Journal of the Korea Academia-Industrial cooperation Society
Vol. 13, No. 6 pp. 2739-2742, 2012

http://dx.doi.org/10.5762/KAIS.2012.13.6.2739

Requirements and Analysis for Efficient Key Management Mechanism on IPSec-6LoWPAN

YunJung Lee[1] and Jungwon Cho[2*]

[1]**Dept. of Computer Science and Statistics, Jeju National University**
[2]**Dept. of Computer Education, Jeju National University**

IPSec-6LoWPAN을 위한 키 관리 요구사항과 프로토콜 분석

이윤정[1], 조정원[2*]
[1]제주대학교 전산통계학과, [2]제주대학교 컴퓨터교육과

Abstract 6LoWPAN is a standard to enable IPv6 packets to be carried on top of low power wireless networks. It needs to achieve security in 6LoWPAN, which is being defined at the 6LoWPAN working group of the IETF. IPSec is already part of IPv6, which makes it a candidate to be directly employed or adapted for WSNs. Some results showed that the adoption of IPSec is viable, and also point towards the successful design and deployment of security architecture for WSNs. IPSec requires two communicating entities to share a secret key that is typically established dynamically with the IKE. However, there are some limitations to use IKE on wireless networks. In this article, we show requirements for being Efficient Key management Mechanism for IPSec on 6LoWPAN and analyze candidate protocols.

요 약 6LoWPAN (IPv6 over Low Power Personal Area Network)은 IPv6 패킷을 저전력 무선 네트워크인 센서 네트워크를 통한 전송을 가능하게 하는 표준이다. 이를 위해서는 6LoWPAN에서의 보안 문제를 해결해야할 필요가 있다. IPSec은 IPv6에서의 보안을 담당하는 프로토콜로서, 일부 연구 결과는 6LoWPAN에서 IPSec 채택에 대한 가능성을 보여주고 있다. IPSec에서 두 통신 주체는 일반적으로 키 관리 프로토콜인 IKE를 통하여 동적으로 보안 파라미터와 비밀키를 공유하게 되는데, IKE를 그대로 6LoWPAN에 채용하기에는 많은 제약이 있다. 본 논문에서는 6LoWPAN에서 IPSec을 위한 키 관리 메커니즘의 요구 사항을 제시하고 후보 프로토콜들을 분석하여 가능성을 제시한다.

Key Words : Key Management, 6LoWPAN, IPSec, WSNs

1. Introduction

6LoWPAN (IPv6 over Low Power Personal Area Network) is a standard to enable IPv6 packets to be carried on top of low power wireless networks.[1, 2] The adoption of IPv6 on WSNs is currently being defined in the working group of the internet area of IETF. This group works on adapting IPV6 to low power WPANs employing IEEE 802.15.4.[3] Assumptions, problem statement and goals for 6LoWPAN, while the adaptation layer for the transmission of IPv6 packets over IEEE 802.15.4 is described in [4]. The usage of security mechanisms in the context of 6LoWPAN is not mostly defined. Therefore, the feasibility of employing IPSec (a

This work was supported by the research grant of the Jeju National University in 2009.
*Corresponding Author : Jungwon Cho
Tel: +82-10-2004-3297 email: jwcho@jejunu.ac..kr
Received May 24, 2012 Revised June 5, 2012 Accepted Jun 7, 2012

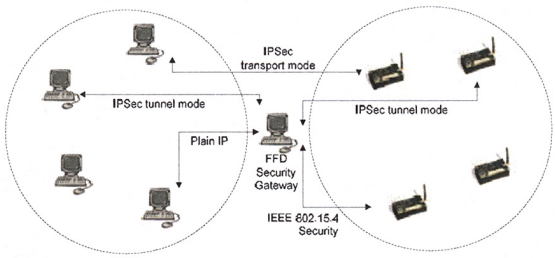
mandatory part of IPv6) with IPv6 on WSNs is currently an open issue.

Acceptance of IPSec into WSNs brings the advantage of introducing security at the network layer, thus bringing authentication and encryption transparently to higher layers protocols and solving many of the security issues previously discussed.[2 ,5]

In this paper we discuss 6LoWPAN as a standardized IP-USN with respect to its security requirements for being Efficient Key management Mechanism for IPSec on 6LoWPAN and analyze candidate protocols.

2. IPSec over 6LoWPAN

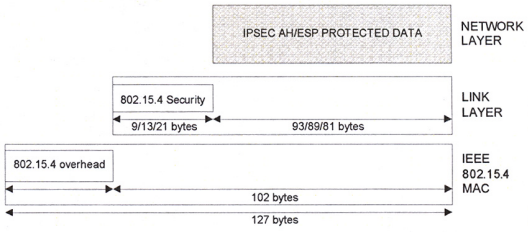
The application in 6LoWPAN needs inter-communication with the Internet. The proper security for 6LoWPAN is necessary. IPSec is already part of IPv6 that makes it a candidate to be adapted for WSNs. Figure 1 shows scenarios of IPSec over WSNs.



[Fig. 1] Scenarios of IPSec over WSNs

Security at the network layer can be achieved directly between a node on the Internet and a node on the WSNs, employing IPSec in transport mode and tunnel mode. Security on the WSNs may be accomplished using IPSec in tunnel mode to connect to a sensor node or simply by using the security mechanisms available on IEEE 802.15.4. It is currently undefined what security mechanisms can be employed above the network layer on WSNs using IPv6. Therefore, IPSec would bring the advantage of introducing security mechanisms that transport and application layers can select from. The security gateway can handle IPSec or other IP traffic from the Internet side and enforce the usage of IPSec on the WSNs. IPSec also presents benefit of being easy to integrate with new automatic key management mechanisms designed for WSNs.[1, 2]

The MAC of IEEE 802.15.4 [3] provides link layer security services that are controlled by the MAC PIB (PAN Information Base). A critical function of IEEE 802.15.4 MAC is frame security, which is actually a set of optional services that may be provided by the MAC to the upper layers (applications). If an application does not set any security parameters, then security is not enabled by default. Figure 2 illustrates the available transmission payload for IPSec at the network layer. The packet format and size at the MAC level is defined by IEEE 802.15.4. The ability of efficiently applying cryptographic algorithms to a payload can be considered a basic requirement for the successful implementation of IPSec on real sensor hardware.[2]



[Fig. 2] IPSec in the Context of 6LoWPAN

There are some limitations of 6LoWPAN, as follows: Small packet size; Low bandwidth; Low power (small battery-powered devices). This constraints existing in 6LoWPAN environments, IPSec might not be suitable as is to use in such environments. The possibility of applying IPSec to WSNs brings the advantage of introducing security at the network layer, thus bringing authentication and encryption transparently to higher layers protocols and solving many of the security issues. If the devices in the 6LoWPAN need to securely communicate with the devices at the Internet, a secure layer is required upon the 6LoWPAN layer. IPSec could be the layer. But IPSec is not always required because there is other security layer like TLS which is most useful currently. But overhead of TLS is much bigger than IPSec.[6]

IPSec basically is based on symmetric cryptography. This sentence is only correct for some key management protocols to establish the keys, like IKE. It is not needed

to support all of IPSec algorithm on 6LoWPAN. Algorithm to be implemented for interoperability can be reduced according to RFC4305. And RFC4309 defines how to use AES-CCM with IPSec so that a stack size might be reduced because IEEE 802.15.4 does include AEC-CCM. Actually, ESP of IPSec with AES-CCM requires additional 32 bytes. It is considerable. However, the security overhead of the packet size depends on the 6LoWPAN application. It might be drastically decreased. Multiple security association (SAs) between a 6LoWPAN node and different end points make packet sizes increase. However, such usage is not suitable for a 6LoWPAN node. Such usage is not realistic even for full function devices like PC.

The computational and energetic demands introduced by cryptography, although significant, do not compromise the applicability of security solutions such as IPSec on sensor nodes. The future implementation of IPSec with IPv6 on WSNs to be viable, particularly as new sensor nodes become available with more storage space and computational capabilities.

3. Requirements for Key Management on 6LoWPAN

Packets for key exchange of IPSec-6LoWPAN are obviously necessary to establish keys even if any method except manual keying are applied. In general, for key management, the most critical requirements are robustness and self-organization. Although confidentiality and integrity are important, the ability to distribute secret, shared keys satisfies both requirements, and all key management schemes are able to accomplish this. Likewise, data freshness is typically attained by including a nonce (a cryptographic time stamp) in each packet to verify that the data is new. As limitations of 6LoWPAN, the following is needed additionally:

low power consumption:

low bandwidth consumption:

Less number of messages:

We consider IKEv2 and KINK as candidate key managements for IPSec-6LoWPAN.

3.1 IKE

IKE (Internet Key Exchange) [7] is a Key Exchange protocol to establish Session Key used for transmitting data securely in IPSec. They are obviously necessary to establish keys even if any method except manual keying are applied. However, IKE requires much power to process asymmetric cryptography (RSA, DSA) comparing to low computational power devices such as sensor. Indeed, a certain algorithm like ECC or XTR [9] can save power.

IKEv2 [8] being new version of IKE have several advantages over IKEv1. The followings are the main improvements of IKEv2 from IKEv1. Key exchange process of IKEv2 is simplified with 4 to 6 message exchanges; IKEv1 needs 6 to 9 of message exchanges. IKEv2 includes the functions such as NAT Traversal, DPD, X Auth in draft. IKEv2 includes the mechanism that protects against DoS attack in IKE negotiation.

IKEv2 have lighter bandwidth and less messages than IKEv1. Therefore it can be a powerful candidate other than existing protocols. However, to be a key management protocol of 6LoWPAN, IKEv2 sould be used with ECC or XTR for saving sensor's power.

3.2 KINK

Kerberized Internet Negotiation of Keys (KINK) is a protocol definition used to set up an IPsec security association (SA), similar to Internet Key Exchange (IKE), utilizing the Kerberos protocol to allow trusted third parties to handle authentication of peers and management of security policies in a centralized fashion.

Its motivation is an alternative to IKE, in which peers must each use X.509 certificates for authentication, use Diffie-Hellman key exchange (DH) for encryption, know and implement a security policy for every peer with which it will connect,[2] with authentication of the X.509 certificates either pre-arranged. Utilizing Kerberos, KINK peers must only mutually authenticate with the appropriate Authentication Server (AS), with a Key Distribution Center (KDC) in turn controlling distribution of keying material for encryption and therefore controlling the IPSec security policy. Therefore, KINK is computationally inexpensive protocol to establish and maintain security associations using the Kerberos authentication system.

The power consumption impact in KINK is mitigated.

However, total message size of KINK is typically bigger than IKE's, as KINK reuses the Quick Mode payloads of the Internet Key Exchange (IKE), which should lead to substantial reuse of existing IKE implementations.

4. Conclusions

We showed requirements for being Efficient Key management Mechanism for IPSec on 6LoWPAN and analyze IKEv2 and KINK as candidate protocols. IPSec is the successful design and deployment of security architecture for WSNs. IPSec requires two communicating entities to share a secret key that is typically established dynamically with the IKEv2. that requires much power to process asymmetric cryptography. KINK is symmetric cryptography based KMPs using Kerberos mechanisms, and is computationally inexpensive protocol, but have more message size than IKEv2. Therefore, IKEv2 is more proper key management protocol than KINK. To be a key management protocol of IPSec-6LoWPAN, IKEv2 should be considered usage with ECC or XTR for saving sensor's power.

In the future work, we plan to research light-weight key management protocol for IPSec-6LoWPAN.

References

[1] N. Kushalnagar, et aI., IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem, Statement, and Goals (RFC 4919), Aug. 2007.

[2] J. J. Granjal, R. Silva, E. Monteiro,et aI., Why is IPSec a viable option for Wireless Sensor Networks, In: 5th IEEE International Conference on Mobile Ad Hoc and Sensor Systems, pp. 802－807. IEEE Press, New York, 2008.

[3] IEEE 802.15.4 MAC.

[4] Transmission of IPv6 Packets over IEEE 802.15.4 Networks (RFC 4944), Sep. 2007.

[5] S. Park, et aI,, IPv6 over Low Power WPAN Security Analysis, 2006.

[6] The Internet Key Exchange (IKE) (RFC 2409)

[7] The Internet Key Exchange (IKEv2) (RFC4306)

[8] Kerberized Internet Negotiation of Keys (KINK) (RFC4430)

[9] A. K. Lenstra and E. R. Verheul, The XTR Public Key System, Advances in Cryptology－CRYPTO, 2000.

Yunjung Lee [Regular member]

- Aug. 2002 : Korea Univ., Computer Science, PhD
- Sep. 2004 ~ current : Jeju National Univ., Dept. of Computer Science and Statistics. Professor

<Research Interests>
Information Security, Network Security.

Jungwon Cho [Life member]

- Feb. 2004 : Hanyang Univ., Dept. of Electronic Communication, PhD
- Sep. 2004 ~ current : Jeju National Univ., Dept. of Computer Education, Professor

<Research Interests>
Multimedia, Information Ethics, Smart Learning.