Demo Abstract: Securing Communication in 6LoWPAN with Compressed IPsec

Shahid Raza*, Simon Duquennoy*, Thiemo Voigt* and Utz Roedig†
*Swedish Institute of Computer Science, Kista, Sweden
{shahid, simonduq, thiemo}@sics.se
†Lancaster University School of Computing and Communications, Lancaster, UK
u.roedig@lancaster.ac.uk

***Abstract*—With the inception of IPv6 it is possible to assign a unique ID to each device on planet. Recently, wireless sensor networks and traditional IP networks are more tightly integrated using IPv6 and 6LoWPAN. Real-world deployments of WSN demand secure communication. The receiver should be able to verify that sensor data is generated by trusted nodes and/or it may also be necessary to encrypt sensor data in transit. Available IPv6 protocol stacks can use IPsec to secure data exchanges. Thus, it is desirable to extend 6LoWPAN such that IPsec communication with IPv6 nodes is possible. It is beneficial to use IPsec because the existing end-points on the Internet do not need to be modified to communicate securely with the WSN. Moreover, using IPsec, true end-to-end security is implemented and the need for a trustworthy gateway is removed.**

In this demo we will show the usage of our implemented lightweight IPsec. We will show how IPsec ensures end-to-end security between an IP enabled sensor networks and the traditional Internet. This is the first compressed lightweight design, implementation, and evaluation of a 6LoWPAN extension for IPsec. This demo complements the full paper that will appear in the parent conference, DCOSS'11.

I. Introduction

Researchers have unanimous consensus that security is very important for the future IP based WSN and its integration with the traditional Internet. Due to its unlimited address space, IPv6 is the obvious choice for these networks [1]. IPv6 over Low-power Wireless Personal Area Network (6LoWPAN) [2] enables carrying of IPv6 packets over IEEE 802.15.4 networks. This enables the integration of IPv6 connected wireless sensor networks with existing IP based infrastructures. Sensor nodes using 6LoWPAN can directly communicate with IPv6 enabled hosts and, for example, sensor data processing can be performed by standard servers. Thus, 6LoWPAN greatly simplifies operation and integration of WSNs in existing IT infrastructures.

6LoWPAN today relies on the IEEE 802.15.4 (referred to as 802.15.4 in the following) link-layer which provides data encryption and integrity checking. This solution is appealing since it is independent of the network protocols and is currently supported by the hardware of 802.15.4 radio chips. However, such link-layer mechanism only ensures *hop-by-hop* security where every node in the communication path (including the 6LoWPAN gateway) has to be be trusted, and where neither host authentication nor key management is supported. Furthermore, messages leaving the sensor network and continuing to travel on an IP network are not protected by link-layer security mechanisms.

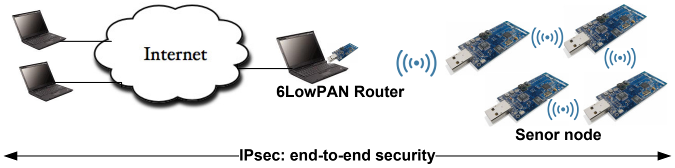

Fig. 1: We propose to use IPsec to secure the communication between sensor nodes in 6LoWPANs and hosts in an IPv6-enabled Internet. IPsec provides E2E security using existing methods and infrastructures.

The IPsec protocol suite, mandated by IPv6, provides end-to-end security for any IP communication [3]. Unlike hop-by-hop solutions, it includes a key exchange mechanism and provides authentication in addition to confidentiality and integrity. By operating at the network-layer, it can be used with any transport protocols, including potential future ones. Furthermore, it ensures the confidentiality and integrity of the transport-layer headers (as well as the integrity of IP headers), which cannot be done with a higher-level solution like TLS. For these reasons, researchers [4], [5], [6] and 6LoWPAN standardizations groups [2] consider IPsec a potential security solution for IP based sensornets, providing secure communications between Internet hosts and sensor nodes, as illustrated in Figure 1.

Our IPsec implementation the Contiki OS supports both AH and ESP protocols. It includes several standard encryption/authentication algorithms such as SHA1, AES-XCBC, AES-CBC or AES-CTR. IPsec requires both pre-shared key and certificate based mechanism for creating security association in IPsec. This means that every standard implementation of IPsec supports pre-shared key mechanisms, as we use in our implementation and in this demo. We intend to evaluate the suitability of certificate based automatic key exchange mechanisms in future.

This demonstration comes as a complement to the paper entitled *Securing Communication in 6LoWPAN with Compressed IPsec* that will appear in the parent conference, DCOSS'11 [7].

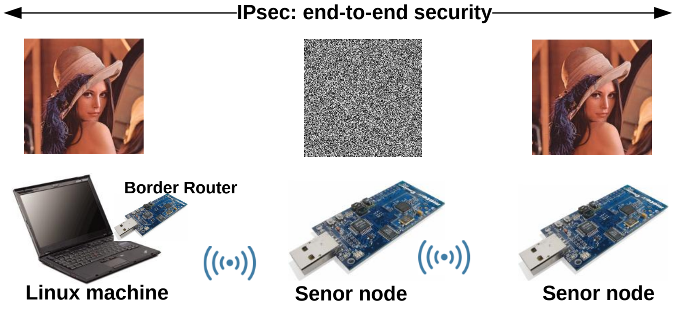

Fig. 2: The demonstration setup consisting of a standard Linux machine, border router, and two hop 6LoWPAN network. Lena's picture is secured in a end-to-end manner thanks to IPsec.

II. Demonstration Description

The purpose of our demonstration is to illustrate in a visual way the transport of confidential data over a low-power sensor network using lightweight IPsec ESP. We have implemented AH as well but this demo shows only ESP [8], which provides origin authenticity, integrity, and confidentiality protection of IP packets.

Our setup consists of a PC running out-of-the box Linux IPsec implementation, connected to a small sensornet, as illustrated in Figure 2. The network is made of Tmote sky, based on a 16-bits msp430 processor, with 10 kb RAm and 48 kb EEPROM. All motes have their own IPv6 addresses, and run Contiki with 6LoWPAN and uIP stack. They also embed our IPsec ESP implementation with authentication and integrity provided by AES-XCBC and encryption provided by AES-CBC. All motes are connected to the PC via USB, allowing to monitor and display the data received at every node.

The demonstration scenario is as follows. The PC sends private data to one of the motes in the WSN. The PC displays the original data (the famous Lena portrait) before sending it. It sends the picture to a 2-hops mote. We display the encrypted picture as seen by the intermediate mote. The encrypted picture looks like random noise. The destination node, that has a IPsec security associate with the Linux machine can decrypt the cipher-text and get the original picture. The destination node also verifies the integrity of the picture and can ensure that the picture was not modified while in transit.

We also measure response time between the source and destination. This is the time passed when a picture is sent by the sender, stored by the destination, and received back at the sender. We measure this time without IPsec, with software-implemented IPsec, and hardware enabled IPsec. We display all these times in a table and also as draws charts for comparison purpose. We show that hardware support significantly decreases the response time.

The demonstration shows that motes with limited hardware can run standard IPsec implementation, enabling end-to-end secure communications with unmodified Internet hosts. Our solution leverage IPsec as a well-known standard based on state of the art cryptographic algorithms.

III. Conclusion and Future Works

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 to secure Internet communication and we investigate if IPsec can be extended to sensor networks. We have presented the first IPsec specification and implementation for 6LoWPAN. We have extensively evaluated our implementation and demonstrated that it is possible and feasible to use compressed IPsec to secure communication between sensor nodes and hosts in the Internet.

To securely communicate with any IPv6 enabled node on the Internet pre-shared keys are sufficient but not very flexible. Therefore, we plan to investigate if an automatic key exchange protocol for 6LoWPANs based on IPsec's Internet Key Exchange protocol (IKE) is feasible.

Acknowledgments

This work has been partly performed within the SICS Center for Networked Systems funded by VINNOVA, SSF, KKS, ABB, Ericsson, Saab SDS, TeliaSonera, T2Data, Vendolocus and Peerialism. This work has been supported by VINNOVA, SSF and by the European Commission with contract FP7-2007-2-224053 (CONET).

References

[1] J. Vasseur and A. Dunkels. *Interconnecting Smart Objects with IP - The Next Internet*. Morgan Kaufmann, 2010.

[2] G. Deloche, N. Kushalnagar, J. Hui, and D. Culler. Transmission of IPv6 Packets over IEEE 802.15.4 Networks. RFC 4944, September 2007.

[3] S. Kent and R. Atkinson. Security architecture for the internet protocol, 1998.

[4] J. Granjal, R. Silva, E. Monteiro, J. Sa Silva, and F. Boavida. Why is IPsec a viable option for wireless sensor networks . In *WSNS2008*, Atlanta, USA, September 2008.

[5] R. Riaz, Ki-Hyung Kim, and H.F. Ahmed. Security analysis survey and framework design for ip connected lowpans. In *ISADS '09*, mar. 2009.

[6] R. Roman and J. Lopez. Integrating wireless sensor networks and the internet: a security analysis. *Internet Research*, 19(2):246–259, 2009.

[7] S. Raza, S. D., A. Chung, D. Yazar, T. Voigt, and U. Roedig. Securing communication in 6lowpan with compressed ipsec. In *7th International Conference on Distributed Computing in Sensor Systems (DCOSS'11)*, Barcelona, Spain, 2011. To Appear.

[8] S. Kent. IP Encapsulating Security Payload. RFC 4303, 2005.