IJICTR
International Journal of Information & Communication Technology Research

Volume 16- Number 2 – 2024 (17 -24)

An Overview of Secure Communications for the Internet of Things

Seyed Ali Zoljalali Moghadam*
Electrical Engineering Department
Electrical and Computer Faculty
Tarbiat Modares University
Tehran, Iran.
ali2451377@gmail.com

Peyman Vafadoost
Biomedical Engineering Department
Electrical and Computer Faculty
Hakim Sabzevari University
Sabzevar, Iran.
peymanvafadoost@sun.hsu.ac.ir

Received: 24 November 2023 – Revised: 16 April 2024 - Accepted: 6 May 2024

Abstract—**As an emerging technology that combines both digital and physical realms, access to information technology has expanded (IoT) the Internet of Things. The Internet of Things, as it becomes more pervasive, will overshadow human life as much as possible. Some of the major challenges associated with the development of this phenomenon have been the issue of security, which is needed in all its layers and even specifically in individual layers. According to the structure and applications of the Internet of Things, as well as the threats and challenges in cyberspace, we first examine security needs and then, by examining some methods of securing the Internet of Things, we propose a method according to the approaches discussed.**

Keywords: IoT, IPsec, 6LoWPAN, Security, IEEE 802.15.4, Security, Privacy

Article type: Research Article

I. INTRODUCTION

The future of the Internet is a network with the IPv6 protocol that includes traditional computers and a large number of smart objects [1]. Smart objects, often referred to as things, usually have small built-in computers with communication, measurement, and excitation capabilities. The Internet of Things (IoT) function will be the beginning of many services, enabling the connection between traditional computers and intelligent objects on a global scale. Therefore, it is very important to check the security conditions, ie authentication, integrity, nonrepudiation and confidentiality in IoT.

The Internet of Things (IoT) refers to the concept of connecting everyday objects and devices to the internet, enabling them to collect and exchange data. These objects, also known as smart objects or things, are equipped with sensors, actuators, and embedded systems that allow them to interact with their environment and communicate with other devices or systems.

One of the key aspects of IoT is the use of the IPv6 protocol, which provides a much larger address space

* Corresponding Author

compared to the older IPv4 protocol. With IPv6, there are virtually limitless unique addresses available, allowing for the connection of a vast number of devices and objects to the internet.

The integration of IoT into our lives opens up a wide range of possibilities and applications. Smart homes, for example, can have interconnected devices such as thermostats, lighting systems, security cameras, and appliances that can be controlled and monitored remotely. Industrial sectors can benefit from IoT by implementing smart systems for monitoring and optimizing processes, predictive maintenance, and inventory management.

The Internet of Things has become an integral part of modern life, connecting devices and data to provide greater efficiency, automation and control.

In general, at present, the architecture has not been designed and built with a global standard for the Internet of Things, and for this reason, explaining the architecture of the Internet of Things can be a bit difficult and problematic. If we want to talk about this issue in general, it can be said that it completely depends on the functioning and implementation of its various components and parts. However, there is a basic process in the architecture of the Internet of Things in this field, which the Internet of Things is built on. This architecture is also called the four-layer architecture of the Internet of Things.

- The layer of sensors that is responsible for receiving information.
- The network layer that is responsible for transmitting the received data.
- The information and data processing layer that can draw conclusions from the received data.
- Finally, they are the application layer that directly communicates with the user.

The proper functioning of each of these layers will be necessary and necessary for the proper functioning of Internet of Things equipment [20]. Figure 1 is for Internet of Things architecture

However, with the increased connectivity and data exchange in IoT, security becomes a critical concern. It is essential to ensure that IoT systems and devices are protected from unauthorized access, data breaches, and malicious attacks. Authentication methods, such as secure protocols and encryption, are used to verify the identity of devices and establish secure communication channels. Integrity mechanisms help ensure that data remains unaltered during transmission, while non-repudiation measures prevent the denial of actions or transactions. Additionally, confidentiality measures, such as data encryption, protect sensitive information from unauthorized disclosure.

As IoT continues to evolve and expand, addressing security challenges will be crucial to leverage its full potential while safeguarding privacy and mitigating risks.

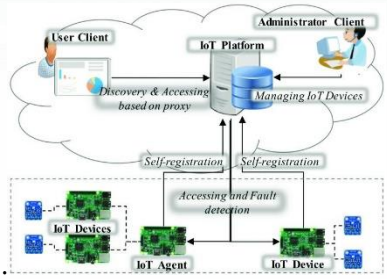

Figure 1. Internet of Things architecture [21]

Smart objects are usually connected to each other using a wireless IEEE 802.15.4 [2] network. You can use the border router to connect to the 802.15.4 network on the Internet to activate the IPv6 connection between smart objects and the Internet host. However, IPv6 packets that travel on 802.15.4 networks use IPv6 compressed header templates to use bandwidth sources. To ensure compatibility with the available Internet, the border router must compress the IP packet header when sending packets.

In IoT networks, smart objects often communicate with each other using a wireless IEEE 802.15.4 network [2]. To establish a connection between these smart objects and the internet, a border router can be utilized. The border router acts as a bridge between the 802.15.4 network and the internet, enabling the activation of IPv6 connectivity for the smart objects to communicate with internet hosts.

When transmitting IPv6 packets over 802.15.4 networks, a technique called IPv6 compressed header is employed to optimize bandwidth usage. This involves using compressed header templates specifically designed for IPv6 packets traveling through 802.15.4 networks. By compressing the IP packet headers, it allows for more efficient utilization of network resources and reduces the overhead associated with transmitting data.

For compatibility with the existing internet infrastructure, the border router is responsible for compressing the IP packet headers when sending packets from the 802.15.4 network to the internet. This compression process ensures that the IPv6 packets can seamlessly traverse the network while minimizing bandwidth consumption and maintaining efficient communication between smart objects and internet hosts.

By utilizing these techniques, the IoT ecosystem can efficiently exchange data between smart objects and the internet, enabling seamless connectivity and communication while optimizing network resources.

Currently, 6LoWPAN relies on 802.15.4 security mechanisms. A single network key is used to secure data based on the hop-by-hop. This prevents unauthorized access to the 802.15.4 network and ensures its security until the key is secure and not available to hackers. However, in the context of the IoT, such an approach cannot provide end-to-end (E2E) security in terms of authentication, integrity, nonrepudiation, and confidentiality. Clearly, additional or alternative mechanisms are needed. How to make a connection is E2E using the IPsec protocol [4]. IPsec defines the security plugins of the IP protocol to

implement security. Therefore, it makes sense to consider the option of using IPsec in 6LoWPAN networks. In this article, we present 6LoWPAN / IPsec and show the durability and reliability of this approach.

Our 6LoWPAN / IPsec Add-ons app is shown in Figure 2 for a real E2E secure connection between smart objects and the Internet host. We define header compression for IPsec IPv6 add-on headers: authentication header (AH) and Encapsulating Security Payload (ESP). We provide an implementation and evaluation of the 6LoWPAN / IPsec extension for intelligent running objects running the well-known Contiki operating system [5]. This implementation takes advantage of the encryption capability provided by the 802.15.4 standard transceivers.

The main focus of this article is to compare the security of 6LoWPAN / IPsec with the security of 802.15.4 traditional link-layer. To do this, we also implement 802.15.4 link layer security for the Contiki operating system, which allows us to test and compare both security mechanisms in one platform. Our experiments show that traditional 802.15.4 link layer security does not significantly improve network performance better than our proposed 6LoWPAN/IPsec security.

The main points of the article, which we will discuss more, are as follows:

- We provide a definition of 6LoWPAN for IPsec, supporting AH and ESP.
- We provide a complete implementation and evaluation of the tested performance of 6LoWPAN / IPsec. We also show the benefits of using cryptographic hardware support from the 802.15.4 transceivers.

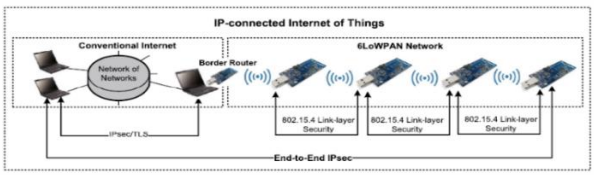

Figure 2. IEEE 802.15.4 security can communicate via IPv6 via a low-power personal wireless device (6LoWPAN)

II. INTERNET OF THINGS APPLICATIONS

The development of new types of sensors and actuators in the combination of inclusive and growing network communications shapes the Internet of Things concept and greatly demands users for new services in the evolution of the Internet and IoT [16]. There are many factors involved, including reducing the price of the equipment involved. Increasing the efficiency of the devices will lead to more and better services to the end user. Over the next few years, we will see the widespread penetration of IoT-capable chips into all types of physical objects, which will expand applications such as the following:

- Smart homes (environmental control and smart appliances) ·
- Smart city (resource control, such as street lighting, waste management, water and energy management, traffic control, etc.)
- Industry (process control)
- Construction (intelligent construction management)
- Individuals (location services, health management and supervision, etc.)

III. IOT GROWTH

As shown in Figure 3, the increase in the number of devices connected to the Internet has a very fast trend. An interesting trend that has contributed to the growth of the Internet of Things is the transition of the Internet of Things. 4 IP protocol is version 6 of that protocol. If we consider version 4 for consumers such as laptops and tablets, version 6 of this protocol includes sensors, smart systems and cluster systems[17].

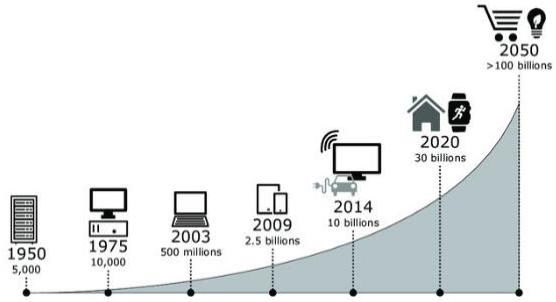

Figure 3. Anticipated increase in IoT device adoption.

In recent years, the Internet of Things has emerged as one of the fastest growing technologies in the field of information and communication technology (ICT). This concept means connecting various devices, sensors and objects to the Internet in order to collect, send and exchange data and information. With the advancement of various technologies, including the Internet of Things, we have seen a significant growth in the number and type of objects connected to the Internet.

This massive growth in the Internet of Things is due to the many benefits it brings, including:

- Access to information at any time and place: Connecting objects to the Internet provides the possibility of accessing data and information about them instantly and at any time and place, which helps to improve the efficiency and usability of various services. .
- Optimal use of resources: The Internet of Things enables the optimal use of various resources, including energy, time, and materials needed to execute processes and tasks.
- Smart and automatic connections: Using the Internet of Things, connections between objects are made smarter and more automatic, which helps to improve the efficiency and functions of various systems and devices.

The Internet of Things will play an important role in human life in the future. The Internet of Things will be

used in various industries, including healthcare, automotive, agriculture, smart cities, environment, etc., which will help improve the quality of life, productivity, security, and sustainability of communities and the environment. In general, the Internet of Things, as one of the main technological developments in recent decades, has a lot of potential to change and improve people's lives in the future.

IV. The Challenge of Security on the Internet of Things

Undoubtedly, information is one of the most valuable assets of today's organizations and businesses, and defects in data storage equipment, human errors, virus attacks, software errors, and accidents such as fire and earthquake are among the most common causes of destruction and loss. giving digital information and data, and in order to protect data, considering that the budget for dealing with cyber-attacks on the Internet of Things is not high and it is necessary to adopt appropriate tactics in this sensitive field, strict regulatory standards for greater security can be integrated in order to integrate Information technology and computing technology mentioned [18]. Also, the hardware and software equipment available in the Internet of Things has provided different platforms for exchanging information between them. The information on the chips of objects connected to the Internet can be stolen, therefore, by using the encryption and decryption protocols available in the platforms, the information can be protected, mostly the data generated by the Internet of Things devices based on time and They are based on events that respond to needs with the help of a database. One of the requirements of this type of databases is to have a suitable platform [19].

In this situation, although this equipment is present in all aspects of personal life and controls it and supports new business models, it increases the efficiency of many applications and ultimately improves people's lives, but naturally its risks are also significant. It is more and therefore requires strong security components. In particular, if we focus on the important approach of smart homes, we can limit the ability to intrude on privacy by considering explicit and directly related data to the people living in the home. However, the activities of these people can be followed indirectly by examining the physical and network activities of the equipment and devices inside the house. Cyberspace security is defined by the three components of confidentiality, accuracy and accessibility, which can be considered as the basic needs of IoT security. In many cases, a major disruption to the traditional model poses its own challenges. The following are some of the challenges posed by the Internet of Things:

- Critical functionality: In addition to devices, systems and appliances in a home, embedded devices also are found controlling the world’s transportation infrastructure, the utility grids, communication systems and many other capabilities relied upon by modern society. Interruption of these capabilities by a cyber-attack could have catastrophic consequences.
- Replication: Once designed and built, embedded devices are mass produced. There may be

  thousands to millions of identical devices. If a hacker is able to build a successful attack against one of these devices, the attack can be replicated across all devices.
- Security assumptions: Many embedded engineers have long assumed that embedded devices are not targets for hackers. These assumptions are based on outdated assumptions including the belief in security by obscurity. As a result, security is often not considered a critical priority for embedded designs. Today’s embedded design projects are often including security for the first time and do not have experience and previous security projects to build upon.
- Not easily patched: Most embedded devices are not easily upgraded. Once they are deployed, they will run the software that was installed at the factory. Any remote software update capability needs to be designed into the device to allow security updates. The specialized operating systems used to build embedded devices may not have automated capabilities that allow easy updates of the device firmware to ensure security capabilities are frequently updated. The device itself may not have the IO or required storage that allows for updating to fight off security attacks.
- Long life cycle: The life cycle for embedded devices is typically much longer than for PCs or consumer devices. Devices may be in the field for 15 or even 20 years. Building a device today that will stand up to the ever evolving security requirements of the next two decades is a tremendous challenge.
- Proprietary/industry specific protocols: Embedded devices often use specialized protocols that are not recognized and protected by enterprise security tools. Enterprise firewalls and intrusion detection system are designed to protect against enterprise specific threats, not attacks against industrial protocols.
- Deployed outside of enterprise security perimeter: Many embedded devices are mobile or are deployed in the field. As a result, these devices may be directly connected to the Internet with none of the protections found in a corporate environment.

A. Embedding cryptographic algorithms

Much research has been done on reducing the complexity of encryption algorithms or improving the efficiency of protocols and key distribution in a secure manner.

For example, TinyECC [6] and NanoECC [7] used elliptical curve encryption to allow encryption on open source devices. For example, Liu and Ning [8], and Chong and Rudig [9] provided key distribution mechanisms to store bandwidth in limited resource networks.

B. IoT security at the link layer

IP communication between intelligent objects uses 6LoWPAN [3], each based on the IEEE 802.15.4 [2] link layer. IEEE 802.15.4 provides data encryption and integrity verification. Link layer security provides hop-by-hop security in which each node in the communication path (including the 6LoWPAN border router; as shown in Figure 2) is reliable. A private key is used to protect all messages and packets. In addition, messages sent from the 802.15.4 network and continue their route on the network using IP are not protected by link layer security mechanisms. Therefore, in many of the solutions provided for this challenge, a separate security mechanism has been added to protect data between Internet hosts and border routers. An example of this solution is ArchRock PhyNET [10], which adds IPsec in a tunnel mode between the border router and the Internet host. Recently, Roman and a number of colleagues. [11] Provides a method for key management systems for the sensor network that is applicable to the security of the link layer. Because any node, including border routers, must be trusted, E2E security in the IoT cannot be achieved using the specified method.

C. Securing the IoT at the transport layer

End-to-end security may be provided using (TLS) [12] or (SSL). TLS and SSL are used extensively on the Internet to ensure secure communication between hosts. In addition to being confidential and integrity, TLS and SSL also authentication between Internet hosts. There are problems that challenge the use of these protocols to ensure security in the IoT. TLS can only be used in TCP, which is not a good way to communicate between smart objects because TCP makes it possible to use more resources from low-power devices. However, Hong and colleagues have proposed SSL as a security mechanism for the IoT. [13] Their assessment shows that this security mechanism is actually quite costly because full access to SSL is done if data transfer takes 2 seconds. Also (UDP) version of TLS called DTLS can be used in 6LoWPAN networks. However, the 6LoWPAN specification does not provide compression for DTLS.

V. BACKGROUND

In this section, we provide an overview of the work-related technologies presented in this article. We provide background information on IPv6 and 6LoWPAN [3], IPsec [4] and on security 802.15.4 [2].

A. Overview of 6LoWPAN

IPv6 is used through a low-power wireless personal network [3] to connect to the Internet and smart objects by specifying how IPv6 data is transmitted over the IEEE 802.15.4 network (Fig 4). 6LoWPAN works as a unique layer between the IP layer and the link layer, one of which is to compress the IP header and, if necessary, fragment the data. The maximum transmission unit (MTU) of 802.15.4 is 127 bytes. If 802.15.4 security is enabled, the maximum load will be reduced to 81 bytes.

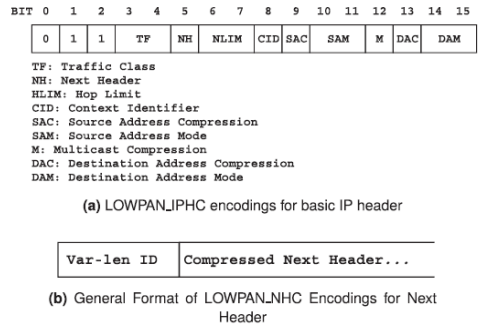

Figure 4. IPv6 over low-power wireless personal area networks (6LoWPAN) context-aware compression mechanisms [14].

B. Overview of IEEE 802.15.4 security

Currently, 6LoWPAN trusts 802.15.4 [2] security to protect communication between neighboring nodes. The standard supports access control, message integrity, confidentiality, and replay protection. Message integrity is achieved using (MAC) in envelopes. If the recipient fails to confirm the desired MAC, the envelope will be deleted according to the pre-defined instructions. Figure 5 shows the structure of an 802.15.4 packet with optional security headers. Security modes supported by 802.15.4 include (AES-CTR) only for encryption, AES in blockchain mode (AES-CBC) only to validate the message. For MAC modes, the authentication code is 4, 8 or 16 bytes. In addition to the default mode (security features not available), AES-CCM is the only mandatory state by default that must be implemented on all devices compatible with the standard.

The IEEE 802.15.4 standard currently uses pre-shared keys to encrypt and integrity message.

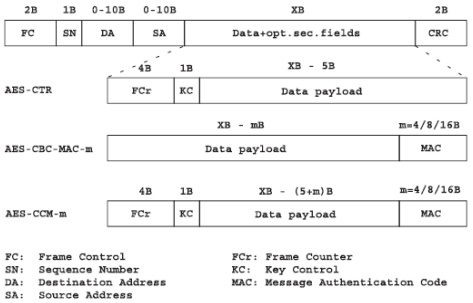

Figure 5. IEEE 802.15.4 frame with security headers [14].

C. Overview of IPsec

IPv6, with its unlimited potential of 2^{128} address space, makes it possible to assign a unique address to any physical device on Earth. In addition to increasing the address space, IPv6 also provides IP security compared to IPv4. IPv6 uses IPsec [4] to communicate IP between two endpoints. IPsec is a set of protocols, which include AH and ESP. AH, which provides authentication services, ESP provides both authentication and privacy services.

In this article, various security methods that are used to protect information in network communication were investigated. In general, the use of IPSec provides security compared to other methods such as SSL/TLS and SSH, by providing protection for data transmission through encryption and creating secure tunnels

between devices, while SSL/TLS uses encryption protocols for It uses secure communication between user and server (such as HTTPS) and SSH provides secure communication between two devices using encryption.

The following table provides some basic and important features for comparison between IPsec and IEEE 802.15.4.

TABLE I. COMPARISON BETWEEN IPSEC AND IEEE 802.15.4 METHODS

Property	IPsec	IEEE 802.15.4
Type of communication	between different networks	between wireless devices on a network
Common use	Wireless sensor networks, ZigBee	VPN, secure connection between networks, secure internet connections
Security level	High	Middle
Encryption	Yes	Depending on the implementation and communication
Authentication	Yes	Depending on the implementation and communication
Related protocols	IP, ESP, AH	MAC, Zigbee

VI. 6LOWPAN/IPSEC EXTENSION

Of the eight possible EID values, six are allocated by specification HC15. There are actually two remaining slots (101 and 110) in reserve. Since AH and ESP are headers for IP extensions, it makes sense to use one of those reserved AH and ESP slots for compression. We 're proposing to use one of the reserved slots, say 101, to identify an AH or ESP header as the next header.

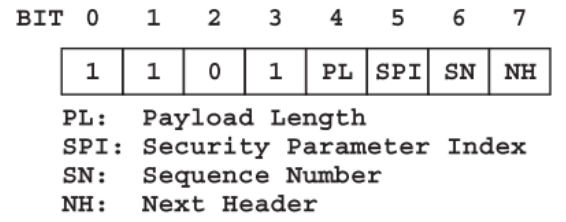

Figure 6. LOWPAN_NHC_AH: next header compression

A. *LOWPAN_NHC_AH encoding*

Figure 6 illustrates our AH encoding for the NHC. Next we went

Describe the position of all relevant fields:

- The first four bits of the NHC AH represent the NHC ID we define for AH. These are fixed at 1101
- If PL = 0, the area of payload (length of header IPsec) is omitted in AH. This length can be obtained from the SPI value, since the authentication data length depends on the algorithm used and is fixed for any input size
- When PL = 1, the payload value after the NHC AH header is held inline.
- If SPI = 0, then the default SPI is used for the 802.15.4 network and the SPI field is omitted. We set SPI by default to 1. This does not mean all nodes are using the same SA, but each node has a single preferred SA defined by SPI 1.
- If SPI = 1, all 32 bits displaying the SPI will be brought inline
- If SN = 0, the first 16 bits of the number of sequences are elided. The remaining bits are transported inline.
- If SN = 1 is carried inline all 32 bits of the sequence number
- If NH = 0, the next header field in AH is used to specify the next header.
- If NH = 1, then elide the next header field in AH. The next header is encoded through NHC.

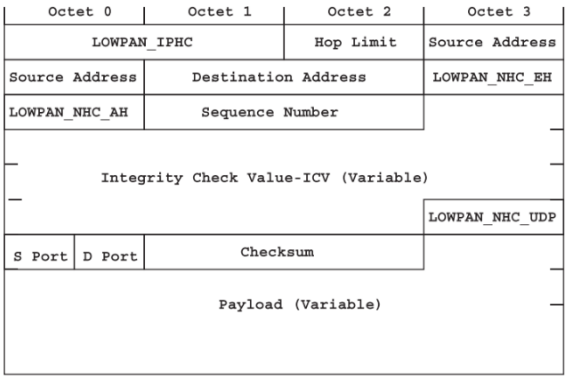

Figure 7. A compressed and authentication header secured IPv6/User Datagram Protocol packet

Note that AH calculates the MIC on the uncompressed IP header even when used in 6LoWPAN, thus allowing authenticated communication with the Internet hosts. The minimum length of a standard AH which supports the mandatory HMAC-SHA1-96 and AES-XCBC-MAC-96 consists of 12 bytes of header fields plus 12 bytes of ICV. Following optimum compression, we get a header size of 4 bytes plus 12 bytes of ICV.

Figure 7 shows a compressed IPv6 / UDP packet which is secured using HMAC-SHA1-96 with AH.

B. *LOWPAN_NHC_ESP encoding*

Figure 8 shows the encoded NHCs we are proposing for ESP. Next, the function of each header field is described as:

- The first 4 bits we define for ESP in the NHC ESP represent the NHC ID. These are fixed at 1110.
- The next bit remains unused. To achieve coding similarity between AH and ESP, we leave this field empty (ESP does not have a field for payload lengths). This field could however be used to increase SPI coding to 2 bits if necessary
- If SPI = 0, then the default SPI is used for the

802.15.4 network and the SPI field is omitted. We set SPI by default to 1. This does not mean all nodes are using the same SA, but each node has a single preferred SA identified by SPI 1.

- If SPI = 1, all 32 bits showing the SPI will be carried inline
- If SN = 0 is used first 16 bits of sequence number. The remaining 16 bits are presumed to be nil.
- If SN = 1 is carried inline all 32 bits of the sequence number
- If NH = 0, then the next ESP header field will be used to specify the next header, and it will be carried inline.
- If NH = 1, it encodes the next header using NHC. In the case of ESP, we cannot skip the next header unless 6LoWPAN compression / decompression and encryption / decryption are jointly executed by the end hosts. Based on the next header value, the nodes in the 6LoWPAN network make their decision about the next header, not the actual header that is carried inline.

Remember that the minimum overhead for ESP without authentication is 18 bytes, AES-CBC and perfect block alignment. This header overhead is reduced to 14 bytes, after optimal compression. ESP with authentication contains a further 12 ICV bytes. Figure 8 shows a secured UDP / IP packet with compressed ESP. The shaded portion stands for cipher-text.

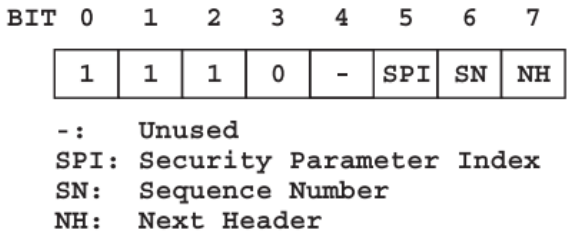

Figure 8. LOWPAN_NHC_ESP: next header compression

The UDP header is encrypted when using ESP, and can therefore not be compressed. One solution for enabling UDP header compression when using ESP is to specify a new encryption algorithm for ES, which can perform 6LoWPAN UDP header compression plus source and destination encryption. Since such a solution would not be viable until 6LoWPAN is massively adopted, we do not specify its details.

VII. Conclusion

The future of the Internet of Things will be based on IP. Because we will benefit from many services in the future, our daily lives will depend on its availability and reliable performance. So it's important to find ways to secure your IoT. Because the security of the IEEE 802.15.4 link layer does not provide the necessary security for E2E, alternative methods must be found to ensure network security. In this article, we've shown that IPsec, implemented through the 6LoWPAN extensions, is a good option for providing E2E security on IoT.

Indeed, the future of the Internet of Things (IoT) heavily relies on IP (Internet Protocol) as it provides the foundation for connectivity and communication. As we increasingly depend on IoT for various services in our daily lives, the availability and reliable performance of IP become crucial. However, alongside the benefits of IoT, ensuring its security is of paramount importance.

While the IEEE 802.15.4 link layer provides some security features, it may not offer the necessary end-to-end (E2E) security required for IoT deployments. Therefore, alternative methods need to be explored to enhance network security and protect IoT systems and data.

One such method is the use of IPsec (IP security), which can be implemented through the 6LoWPAN (IPv6 over Low Power Wireless Personal Area Networks) extensions. IPsec provides a robust framework for securing IP communications by offering features such as authentication, encryption, integrity, and confidentiality. By leveraging 6LoWPAN, IPsec can be extended to IoT devices and networks, enabling E2E security.

Implementing IPsec through 6LoWPAN extensions allows for secure communication between IoT devices, ensuring that data remains confidential, unaltered, and protected from unauthorized access. It enhances the overall security posture of IoT deployments and helps mitigate the risks associated with potential vulnerabilities in the network.

By adopting IPsec with 6LoWPAN, IoT systems can benefit from E2E security, safeguarding sensitive information and ensuring the integrity and privacy of data transmitted within the IoT ecosystem. This approach provides a viable option for addressing the security challenges of IoT and enhancing the trustworthiness of IoT-enabled services and applications [15].

References

[1] G. Eason, B. Noble, and I. N. Sneddon, “On certain integrals of Lipschitz-Hankel type involving products of Bessel functions,” Phil. Trans. Roy. Soc. London, vol. A247, pp. 529–551, April 1955. (references)

[2] J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

[3] I. S. Jacobs and C. P. Bean, “Fine particles, thin films and exchange anisotropy,” in Magnetism, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271–350.

[4] Lombardi, Marco, Francesco Pascale, and Domenico Santaniello. "Internet of things: A general overview between architectures, protocols and applications." Information 12, no. 2 (2021): 87.

[5] Dunkels A, Grönvall B, Voigt T. Contiki—a lightweight and flexible operating system for tiny networked sensors. In Proceedings of 1st IEEE Workshop on Embedded Networked Sensors (EmNetS’04), Tampa, USA, 2004.

[6] Liu A, Ning P. TinyECC: a configurable library for elliptic curve cryptography in wireless sensor networks. In Proceedings of 7th International Conference on Information Processing in Sensor Networks (IPSN’08), Washington, DC, USA, 2008.

[7] Szczechowiak P, Oliveira L, Scott M, Collier M, Dahab R. NanoECC: testing the limits of elliptic curve cryptography in sensor networks. In Proceedings of 5th European Conference on Wireless Sensor Networks (EWSN’08), Bologna, Italy, 2008.

[8] Liu D, Ning P. Establishing pairwise keys in distributed sensor networks. In Proceedings of 10th ACM Conference on Computer and Communications Security (CCS), New York, NY, USA, 2003.

[9] Chung A, Roedig U. DHB-KEY: an efficient key distribution scheme for wireless sensor networks. In Proceedings of 4th IEEE International Workshop on Wireless and Sensor Networks Security (WSNS'08), Atlanta, USA, 2008.

[10] Arch Rocks Adds Ruggedized Version Of IP-Based 'PhyNet' Wireless Sensor Network for Harsh Outdoor Enivorments, With PhyNet N4X, Protected Devices Monitor Air Quality, Traffic, Toxics, Solar Power, Crop Health and More; Users Analyze the Data Remotely,2008

[11] 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.

[12] Oppliger, Rolf. SSL and TLS: Theory and Practice. Artech House, 2023.

[13] Hong S, Kim D, Ha M, et al. SNAIL: an IP-based wireless sensor network approach to the Internet of Things. Wireless Communications, IEEE 2010; 17(6): 34–42.

[14] Shahid Raza, Simon Duquennoy, Joel Höglund,Utz Roedig and Thiemo Voigt: Secure communication for the Internet of Things— a comparison of link-layer security and IPsec for 6LoWPAN, Networks 2014; 7:2654–2668

[15] Rachit, Shobha Bhatt, and Prakash Rao Ragiri. "Security trends in Internet of Things: A survey." SN Applied Sciences 3 (2021): 1-14.

[16] D.Geneiatakis, I.Kounelis, R.Neisse , I.Nai-Fovino " Security and Privacy Issues for an IoT based Smart Home" 2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO) , Pages: 1292 - 1297 IEEE Conference Publications.

[17] Hamdan, Salam, Moussa Ayyash, and Sufyan Almajali. "Edge-computing architectures for internet of things applications: A survey." Sensors 20, no. 22 (2020): 6441.

[18] Nick Heudecker. DBMS Characteristics for the Internet of Things. 2015. gartner.com

[19] Scott Matteson. How to secure your IoT devices from botnets and other threats. 2017.techrepublic.com.

[20] Anthi, Eirini, Lowri Williams, Małgorzata Słowińska, George Theodorakopoulos, and Pete Burnap. "A supervised intrusion detection system for smart home IoT devices." IEEE Internet of Things Journal 6, no. 5 (2019): 9042-9053.

[21] Jin, Wenquan, and Dohyeun Kim. "Resource management based on OCF for device self-registration and status detection in IoT networks." Electronics 8, no. 3 (2019): 311.

Seyed Ali Zolajalali Moghaddam received his B.Sc. degree in Electrical Engineering from Hakim Sabzevari University, Sabzevar, Iran, in 2019 and M.Sc. degree in Electrical Engineering from Tarbiat Modares University, Tehran, Iran, in 2022.

Peyman Vafadoost Sabzevar received his B.Sc. degree in Computer Engineering and his M.Sc degree in Biomedical Engineering in 2020 and 2023 from Hakim Sabzevari University, Sabzevar, Iran, respectively. His research interests include Internet of Things and Machine Learning.