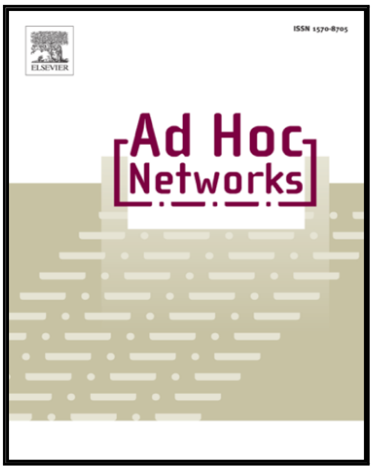
Accepted Manuscript



6LowPSec: An End-to-End Security Protocol for 6LoWPAN

Ghada Glissa, Aref Meddeb

PII: S1570-8705(18)30029-5
DOI: 10.1016/j.adhoc.2018.01.013
Reference: ADHOC 1634

To appear in: *Ad Hoc Networks*

Received date: 29 March 2017
Revised date: 3 December 2017
Accepted date: 30 January 2018

Please cite this article as: Ghada Glissa, Aref Meddeb, 6LowPSec: An End-to-End Security Protocol for 6LoWPAN, *Ad Hoc Networks* (2018), doi: 10.1016/j.adhoc.2018.01.013

6LowPSec: An End-to-End Security Protocol for 6LoWPAN

Ghada Glissa[a,*], Aref Meddeb[b]

[a] *National Engineering School of Tunis, University of Tunis-El Manar, Tunisia*
[b]*National School of Engineering of Sousse, University of Sousse, Tunisia*

Abstract

6LoWPAN has radically changed the IoT (Internet of Things) landscape by seeking to extend the use of IPv6 to smart and tiny objects. Enabling efficient IPv6 communication over IEEE 802.15.4 LoWPAN radio links requires high end-to-end security rules. The IEEE 802.15.4 MAC layer implements several security features offering hardware hop-by-hop protection for exchanged frames. In order to provide end-to-end security, researchers focus on lightweighting variants of existing security solutions such as IPSec that operates on the network layer. In this paper, we introduce a new security protocol referred to as "6LowPSec", providing a propitious end-to-end security solution but functioning at the adaptation layer. 6LowPSec employs existing hardware security features specified by the MAC security sublayer. A detailed campaign is presented that evaluates the performances of 6LowPSec compared with the lightweight IPSec. Results prove the feasibility of an end-to-end hardware security solution for IoT, that operates at the adaptation layer, without incurring much overhead.

Keywords: Internet of Things, 6LoWPAN, End-To-End Security, IPSec, IEEE 802.15.4, Routing Protocols

1. Introduction

The mash-up of captured data with retrieved Internet data gives rise to new synergistic services that surpass the services supported by isolated embedded systems. This new vision introduced by the Internet of Things (IoT) allows IP communication and interaction between objects possessing computing and sensorial capabilities [1]. This lead to the definition of Low Power and Lossy Networks (LLN) composed of a large number of constrained devices characterized by limited power and memory processing, high loss rates, and short-range wireless communications [2][3].

With respect to all these constraints, defining appropriate protocol stacks covering all aspects, from application to radio layer, has became a major concern of researchers and industrials. To address this need, the Internet Engineering Task Force (IETF) created the 6LoWPAN Working Group (IPv6 in Low-Power Wireless Personal Area Networks) [4]to standardize necessary adaptations of IPv6 for networks that use the IEEE 802.15.4 physical and MAC layers [5].

Provision of an end-to-end security connection is key to ensure fundamental functionalities. In fact, 6LoWPAN takes advantage of the strong AES-128 link-layer security mechanisms provided by IEEE 802.15.4 [5], but this robust hardware solution is restricted to hop by hop security, i.e., end-to-end security is managed by upper layers. End-to-End (E2E) security solutions protect communications between IP enabled sensors and the traditional Internet.The 6LoWPAN Border Router (6LBR) [6] has the responsibility to interconnect the traditional Internet with the LLN and to allow access to 6LoWPAN devices. Thus, the 6LBR is the best part where one should implement E2E security features.

While IPSec [7] and Transport Layer Security (TLS) [8] are mature and proven technologies in the world of the Internet, their adaptation to the LoWPAN world is still a challenge. These protocols require considerable amounts of resources and substantial overhead.

A protocol that compresses IPSec headers only in transport mode is provided in [9][10][11]. This protocol implements the route-over routing scheme. However, despite the compression, this protocol remains unsuitable for constrained devices due to its overhead and heavy key establishment process i.e., the Internet Key Exchange protocol (IKEv2) [12].

On the other hand, the use of DTLS (Datagram Transport-Layer Security) to secure the CoAP (Constrained Application Protocol) application layer raises many questions about its implementation and its usability in the real world is still unproven [13][14]. The new design of DTLS for IoT requires the use of a header compression scheme, which could compromise end-to-end security properties provided by the original DTLS protocol. Further, its handshake (for authentication and key agreement scheme, using ECC (Elliptic Curve Cryptography), is unsuitable for constrained devices due to the fragmentation of large messages performed at the adaptation. This implies retransmission and reordering of DTLS handshake messages. In addition, this solution does not support multicast communications, which is a major requirement in IoT environments.

The lack of authentication at the 6LoWPAN layer renders fragmentation mechanisms vulnerable despite some lightweight defense mechanisms. In fact, there is a proposal

[*] Corresponding author. Tel: +216 53950898 +216 98646281
Email addresses: ghadaglissa@gmail.com (Ghada Glissa), Aref.Meddeb@infcom.rnu.tn (Aref Meddeb)