On the design of lightweight link-layer security mechanisms in IoT systems

S. Sciancalepore*, A. Capossele†, G. Piro*, G. Boggia* and G. Bianchi‡
*Dep. of Electrical and Information Engineering (DEI), Politecnico di Bari, Italy; e-mail: {name.surname}@poliba.it.
† Department of Computer Science "Sapienza", University of Rome, Italy; e-mail: capossele@di.uniroma1.it
‡ Department of Electronic Engineering, University of Rome 2 "Tor Vergata", Italy; e-mail: giuseppe.bianchi@uniroma2.it

EXTENDED ABSTRACT

The latest estimates from the major leading companies around the world, forecasting about 50 billions of devices connected by the 2020, has certified the explosion of the Internet of Things (IoT), a world vision in which everyday objects become smart and able to interact each other and with humans, in order to provide advanced services in application domains as intelligent transportation systems, smart metering and monitoring, health-care, industrial applications, and building automation [1][2][3].

Simultaneously, the high volume of exchanged data and the sensibility of the conveyed information poses new security risks. Eavesdropping on the wireless communication channel, unauthorized access to devices, devices tampering, and privacy issues are only a subset of possible threats, but can irremediably prevent the spreading of the IoT technology, if not carefully considered.

Secure key establishment algorithms emerges as the main countermeasure, able to guarantee the protection of Machine-to-Machine (M2M) communications. Nevertheless, the straightforward adoption of well-known cryptographic algorithms and protocols, hihgly used in todays' wireless networks, is not well suited for the IoT environment, because of limited storage, energy and computational capabilities characterizing the great part of smart objects.

This work focuses on layer-2 security, the first line of defense in constrained IoT networks. In this context, the IEEE 802.15.4 standard is recognized as the leading enabling technology for short-range low-rate wireless communications [4], and covers all the details related to the Media Access Control (MAC) and physical layers of the protocol stack. Although supporting the possibility to protect MAC packets by means of symmetric-key cryptography techniques, the standard does not explain how it is possible to generate and exchange keys, but delegates upper layers to orchestrate and configure security services.

Many efforts have been produced within the ZigBee IP specification [5], IETF Working Groups (WGs) [6][7] and research communities [8], [9], [10], [11], suggesting the use of high-level protocol entities (e.g., application and transport layers), and thus involving to high computational efforts and bandwidth requirements.

This work allows the negotiation of layer-2 keys by directly using lightweight and standard compliant MAC protocols; this kind of approach could be very useful for solving issues related to bandwidth waste and limited processing capabilities available on IoT devices. Preliminary works have been discussed in [12][13][14], focusing on a layer-2 Key Management Protocol (KMP) scheme, based on authenticated Diffie-Hellman (DH) algorithm. However, such solutions integrates the use of heavy X.509 certificates, which involve an bandwidth waste and large times in order to realize the key negotiation procedure.

The conceived KMP is based on the Station-To-Station protocol structure [15] and integrates Elliptic Curve Qu-Vanstone (ECQV) algorithm, a well-known technique used to generate implicit certificates. In this way the identity of a node and its public key can be bind without requiring an explicit signature [16]. The significant reduction in terms of both certificate size and transmission requirements (bandwidth, latency, and energy consumption) makes this kind of certification technique particularly suited for the use in Low-power and Lossy Networks (LLNs).

The conceived KMP scheme, illustrated in fig. 1, integrates the Station-to-Station (STS) protocol and ECQV scheme, allowing the negotiation of a session key by means protecting all communications between any pair of nodes.

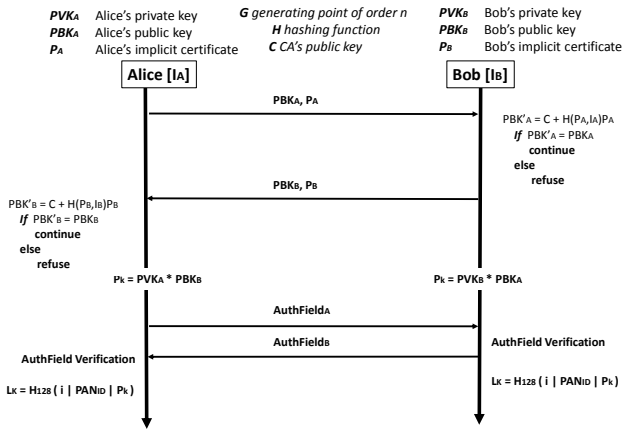

Fig. 1. Steps of the key negotiation phase.

It is very important to remark that ECQV, in its original version, jointly offers key agreement and authentication services. As a consequence, the latest two messages provided by the STS protocol could be made optional.

If devices involved in the secure communication wants to verify the correct key computation by the counterpart, the latest two messages are necessary; in this way a node realizes the presence of an attack (e.g., a Man-In-The-Middle (MITM) attack), because it is not able to verify the mutual authentication and correctly generate the shared key.

Tab.I highlights how the proposed approach asks for the lowest bandwidth requirements, if compared to lighter version of Datagram Transport Layer Security (DTLS) and Internet Key Exchange (IKE) protocols (described in [17] and [18], respectively), and other approaches discussed in [14] and [19], thus being more suitable for LLN scenarios.

TABLE I
COMPARISON AMONG PROTOCOL OVERHEADS.

Considered strategy	**Logical messages**	**MAC packets**
Proposed approach	4	4
Proposal in [14]	4	22
Proposal in [19]	6	59
Lightweight version of DTLS proposed in [17]	7	60
Lightweight version of IKE proposed in [18]	11	69

Moreover, the described KMP scheme has been implemented within the OpenWSN protocol stack [20], on top of the security extension recently presented in [21]. Some tests has been conducted using the TelosB hardware platform, in order to understand the impact that the described KMP has on regular protocol stack operations.

The implementation required a number of tricks, adopted to overcome some relevant challenges emerged from the TelosB limited capabilities. In summary, they are:

- integration of KMP messages in a real protocol;
- implementation of optimized elliptic curve operations;
- timing settings;
- management of time-expensive Elliptic Curve Cryptography (ECC) operations and de-synchronization events;
- administration of the workload at the coordination side;

Fig. 2 shows that the highest computational effort is required for calculating the public key from the implicit certificate and the *Pre Link Key*. Starting from this premises, the first mandatory part of the KMP scheme is completed in little more than 16 s.

Finally, we evaluated the impact that parallel KMP sessions coordinated by a single device has on the overall time needed to establish a secure domain. Fig. 3 shows that, considering a star topology composed by up to 5 child node, the mandatory phase can be completed in less than 100 s, while the complete procedure lasts for about 150 s if the mutual authentication phase is realized.

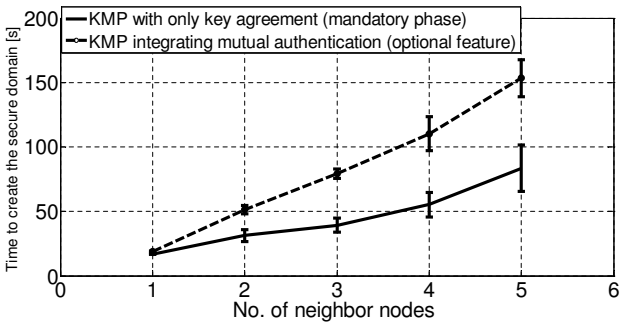

Fig. 3. Duration of concurrently KMP schemes in a star topology, with basic and completed KMP.

REFERENCES

[1] B. Emmerson, "M2M: the Internet of 50 billion devices," *Huawei WinWin Magazine Journal*, no. 4, pp. 19–22, Jan. 2010.

[2] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, Privacy & Trust in Internet of Things: the road ahead," *Computer Networks (Elsevier)*, vol. 76, pp. 146–164, 2015.

[3] L. A. Grieco, A. Rizzo, S. Colucci, S. Sicari, G. Piro, D. Di Paola, and G. Boggia, "IoT-aided robotics applications: technological implications, target domains and open issues," vol. 54, December 2014.

[4] IEEE std. 802.15.4, *Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs)*, Standard for Information Technology Std., 16 June 2011.

[5] ZigBee IP Specification Overview. [Online]. Available: http://www.zigbee.org/Specifications/ZigBeeIP/Overview.aspx

[6] S. Chasko, S. Das, R. Marin-Lopez, Y. Ohba, P. Thubert, and A. Yegin, "Security Framework and Key Management Protocol Requirements for 6TiSCH draft-ohba-6tisch-security-01," IETF, Internet Draft, Mar. 2014.

[7] M. Richardson, "security architecture for 6top: requirements and structure draft-richardson-6tisch-security-architecture-02," IETF 6tisch WG, Internet Draft, Apr. 2014.

[8] M. Brachmann, S. L. Keoh, O. Morchon, and S. Kumar, "End-to-End Transport Security in the IP-Based Internet of Things," in *Int. Conf. on Comp. Commun. and Netw. (ICCCN)*, 2012, pp. 1–5.

[9] S. Raza, H. Shafagh, K. Hewage, R. Hummen, and T. Voigt, "Lithe: Lightweight Secure CoAP for the Internet of Things," *IEEE Sensors J.*, vol. 13, no. 10, pp. 3711–3720, 2013.

[10] P. Varadarajan and G. Crosby, "Implementing IPsec in Wireless Sensor Networks," in *Proc. of Int. Conf. on New Technologies, Mobility and Security (NTMS)*, Mar. 2014, pp. 1–5.

[11] L. Veltri, S. Cirani, G. Ferrari, and S. Busanelli, "Batch-based group key management with shared key derivation in the Internet of Things," in *Proc. of Int. Wir. Comm. and Mob. Comp. Conf. (IWCMC)*, Jul. 2013, pp. 1688–1693.

[12] G. Piro, G. Boggia, and L. A. Grieco, "A Standard Compliant Security Framework for IEEE 802.15.4 Networks," in *Proc. of IEEE World Forum on Internet of Things (WF-IoT)*, Seoul, South Korea, Mar. 2014.

[13] S. Sciancalepore, G. Piro, E. Vogli, G. Boggia, and L. Grieco, "On securing IEEE 802.15.4 networks through a standard compliant framework," in *Proc. of EuroMed Telco Conference (EMTC) 2014*, Naples, IT, November 2014.

[14] Piro, G. and Boggia, G. and Grieco, L.A., *A standard compliant security framework for Low-power and Lossy Networks draft-piro-6tisch-security-issues-03 (work in progress)*, IETF 6TiSCH WG, Dec. 2014.

[15] W. Diffie, P. C. Van Oorschot, and M. J. Wiener, "Authentication and authenticated key exchanges," *Des. Codes Cryptography*, vol. 2, no. 2, pp. 107–125, Jun. 1992.

[16] D. Hankerson, S. Vanstone, and A. Menezes, *Guide to Elliptic Curve Cryptography*. Springer, 2004.

[17] S. Raza, D. Trabalza, and T. Voigt, "6LoWPAN Compressed DTLS for CoAP," in *Proc. of IEEE Int. Conf. on Distr. Comp. in Sensor Systems (DCOSS)*, May 2012, pp. 287–289.

[18] ——, "Lightweight IKEv2: A Key Management Solution for both the Compressed IPsec and the IEEE 802.15.4 Security," *Workshop on Smart Object Security, Paris*, Mar. 2012.

[19] G. Bianchi, A. T. Capossele, A. Mei, and C. Petrioli, "Flexible key exchange negotiation for wireless sensor networks," in *Proc. of ACM*

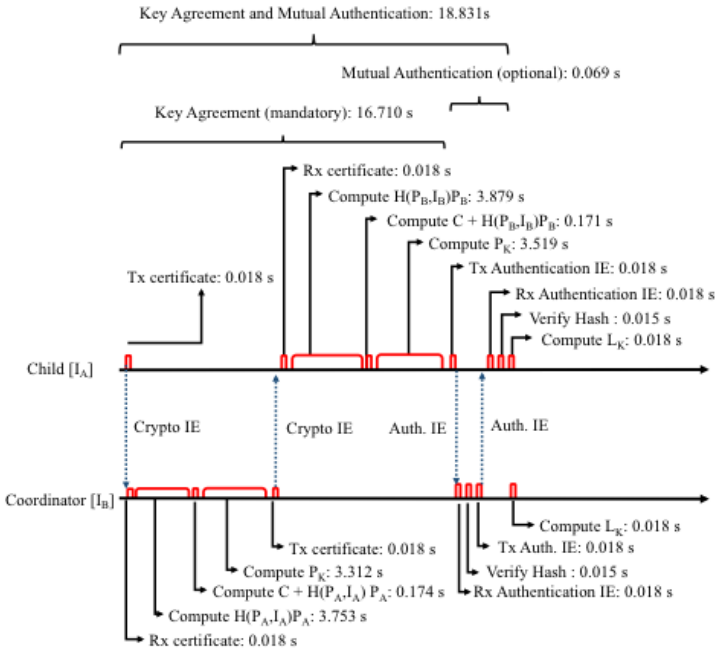

Fig. 2. Temporal diagram of the proposed KMP and relative durations on TelosB hardware platform.

Int. Workshop on Wirel. Netw. Testbeds, Experim. Eval. and Charact., 2010, pp. 55–62.

[20] T. Watteyne, X. Vilajosana, B. Kerkez, F. Chraim, K. Weekly, Q. Wank, S. Glaser, and K. Pister, "OpenWSN: a standards-based low-power wireless development environment," *Tans. on Emerg. Telecom. Technol.*, vol. 23, no. 5, p. 480–493, 2012.

[21] S. Sciancalepore, G. Piro, G. Boggia, and L. A. Grieco, "Application of IEEE 802.15.4 security procedures in OpenWSN protocol stack," *IEEE Standards Education e-Magazine*, 2014, to appear.