compression mechanism by using LOWPAN_IPHC for IP header compression and LOWPAN_NHC for the next header Compression.

The IPHC reduces the IP header length to 2 bytes for a single-hop network and 7 bytes for a multihop network. The IPHC header is shown in below figure. The next header field when set to 1 indicates that the compressed IPv6 header is encoded with NHC.



BIT	0	1	2	3 4	5	6 7	8	9	10 11	12	13	14 15
	0	1	1	TF	NH	NLIM	CID	SAC	SAM	M	DAC	DAM

Fig. 1. LOWPAN_IPHC encoding for IP header compression

TF: Traffic Class
NH: Next Header
HLTM: Hop Limit
CID: Context Identifier
SAC: Source Address Compression
SAM: Source Address Mode
M: Multicast Compression
DAC: Destination Address Compression
DAM: Destination Address Mode

The general format of NHC is shown in fig.2. Next header compression has number of octets; where the first variable length bit identifies the next header type and the remaining bits are used for encoding the header information.

variable – length ID	Compressed next header

Fig. 2. LOWPAN_NHC for next header compression format

B. Overview of IEEE 802.15.4 Security

IEEE 802.15.4 mechanism is used in IoT standard for MAC. This mechanism defines a frame format with headers including source and destination addresses. It supports a low power communication. It uses channel hopping and time synchronization to enable high reliability, low cost to meet IoT communication requirements.

6LoWPAN relies on IEEE 802.15.4 security to protect the communication between neighboring nodes. The IEEE 802.15.4 support message integrity, confidentiality, access control and replay protection. Message integrity is achieved by including a message authentication code (MAC) in packets. If the receiver cannot verify the MAC, the packet will be discarded. Confidentiality is provided by applying symmetric cryptography to outgoing packets through the inclusion of a monotonically increasing counter in messages; nodes can discard packets being resent by malicious nodes, achieving replay protection.

The security modes supported by the IEEE 802.15.4 standard includes encryption standard in counter mode (AES-CTR) for encryption. AES in counter with CBC-MAC mode (AESCCM) combines encryption and message authentication and AES in cipher block chaining mode (AES-CBC) for message authentication.

DOI 10.17148/IJARCCE.2017.6282

For the MAC modes, the included authentication code is 4,8or 16 bytes. Besides the null mode, AES-CCM is the only mode mandated by the standard, which must be available on all standard devices. A Network with only encryption and no authentication are open to insertion of false packets and shows vulnerable [11]. The IEEE 802.15.4 mechanism provides pre-shared keys for encryption and integrity verification.

Apart from encryption, IEEE 802.15.4 provides another level of security i.e. ACL (Access Control List), to manage the authorization of the devices. It can support up to 255 entries. The MAC layer looks for destination address in the ACL table if it is found, it uses the security specified for this input to encryption and authentication of outgoing packets. The packets used at the data link layer communication are data packets, beacon packets, control packets and acknowledgments packets but the standard does not include any acknowledgments packets as security parameters which give the opportunity to attack the network via this section.

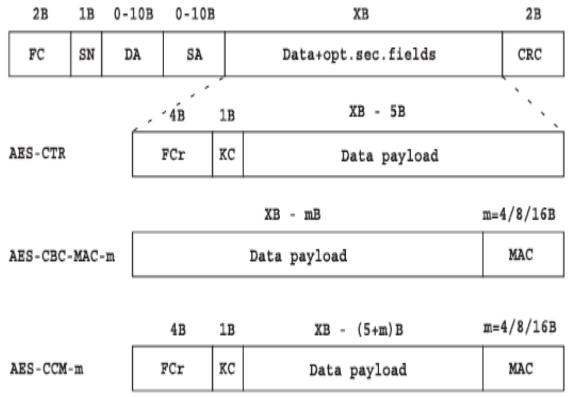


Fig. 3. IEEE 802.15.4 frame with security header format

FC: Frame Control
SN: Sequence Number
DA: Destination Address
SA: Source Address
FCr: Frame Counter
KC: Key Control
MAC: Message Authentication Code

C. Overview of IPv6

IPv6 provides a highly scalable address scheme mechanism. It provides 2^{128} unique addresses. These addresses are sufficient for present and future communicating devices.

IPv6 decreases the size of routing tables and make it more efficient and hierarchical. IPv6 allows ISPs to aggregate the prefixes of customer's networks into a single prefix and announce this as a one prefix to the IPv6 Internet. In IPv6 networks, fragmentation is handled by the source device, using a protocol for finding the path's maximum transmission unit (MTU).

IPv6 provide simplified packet header makes packet processing more efficient. As compared with IPv4, IPv6 does not contain any IP-level checksum, so the checksum does not need to be recalculated at every router hop. Getting rid of the IP-level checksum was possible due to the most link-layer technologies already has checksum and error-control capabilities. IPv6 supports multicast instead of broadcast. Multicast allows bandwidth-intensive packet sent to multiple destinations simultaneously by saving network bandwidth. The hosts which are not interested must process broadcast packets.

IPv6 uses IPsec to secure communication between two end points. IPsec is a collection of protocols, which includes AH which provides authentication, ESP which provides both authentication and privacy services, and a set of encryption as well as authentication.

We define NHC encoding for the two IP extension headers AH and ESP. NHC encodings for the IPv6 Extension Headers consist of an NHC octet where three bits (bits 4, 5, and 6). Those are used to encode the IPv6 Extension Header. The NHC_EH encoding for extension headers is shown in Figure 3. Out of eight values of the EID, six values assigned for the HC15 specification. The remaining two slots (110 and 101) are reserved.

BIT	0	1	2	3	4 5 6	7
	1	1	1	0	EID	NH

Fig. 3. LOWPAN_NHC_EH header format

EID: Extension Header
NH: Next Header

Authentication Header gives connectionless integrity, data origin authentication for IP datagram's, as well as protection against replay attacks. AH uses a keyed message integrity code for protecting the complete IP packet including IP header, AH and IP payload. The IP header fields are set to zero while calculating the MIC. AH gives a reference to the next header, a length field, the security parameters index that identifies the used source address, a sequence number to prevent replay attacks, and the integrity check value that is a message integrity code. For IPv6, ICV should be an integral multiple of 32 bits.

BIT	0	1	2	3	4	5	6	7
	1	1	0	1	PL	SPI	SN	NH

Fig. 4. LOWPAN_NHC_AH encoding format

PL: Payload Length
SPI: Security Parameter index
SN: Sequence Number
NH: Next Header

The first 4 bits in the NHC_AH represent the NHC ID that we define for AH. These bits are set to 1101.

• If PL = 0, the payload length field in AH is omitted. This length can be obtained from the SPI value because the length of the authenticating data depends on the algorithm used and are fixed for any input size.

If PL = 1, the payload value is carried inline after the NHC_AH header.

• If SPI = 0, the default SPI for the 802.15.4 network is used and the SPI field is omitted.
If SPI = 1, all 32 bits indicating the SPI are carried inline.
• If SN=0, first 16 bits of sequence number are elided.
The remaining bits are carried inline.
If SN = 1, all 32 bits of the sequence number are carried inline.

Encapsulating Security Payload gives authentication, data integrity, and confidentiality protection of IP packets. ESP operates on the IP payload, not on the header. ESP has common fields with authentication header and contains the encrypted payload as well as padding required for block ciphers. ESP only encrypts payload data, pad length, padding, and the next header; if ICV calculation is selected, it includes all header fields in the ESP. If AES-CTR is considered as encryption algorithm, ESP, with perfect block alignment, will have an overhead of 18 byte.

BIT	0	1	2	3	4	5	6	7
	1	1	1	0	-	SPI	SN	NH

Fig. 5. LOWPAN_NHC_ESP encoding

SPI: security parameter index
SN: sequence number
NH: Next header

The first 4 bits in the NHC_ESP represent the NHC ID that we define for ESP. These are set to 1110.

• The next bit is unused. We leave this field empty to achieve coding similarity between AH and ESP (ESP does not have a payload length field). However, this field could be used to increase SPI coding to 2 bits if required.

• If SPI = 0, the default SPI for the 802.15.4 network is used and the SPI field is omitted. We set the default SPI value to 1.
If SPI = 1, all 32 bits indicating the SPI are carried inline.

• If SN=0, first 16 bits of sequence number are used.
The remaining 16 bits are assumed to be zero.
If SN = 1, all 32 bits of the sequence number are carried Inline.

• If NH= 0, the next header field in ESP will be used to specify the next header and it is carried inline.
If NH= 1, the next header will be encoded using Next Header Compression.

Figure.6 shows a compressed IPv6 packet, secured with authentication header. It consists of source and destination address, integrity check value, Hop limit and LoWPAN IPHC, LoWPAN NHC_AH, LoWPAN NHC_EH encoding.

<table>
<tr><td>Octet 0</td><td>Octet 1</td><td>Octet 2</td><td>Octet 3</td></tr>
<tr><td colspan="2">LoWPAN_IPHC</td><td>Hop
Limit</td><td>Source Address</td></tr>
<tr><td>Source
Address</td><td colspan="2">Destination Address</td><td>LoWPAN_NHC_
EH</td></tr>
<tr><td>LoWPAN_
NHC_AH</td><td colspan="2">Sequence Number</td><td></td></tr>
<tr><td colspan="4">ICV</td></tr>
<tr><td>S
port</td><td>D
port</td><td>CHECKSUM</td><td>------</td></tr>
<tr><td colspan="4">Payload variable</td></tr>
</table>

Fig. 6. General format of IPv6 packet

ICV: Integrity Check value
S port: Source port
D port: Destination Port

IV. PROPOSED METHOD

The proposed method consists of amalgamation of software and hardware. Where software part will be created using Matlab and hardware implantation will be done by using ARM 7.The data transmission and reception is done by using Zigbee.

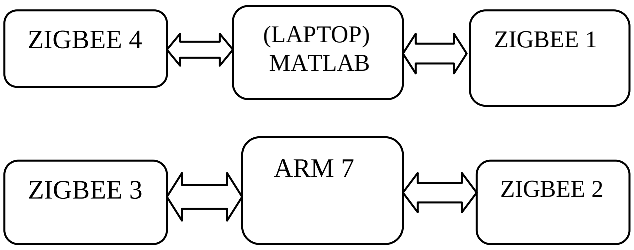


Fig. 7. Proposed Method

The packets creation will be undertaken by using Matlab, and we use encrypted data in packet payload for authentication purpose. A packet is consisting of source address and destination address. In our system, we are using two pairs of Zigbee, one for transmitting a packet and one for receiving a packet, a Zigbee transmitter and receiver pair created by their MSB and LSB Bits respectively. The Zigbee Receiver then send these packets to ARM 7, then ARM 7 will do the decryption of packets based on their destination addresses.

The packets that fail to match the destination address will be discarded from the system. The once that will match up to the correct address and hence fully authenticated packets will be passed to the second Zigbee paired setup that will retransmit the secure packet to our device and the device will compute the results on basis of graph simulation that will give us the better result packet performance when passed through IPsec.

DOI 10.17148/IJARCCE.2017.6282

Below figure shows network topology of IPv6 packet. These nodes are created for IPv6 packets for mobility purpose. We add all parameter in IPv6 packet by using Matlab tool. Each parameter will include header format, hop limit, source address, destination address etc.In future work; we will be able to describe the secure packet communication with gigantic performance for data transmission.

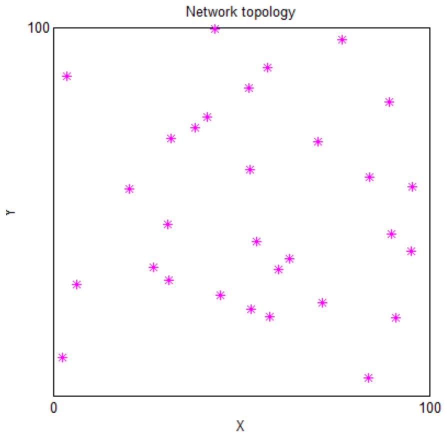


Fig. 7. Network Topology of IPv6 packet

V. CONCLUSION

The earlier technology had compatibility with device communication but it was adequate for substantial performance. In spite this there are certain difficulties that we come across. Especially in Packet data transfer gets affected in when network traffic, isolated network. For example delay in packet delivery, no authentication etc. All this issues can be overtaken by IPsec over 6LoWpan.
Besides increased address space, IPv6, as compared to IPv4, also provides a simplified header format, better support for extensions and mandates IP security. IPv6 with potentially unlimited address space of 2^128 addresses makes it possible to assign a unique address to each physical device on earth.

The security mechanism of IEEE 802.15.4, which are very limited and does not achieve the security objectives of the data packets connected to IP network. IPv6 security mechanism, which are very greedy and supplies energy and space, there is a need to propose and develop new powerful security mechanisms adapted to 6LoWPAN networks. IPsec functionality has enhanced the secure communication in IoT and the same can be observed by implementation of IPv6. Hence, the paper includes several packet formats along with their usage. Alongside comes a proposed method that tests the formats and gives us better security with desired results

REFERENCES

[1] Deloche G, Kushalnagar N, Hui J, Culler D. Transmission of IPv6 Packets over IEEE 802.15.4 Networks RFC 4944, 2007.
[2] IEEE std. 802.15.4—2003: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low Rate Wireless Personal Area Networks (LR-WPANs). IEEE, 2003.
[3] ArchRock Corporation. Phynet n4x series, 2008.
[4] Roman R, Alcaraz C, Lopez J, Sklavos N. Key management systems for sensor networks in the context of the Internet of Things. Computers and Electrical Engineering 2011; 37(2): 147–159.
[5] Kent S, Seo K. Security Architecture for the Internet Protocol. RFC 4301, 2005.
[6] Granjal J, Silva R, Monteiro E, Sa Silva J, Boavida F.Why is IPsec a viable option for wireless sensor networks. In Proceedings of 4th IEEE International Workshop on Wireless and Sensor Networks Security (WSNS'08), Atlanta, USA, 2008.
[7] Riaz R, Kim K-H, Ahmed HF. Security analysis survey and framework design for IP connected LoWPANs. In Proceedings of 9th International Symposium on Autonomous Decentralized Systems (ISADS'09), Athens, Greece, 2009.
[8] Roman R, Lopez J. Integrating wireless sensor networks and the internet: a security analysis. Internet Research 2009; 19(2): 246–259.
[9] Granjal J, Monteiro E, Sá Silva J. Enabling networklayer security on IPv6 wireless sensor networks. In Proceedings of IEEE Global Communications Conference (GLOBECOM'10), Miami, USA, 2010.
[10] Deering S, Hinden R. Internet Protocol, Version 6 (IPv6) Specification. RFC 2460, 1998.
[11] Sastry N, Wagner D. Security considerations for IEEE 802.15.4 networks. In Proceedings of the 3rd ACM Workshop on Wireless Security, WiSe'04, New York, NY, USA, 2004; 32–42. ACM.

BIOGRAPHIES

Ms. Aishwarya Akul, currently studying M.E in VLSI and Embedded system at RMD Sinhgad School of Engg, Pune. The author has her personal filed of interest in the domain of wireless sensor network, VLSI, Embedded system and Internet of Things.

Prof. Mrs. Snehal Bhosale, currently heading Department of E&TC at RMD Sinhgad School of Engg, Pune. Her main research interests are computer networks, network security and wireless sensor networks. She is currently doing her research on security in IoT in Pune University

.

DOI 10.17148/IJARCCE.2017.6282