Ad Hoc Networks 82 (2019) 100–112

Contents lists available at ScienceDirect

Ad Hoc Networks

journal homepage: www.elsevier.com/locate/adhoc

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

ARTICLE INFO

Article history:
Received 29 March 2017
Revised 3 December 2017
Accepted 30 January 2018
Available online 2 February 2018

Keywords:
Internet of Things
6LoWPAN
End-to-end security
IPSec
IEEE 802.15.4
Routing protocols

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.

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 [9–11]. 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 compres-

[*] Corresponding author.
E-mail addresses: ghadaglissa@gmail.com (G. Glissa), Aref.Meddeb@infcom.rnu.tn (A. Meddeb).

https://doi.org/10.1016/j.adhoc.2018.01.013
1570-8705/© 2018 Elsevier B.V. All rights reserved.

sion 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 to protect 6LowPAN networks against packet fragmentation attacks [15,16],

In this paper, we propose a new security solution, referred to as 6LowPSec, implemented over the 6LoWPAN adaptation layer of the Contiki OS, but running using the Mesh-under routing (LOADng) scheme. 6LowPSec benefits from the existing hardware security features of the IEEE 802.15.4 MAC layer. Our goal is to prove the feasibility of our solution and to compare its performance with that of lightweight IPSec solution.

The remainder of the paper is organized as follows. In Section 2, we provide a brief survey on the work done so far on 6LowPan Security as well as the routing methods. Section 3 details the 6LowPSec security protocol. Performance evaluation of 6LowPSec and a comparison with the lightweight IPSec is presented in Section 4. In Section 5, we deal with security and performance analysis of proposed protocol. Finally, conclusions and perspectives are given in Section 6.

2. State of the art

The 6LoWPAN standard enables an efficient use of IPv6 over low power and lossy networks [17]. The gateway device, generally the border router device, runs the fragmentation function and the header compression to forward 6LoWPAN packets between WSNs and the Internet [18]. Security is one of the major issues that must be addressed for such networks [19,20]. Protecting internal communication between network nodes is achieved thanks to the IEEE 802.15.4 security sublayer [21] while securing the communication between the LoWPAN and IPv6 end devices is made using heavyweight legacy security protocols such as lightweight IPSec or DTLS [22]. Routing is one of the factors that may impact security, so we distinguish two types of routing : mesh-under routing and route-over routing [23].

2.1. 6LoWPAN security

Security is a critical and costly trade-off for Low Power and Lossy Networks (LLNs) [24,25]. It can be handled at the link layer, the network layer, and/or the application layer. IEEE 802.15.4 security sublayer guarantees the protection of the wireless medium defined as hop-by-hop security, whereas upper layers security is designed to achieve end-to-end security between two distant equipments. Such networks will be open to many security threats related to the Internet as well as the local network itself [26,27]. Thus providing security using cryptography techniques is required to provide anonymity, privacy *confidentiality*, and integrity to the communicating IoT devices.

2.1.1. IEEE 802.15.4 security

Link layer security is implemented between the MAC and the network layer, referred to as the IEEE 802.15.4 security sublayer [5,28]. All the IEEE 802.15.4 frames are cryptographically protected in order to ensure integrity, authentication, freshness, and optionally confidentiality. The general format of the IEEE 802.15.4 frame is depicted in Fig. 1. The Frame Control field is depicted in Fig. 2.

Octets:2	1	0/2	0/2/8	0/2	0/2/8	0/5/6/10/14	Var.	2
Frame Control	Sequence Number	Destination PAN Id	Destination Address	Source PAN Id	Source Address	Auxiliary Security Header	Frame Payload	FCS
		Addressing Fields						
MHR							MAC Payload	MFR

Fig. 1. IEEE 802.15.4 frame format.

Bits:2	3	4	5	6	7-9	10-11	12-13	14-15
Frame type	Security Enabled	Frame pending	AR	PAN Id Compression	Reserved	Destination Addressing Mode	Frame Version	Source Addressing Mode

Fig. 2. Frame control field.

Octets: 1	4	0/5/9
Security Control	Frame Counter	Key ID

Fig. 3. Format of the auxiliary security header.

Bits: 0-2	3-4	5-7
Security Level	Key Identification Mode	Reserved

Fig. 4. Security control field format.

The Auxiliary Security Header field specifies security related information [5]. This field is present only if the Security Enabled field is set to one. The Auxiliary Security Header field has a variable length and contains three subfields: Security Control, Frame Counter, and a Key Identifier (see Fig. 3).

The Security Control field provides information regarding the type of protection to be applied to the frame. It contains three subfields: Security Level, Key Identifier Mode, and a Reserved field (see Fig. 4).

The Security Level contains a value that indicates the level of frame protection that is provided. This value can be set on a frame-by-frame basis, allowing various security levels depending on application needs. The cryptographic protection offered by the various security levels is given in Table 1. Note that replay protection is provided for all security level values higher than 0. Replay protection is provided by means of the Frame Counter field.

The Key Identifier Mode field indicates whether the key can be derived implicitly or explicitly. It is also used to indicate the particular representations of the Key Identifier field if derived explicitly. The Key Identifier Mode field is set to one of the values given in Table 2. The Key Identifier field (Fig. 5) of the Auxiliary Security Header is present only if the Key Identifier Mode field has a value superior to 0×00.

The Key Source field indicates the originator of a group key, where a group key is defined as a key that is known only to a set of devices. If the Key Identifier Mode field indicates a 4 bytes Key Source field, then the Key Source field is in fact the macPANId of the originator of the group key, right concatenated with the macShortAddress of the originator of the group key. Note that the macPANId is the identifier of the PAN on which the device is operating. If the device is not associated to a PAN, then the value of the mac-

Table 1
Security levels.

Security Level	Security Level field bits 2 1 0	Security Attribute	Data Confidentiality	Data Authenticity	Encrypted Auth. Tag length (bytes)
0	000	None	OFF	NO	0
1	001	MIC-32	OFF	YES	4
2	010	MIC-64	OFF	YES	8
3	011	MIC-128	OFF	YES	16
4	100	ENC	ON	NO	0
5	101	ENC-MIC-32	ON	YES	4
6	110	ENC-MIC-64	ON	YES	8
7	111	ENC-MIC-128	ON	YES	16

Table 2
Values of the Key Identifier Mode field.

Key Identification Mode	Key Identification Mode bits 1 0	Description	Key Id field length
0×00	00	Key is determined implicitly from the originator and recipient of the frame as per the header	0
0×01	01	Key is determined from the Key index field	1
0×02	10	Key is determined explicitly from the 4octet Key source field and Key index field	5
0×03	11	Key is determined explicitly from the 8octet Key source field and Key index field	9

PANId is set to 0×FFFF. Further, the macShortAddress is the address that the device uses to communicate in the PAN.

If the Key Identifier Mode field indicates an 8 bytes Key Source field, then the Key Source field is set to the macExtendedAddress (i.e., the IEEE address assigned to the device) of the originator of the group key [3].

Finally, the Key Index field allows unique identification of different keys with the same originator. It is up to each key originator to make sure that the actively used keys that it issues have distinct key indices and that the key indices are all different from 0×00.

We note that the included Figs. 1–5 and Tables 1 and 2 respects the security specifications format of the IEEE 802.15.4 standard [5].

2.1.2. Lightweight IPSec

IPSec [7] offers integrity and optionally confidentiality of IP (v4 or v6) packets exchanged between two peers. It is performed for devices which are not subject to severe restrictions on battery life, memory allocation, processing and transmission. IPSec supports AH (Authentication Header) for authenticating the IP header and ESP (Encapsulating Security Protocol) for authenticating and encrypting the payload.

Given the inherent constraints of 6LoWPAN networks, IPSec may not be suitable to be used in such environment. IPSec introduces additional overhead (AH or ESP) and requires more bits to be transmitted, and thus more energy consumption. Further, IPSec involves two communicating peers to share a secret key that is typically established dynamically with the Internet Key Exchange (IKEv2) protocol [12]. Thus additional packet overhead will be provoked by IKEv2 exchanges. All these circumstances leads us to lighten this security protocol in order to adapt it to such constrained networks.

Raza et al. [29] proposed a compressed lightweight design, implementation, and evaluation of 6LoWPAN extension for IPSec that is based on already existing compression mechanisms used for compressing IPv6 packets as HC13. In fact HC13 [30] offers context aware header compression mechanisms: the LoWPAN_IPHC (IPHC) encoding for IPv6 header compression and the LoWPAN_NHC (NHC) encoding for the next header compression. This latter could be used to encode AH and ESP extension headers. It is feasible to employ the AH and ESP header in combination, evidently the compressed AH and ESP headers could be used in succession. The AH header is identified by 1101 value in the NH_ID, as for the ESP header is identified by 1110.

Octets: 0/4/8	1
Key Source	Key Index

Fig. 5. Format for the Key Identifier field, if present.

Bit	0	1	2	3	4	5	6	7
LOWPAN_NHC_AH	1	1	0	1	PL	SPI	SN	NH

Fig. 6. LOWPAN_NHC_AH encoding.

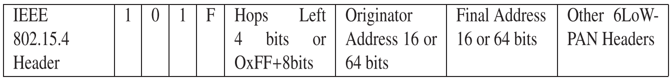
Bit	0	1	2	3	4	5	6	7
LOWPAN_NHC_ESP	1	1	1	0	SPI	SN	-	NH

Fig. 7. LOWPAN_NHC_ESP encoding.

Figs. 6 and 7 illustrate respectively the AH and ESP security extension headers compressed using NHC encoding. The next header field specifies the transport layer protocol used by a packet's payload by indicating which extension header follows such as TCP, UDP, ICMPv6. This field is reduced to two bits. In both security headers, the sequence number field is reduced to two bytes, it ensures safety against replay attacks. Concerning the Security Parameters Index (SPI), which also compressed to two bytes, is responsible for identifying the number of security associations to which the packet belonged.

The payload length in the AH security header is limited to three bits given the restriction of the maximum payload size available with 6LoWPAN. The size of authentication and payload (encrypted) blocks is variable for both AH and ESP security extensions.

In regards to the ESP specifications, the payload is preceded by an Initialization Vector of 8 bytes and succeeded by a vari-



IEEE 802.15.4 Header	1	0	1	F	Hops Left 4 bits or OxFF+8bits	Originator Address 16 or 64 bits	Final Address 16 or 64 bits	Other 6LoWPAN Headers

Fig. 8. 6LoWPAN mesh header.

able Integrity Check Value (ICV) field. The size of the later field depends on the encryption used algorithm and on the security level.The ability of efficiently applying different cryptographic algorithms with different key sizes is considered one fundamental requirement for the successful usage of the new compressed 6LoWPAN security headers.

This proposal is limited to the use of Internet pre-shared keys and could be enhanced by the deployment of IPSec's Internet Key Exchange protocol (IKE). However the idea of compression and appeasement of existing security protocols remains limited and does not make sense when it is to dump efficient protocol of its basic values.

2.2. Routing in 6LoWPAN networks

Routing in 6LoWPAN networks is one of the biggest challenge [31]. There are indubitable routing requirements needed to be satisfied using 6LoWPAN routing protocol like supporting various traffic patterns, diverse communication, scalability, security performances, and distinct routing conditions. 6LoWPAN supports two routing modes: mesh-under and route-over [23]. In practice, mesh-under routing is reflected in LOADng (6LoWPAN Ad Hoc On-Demand Distance Vector Routing Next Generation) [32] and route-over routing is interpreted by RPL (Routing Protocol for Low Power and Lossy Networks) [33].

2.2.1. Route-over vs. mesh-under

In mesh-under, the 6LoWPAN adaptation layer performs routing, the network layer does not fulfill any IP routing [23]. The adaptation layer forwards frame fragments to the destination over multiple radio hops. Routing and forwarding are accomplished at the link layer based on IEEE 802.15.4 header or the 6LoWPAN header. To reach a particular destination, the EUI 64 bit address or the 16 bit short address is used to forward a fragment to a neighbour node. Multiple link layer hops are sought as a single IP hop. In order to determine the source and the destination of a single IP hop within the PAN, 6LoWPAN employs the concept of originator and final address, respectively.

The 6LoWPAN mesh header (4–5 bytes) is depicted in Fig. 8. The mesh header is used to encode the hop limit and the link layer source and destination of the packets. The values of Originator (O bit) and the final destination (F bit) fields are set to 1 if the address is 16 bits and 0 if the address is 64 bits. The Hops left field is used to limit the number of hops between the source and the destination.

The Hops left field is typically coded on 4 bits allowing up to 15 hops, which should be enough for a PAN. The value of 0×F is used to indicate that an extra byte is added, allowing up to 255 hops.

An IP packet is fragmented by the adaptation layer granting each fragment a datagram_tag, the common identifier to all fragments of the same Ip packet, and a datagram_offset, the position of the fragment in the IP packet. Different fragments of an IP packet can be routed via different paths and will be reordered at the destination. If all fragments are delivered to the destination node successfully, the adaptation layer reassembles all fragments and creates an entire IP packet. In case of any loss of fragment, all fragments of the IP packet will be retransmitted.

In route-over, all routing decisions are taken at the network layer and each node acts as an IP router i.e., each hop behaves as an IP hop in terms of routing. IP routing tables and IPv6 hop-by-hop options are used to forward packets. For routing and forwarding decisions, the network layer uses the additional encapsulated IP header [23].

It is widely agreed that route-over performs better than mesh-under in terms of total number of transmissions while mesh-under outperforms route-over in terms of latency.

2.2.2. LOADng

LOADng [32,34] is a lightweight variant of AODV [35] that emerged as an alternative solution intended for use through IEEE 802.15.4 devices in 6LoWPAN and LLN environments. It is standardized by the ITU under the recommendation ITU-T G.9903 [36]. This standard is deployed in particular by the Linky program of smart communicating electricity meters within the context of ERDF and Enexis projects.

LOADng inherited basic operations of AODV, encompassing generation and forwarding of Route Request RREQs to discover a route to a specific destination. Upon receiving RREQ message, only the indicated destination could respond by a RREP (Route Reply) and forward it on unicast, hop-by-hop to the RREQ originator. When receiving RREP message, intermediate devices will unicast a proper RREP_ACK (Route Reply Acknowledgement) to the neighbor from which they obtained the Request message, to the amount of notifying that the link is bidirectional. Moreover, if a route is identified broken, an error message should be returned to the data packet source.

As in any reactive routing protocol, routes are established only when there is data to be sent and there is any path towards destination. Routes are maintained for as long as there is traffic using this path. One of the main drawbacks of LOADng is the route discovery delay.

This protocol is layer-agnostic. It means it may be used at layer 3 as a route over protocol or at layer 2 as a mesh under routing protocol. In our case, it is employed through the 6LoWPAN adaptation layer in order to reach our end-to-end security solution based on hardware security specifications.

2.2.3. RPL

RPL is a promising routing protocol designed for optimizing 6LoWPAN operations. It was introduced in 2012 by the Internet Engineering Task Force (IETF) Routing over Low Power and Lossy Networks (ROLL) group to present a standardized protocol over IPv6 [33]. It is supposed to provide multipoint-to-point routing from nodes in the LoWPAN towards a central control node named sink and viceversa; hence authorizing bi-directional links.

RPL is a distance-vector routing protocol,it adopts Destination Oriented Directed Acyclic Graphs(DODAG), a special tree topology, routed at a single destination. The graph is constructed by the use of an Objective Function (OF) which defines how the routing metric is computed especially rank metric that specifies the position of nodes through the DODAG. Sink node, the DAG root, is responsible for building the network graph topology. It broadcasts its ID, rank and other network information through a DIO (DODAG Information Object).

When intermediate nodes receive the DIO message, it replies the root to be chosen as preferred parent. Then, the designated nodes calculate and update its own rank to send DIO messages to their own neighbours. This process pursues until reaching the leaf nodes. When a node receives a DIO message from more than one neighbour, it has to select its preferred parent rank, energy and other network metrics. In addition, when a device does not receive a DIO message within a specific time to join the DODAG, it should solicit its neighbours by sending DIS (DODAG Information Solicitation) messages.

This routing mechanism is recommended at the network layer when using an IPv6 end-to-end security solution as lightweight IPSec.

2.3. 6LoWPAN key management considerations

The characteristics of 6LoWPAN motes such as limited resources, lack of physical protection, unattended operation, and a close interaction with the physical environment, all make it infeasible to implement some of the most popular key exchange techniques in their literal forms. In fact, the three widely known schemes such as trusted-server, pre-distribution and public key schemes are unsuitable for 6LoWPAN [37].

Trusted-server schemes such as Kerberos rely solely on the server for key agreement between nodes. If the server is compromised, the trust amongst nodes is severed. Such scheme is not suitable for 6LoWPAN s because typically there is no guarantee whatsoever of seamless communication with a trusted server at anytime.

In the pre-distribution or key agreement scheme, the key is distributed among communicating nodes prior to deployment. However, because of the dynamics of nodes, knowing the set of neighbours a priori is not feasible. Further, the presence of intruders at the network deployment and initiation phase may not be possible to detect. Some schemes such as network-shared keying, pair-wise keying, and group keying, have been identified as other key distribution options. However, while featuring the same security level as key pre-distribution, these schemes cannot cope with network dynamics [37].

In [38], a Lightweight Key Establishment and Management Protocol in Dynamic Sensor Networks (KEMP) is proposed. With this protocol, a router or cluster head is employed as sub-base-stations to execute key establishment, avoiding the dependency on a centralized server or base station for key establishment. Also, this reduces the number of hops between two communicating ends which, in turn, reduces the communication cost.

Finally, a promising key management scheme for 6LoWPAN would be based on Elliptic Curve Cryptography (ECC). This is a public-key cryptography based on the algebraic structure of elliptic curves over finite fields. Some implementations have proven ECCs feasibility for sensor networks. In fact, ECC provides security levels comparable to those provided by RSA or AES (Advanced Encryption Standard), but with much smaller key size [37].

3. 6LowPSec protocol

3.1. Why 6LowPSec?

6LowPSec is a new security protocol that aims to introduce effective security features through adaptation 6LoWPAN layer thanks to the safety specifications already existing at the IEEE 802.15.4 MAC security sublayer. This new mechanism requires mesh-under routing turned on adaptation layer that provides low level end-to-end communication between terminals with the intention to facilitate the integration of embedded link layer security features. So it preserves the advantage of performing security functions at the link layer which can be implemented in the hardware. Further, the novel approach envisages security performance with optimal quality of services in such restricted network conditions as opposed to IPSec that exhibits a mitigated effectiveness when dealing with overhead and data transfer delay. In fact, IPSec requires about 50 bytes of overhead. The overhead tax and increased delay can be very costly for end users, especially point-to-point links using static routes, where it is not essential to perform cryptography and security checks at the network layer.

Regarding security requirements, our 6LowPSec complies with all security rules specified by the IETF draft [37]. It supplies confidentiality, authentication, integrity, data and key freshness, network availability, survivability, resistance, and robustness despite the presence of attack(s). So all these performances take advantage of the CCM* which is an extension of the Counter mode encryption and Cipher block chaining Message authentication code (CCM). This generic combined encryption and authentication block cipher mode employs the Advanced Encryption Standard (AES) in order to encrypt payload data. 6LowPSec is implemented under the MAC security sublayer presenting a hardware aspect unlike IPSec encryption which is performed by the software. Thus there are no hardware devices capable of performing layer 3 encryption at very high speeds. All these properties demonstrates that the use of 6LowPSec is crucial in future generation networks.

3.2. Protocol description

The 6LoWPAN Security Protocol (6LowPSec) performs security functions (cipher, integrity check, authentication etc.) only at end devices specially 6LoWPAN border router, without requiring any additional network security functions. It preserves the advantages of performing security functions at the link layer which can be implemented in the hardware. These security features, already specified at the IEEE 802.15.4 MAC layer, perfectly protect data transmitted to each hop. The main purpose of 6LowPSec is to provide end-to-end security, but with minimum overhead, with minimum processing, and especially with minimum control information exchange, so that it can be used to securely deliver time sensitive traffic in resource-constrained environments.

According to IEEE 802.15.4 specifications [5], if the macSecurityEnabled attribute is set to FALSE and the SecurityLevel parameter is not equal to zero, the procedure shall return with a status of UNSUPPORTED_SECURITY. What we suggest here is that in such case, we need to lookup the Reserved subfield of the Security Control field (see Fig. 4). The Reserved subfield may be renamed as end-to-end Security field. If this three-bit field is set to 0×0, then the UNSUPPORTED_SECURITY must be returned. Otherwise, this field can be coded in the same manner as for the standard security i.e., as mentioned in Table 2, delivering the same standard security features but between edge devices only. In this case, when a device receives a frame with the Security Enabled field set to one, it checks the Security Level field. If this latter is set to (000)2, then it checks the end to end Security field i.e., the Reserved field in the current version of IEEE 802.15.4 standard. If this latter is set to (000)2, then the procedure should return UNSUPPORTED_SECURITY. Otherwise, if Destination Address corresponds to the receiving device, this latter shall perform security functions according to the security level indicated in the end-to-end Security field, as mentioned in Table 2.

If the destination address does not match that of the receiving device, this latter shall forward the frame without performing any security functions, but it verifies the CRC and performs routing. If no payload ciphering is performed, then routing can be performed using either route-over or mesh under. However, if ciphering is used, then only the mesh-under scheme can be used since route-over requires the network layer header information to perform routing. Here, we need to check the first bit of the Security Level field. If this bit is set to 1 (ciphering is performed) then the 6LoWPAN device should accept only the mesh-under routing scheme.

If the route-over strategy is required, then the payload ciphering cannot be applied. Note that this is somewhat reasonable since in general, we apply mesh-under to reduce delay, while by implementing ciphering we add delay. If ciphering is required along with route-over, then we must not use end-to-end security but rather the currently supported standard i.e., hop-by-hop security.

3.3. Security association and key management

Upon discovery of a new destination MAC address, an originator node establishes an End-to-End Security Association (EESA) with its counterpart. In order to confine the key exchange process, this is done only once during an initial phase and only if there is at least one data frame that needs to be sent to that particular MAC address. This key exchange is carried out in a secure way. The security includes an authentication (signature), a confidentiality (ciphering) and integrity check.

The number of keys exchanged in the initial phase can be specified by the network administrator. These keys have a length of 128 or 256 bits (16 or 32 bytes) each. Keys are transmitted in a consecutive sequence of Key Frames (KF). Since we do not have an EESA yet, the KFs are ciphered using the standard IEEE 802.15.4 security level 5 at least. The number of KFs exchanged depends on the number of keys set by the administrator.

In order to simplify the protocol and reduce overhead, we limit the maximum number of keys exchanged in this initial phase to 12 keys (see below). We believe this number is sufficient. Indeed, if we assume that we need a new key every one hour, an EESA can last 12 h without reusing keys. Since keys are explicitly transmitted in dedicated frames (the KFs), we can use any key generation algorithm which ought to be known only by the end devices.

Upon the reception of all the KFs (and thus of all the keys), the recipient returns a single Acknowledgement Frame (AF). The AF is protected in the same manner as the KFs. Moreover, the order of the keys is modified by the recipient. The new key order is indicated in the AF. The purpose of modifying the order of keys is to increase security. The ACK also makes sure that the recipient received all the keys.In the case where the AF is lost, the sender retransmits the keys after a timeout. Once the sender receives the AF, an EESA becomes active and the transmission of Data Frames (DF) is allowed.

The Keys are stored in a Key Data Base (KDB) which includes the keys and their order. Note that the network administrator may reset the KDB by triggering a new key exchange phase.

The EESA is established between a pair of nodes as soon as an originator node must transmit a frame to a new destination MAC address. An exchange of KF and AF frames will take place.

A station that sends the KFs will enter into EESA activation state and waits for an AF to activate the EESA. The station that receives a KF enters into a Key learning phase. Note that we generally have two EESAs, one in each direction. An EESA is identified by the MAC address of the other end within the KDB. One station may have as many EESAs as the number of communicating devices. The formats of the KF, AF, and DF frames are given in Fig. 9. We can notice that we need only one additional byte for end-to-end security functions in the data frames, corresponding to the Frame ID (FID) and the Key Number as seen in Fig. 9(a).

In order to distinguish the KF, AF and DF frames, 6LowPSec uses the first two bits of the Frame ID (FID) field. For a DF frame, the key-number field is used to identify the key that was used by a sender to encrypt the frame. For the KF frame, the FID field is 00XX where the X bits are used as KF sequence numbers. This sequence number is needed since the order of the KF frames is not guaranteed at the receiving end.

IEEE 802.15.4 Header	FID 4 bits 1000	Key Number 4 bits	Payload (6LoWPAN header + Application data) X bytes

(a) Data Frame

IEEE 802.15.4 Header	FID 4 bits 00XX	Number of Keys 4 bits	Keys n (128 or 256) bits

(b) Key Frame

IEEE 802.15.4 Header	FID 4 bits 0100	Number of Keys 4 bits	Keys Order n4 bits

(c) ACK Frame

Fig. 9. The 6LowPSec frame formats.

Since the data field of a IEEE 802.15.4 frame can be as low as 102 bytes i.e., 127 minus 25 header-bytes, when the keys are encoded on 128 bits (16 bytes), each KF frame can transport up to 102/ 16 = 6 keys. Since the maximum number of keys is set to 12, the maximum number of Key Frames necessary to transfer all the keys is two KFs. When we use 256 bits keys, we need 4 KFs (three keys per KF frame). These frames are numbered using the XX bits of FID field.

In the AF frame, the number of received keys is indicated in order to increase the reliability of the protocol. The field Keys Order indicates the new order of the keys.

It should be noted that we may set the order of the keys according to a particular reordering algorithm, but that would add complexity. Because the new order of the keys is explicitly indicated in the AF frame, the receiver will not have to run any algorithm to determine the key order, which accelerates the frame delivery process.

Note that in order to perform end-to-end security and routing functions, the originator and final addresses are not ciphered in the Mesh header.

Upon the reception of a frame, a node checks the destination address field. If it matches its own address, and if there is an ESSA established with the source, then it performs security functions such as integrity check, authentication and deciphering, according to the requested security level.

When an originator node receives a new frame from the 6LoWPAN adaptation layer, it checks if it already established an EESA with the final destination. If so, it applies appropriate security functions and forwards the frame to the next hop. Otherwise, it establishes an EESA with the final destination and then it forwards the frame.

Fig. 10 depicts the state diagram for the sender side for establishing an EESA and exchanging DF frames. The EESA is initialized when a frame has to be sent to a MAC address with which there is no EESA and security must be applied. In fact, security is applied only when it is required. The initiator of the EESA sends KF frames to the designated destination and waits to verify the Cyclic Redundancy Check (CRC) when receiving Acknowledgement frames. Once the check phase is successful, the security association persists active,leading to a secure data exchange according to the security level and until session expiration. The mismatch of the security frames or the failure of the authentication check leads immediately to clearing the EESA.

On the other hand, Fig. 11 gives the state diagram for the receiver side. The EESA is initialized upon the reception of the K Frames. Then, an ACK frame should be sent with a new key order allowing hence the secure data exchange. While the EESA has an Active state, received data frames should be verified according to the ciphering algorithm.

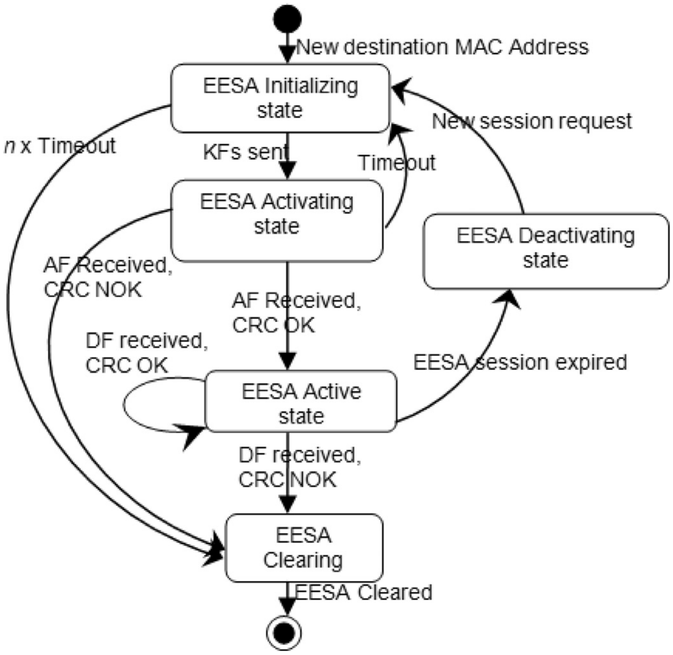


Fig. 10. The 6LowPSec EESA state diagram- sender side.

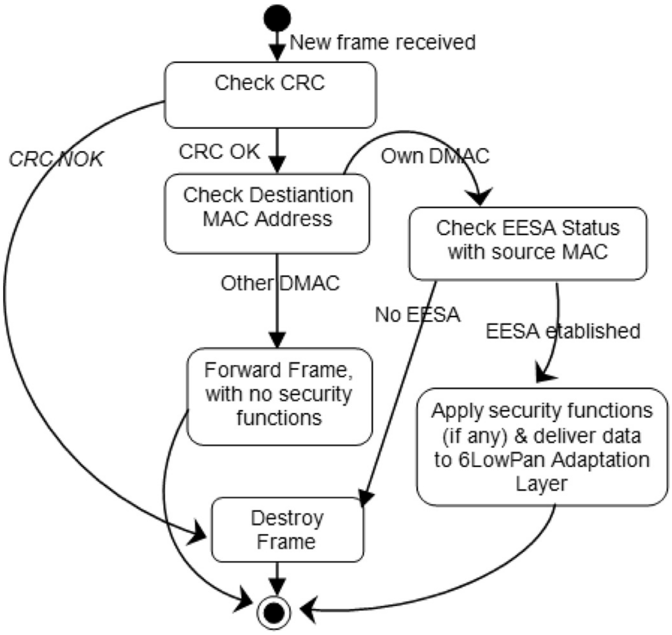

New frame received
Check CRC
CRC NOK
CRC OK
Own DMAC
Check Destiantion MAC Address
Check EESA Status with source MAC
Other DMAC
No EESA
EESA etablished
Forward Frame, with no security functions
Apply security functions (if any) & deliver data to 6LowPan Adaptation Layer
Destroy Frame

Fig. 12. Receive frame state diagram.

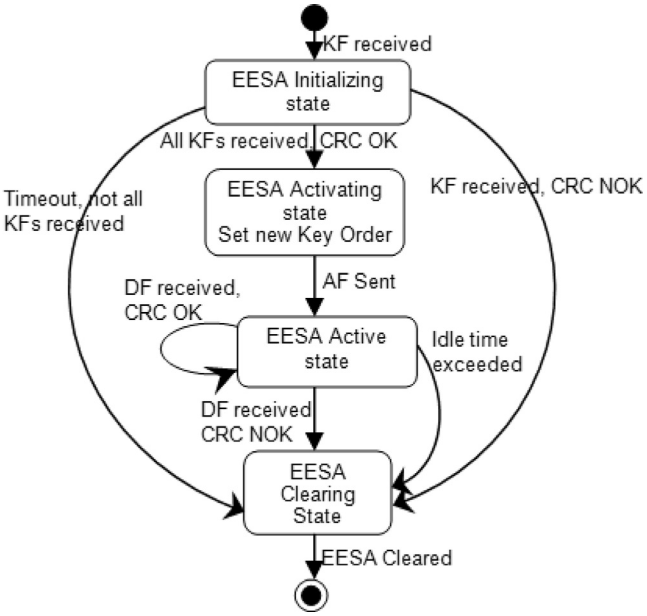


Fig. 11. The 6LowPSec EESA state diagram- receiver side.

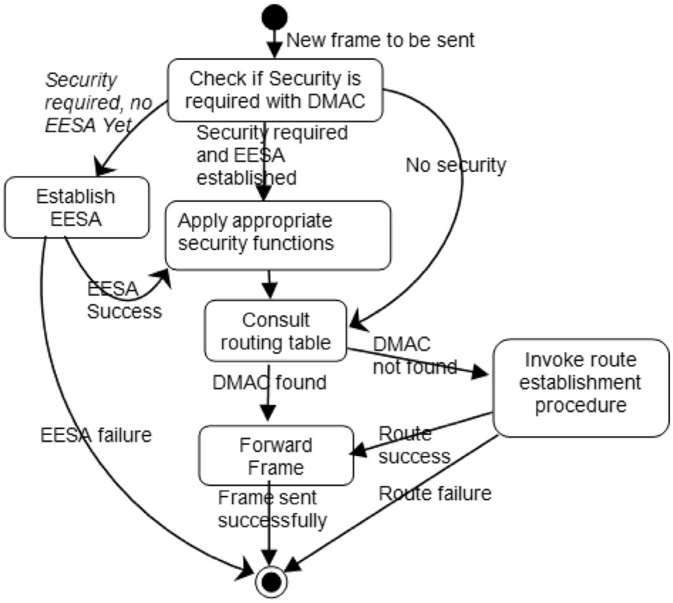

New frame to be sent
Security required, no EESA Yet
Check if Security is required with DMAC
Security required and EESA established
No security
Establish EESA
Apply appropriate security functions
EESA Success
Consult routing table
DMAC not found
Invoke route establishment procedure
DMAC found
EESA failure
Forward Frame
Route success
Frame sent successfully
Route failure

Fig. 13. Send frame state diagram.

Fig. 12 gives the state diagram for the frame reception procedure. A receiver of an IEEE 802.15.4 frame checks if the destination is its own MAC. Otherwise, the DF is forwarded to the next hop until reaching the final destination. The destination device checks if security and EESA apply. If so, then the received frame will be deciphered and/or authenticated as needed. Nevertheless, the lack of the security association EESA, given in Figs. 10 and 11, prevents data interpretation.

On the other hand, Fig. 13 depicts the send frame procedure state diagram. As we can notice, only when security is required and EESA shall security functions apply. Hence, the encrypted Data Frame should be forwarded until reaching the destination, respecting certain the routing table. The absence of the security association when the MAC security is enabled engenders the EESA establishment process detailed in Figs. 10 and 11.

4. Performance evaluation

In this Section, we quantify performance of the proposed 6LowPSec protocol for securing 6LoWPAN networks. After describing our implementation and experimental setup, we evaluate the impact of our E2E security protocol 6LowPSec in terms of packet size, energy consumption, duty cycle, latency and efficiency while comparing it with the famous lightweight IPSec.

4.1. Experimental evaluation setup

Before proceeding with the description of the simulation setup, it is worth noting that Link layer security services can be assured by using the TinySec solution, which offers confidentiality, message integrity, and authenticity for TinyOS [39]. The same services are offered by the network layer through ContikiSec [40].

The integration of the 6LowPSec security protocol is carried out on Contiki operating system [41] that already provides 6LoWPAN functionality.This embedded operating system, using the COOJA network simulator, allows a comprehensive evaluation of the new security scheme. It presents flexible tools, written in C development language, enabling the easy deployment of the MAC and 6LoWPAN security extension. The implementation requires the modification of the existing Contiki rime stack that accommodate mesh-under routing as well as the uIP stack affording route-over routing (RPL). Rime is a layered communication stack for sensor networks, with much tinner layers than traditional architectures and which was designed to simplify the implementation of communication protocols, it was revised in order to implement the LOADng routing protocol proposed by Martinez [42] and to promote the use of IEEE 802.15.4 MAC security specifications at the adaptation layer. Concerning the uIP stack, an optimized TCP/IP stack, has been modified to support IPSec/6LoWPAN compression mechanisms as NHC AH, and NHC ESP encodings.

Security features as confidentiality and authenticity are provided using AES-CCM-128 algorithm to ensure 6LowPSec implementation. As for IPSec integration we focused on the Raza proposition [9] which embed AES-XCBC for ESP integrity and AES-CBC for encryption.

The demonstration scenario is composed of 2 border routers(6LBR) and 50 sky motes randomly localized as specified in Fig. 14. Tmote Sky nodes are characterized by a 16-bit msp430 MCU, a 48 kB of ROM, a 10 kB of RAM, and an external Flash memory. Nevertheless, border routers have enhanced storage and computational capabilities. These IoT devices were designed to secure the end-to-end (E2E) communication between the LoWPAN and the Internet hosts using different routing protocols for different security rules. The main aim is to emphasize the need of introducing our hardware end-to-end security solution.

Zolertia Z1 motes [43,44], running on Contiki OS and compliant with IEEE 802.15.4, are the best environment to introduce embedded security peculiarly the 6LoWPSec scheme.

4.2. Comparing IPSec and 6LowPSec overhead

The authors in [29] suggest the use of a compressed IPSec mode for 6LoWPAN. However, the effectiveness of that protocol has not been proven yet. Further, [45] proposes a compression format for IPSec, able to offer end-to-end security that utilises a variant of AES in Counter with CBC- MAC mode (AES-CCM). Unfortunately, both proposals are rather provide alternatives to layer 3 security approaches, deemed ineffective for sensor networks as they cannot be implemented in the hardware.

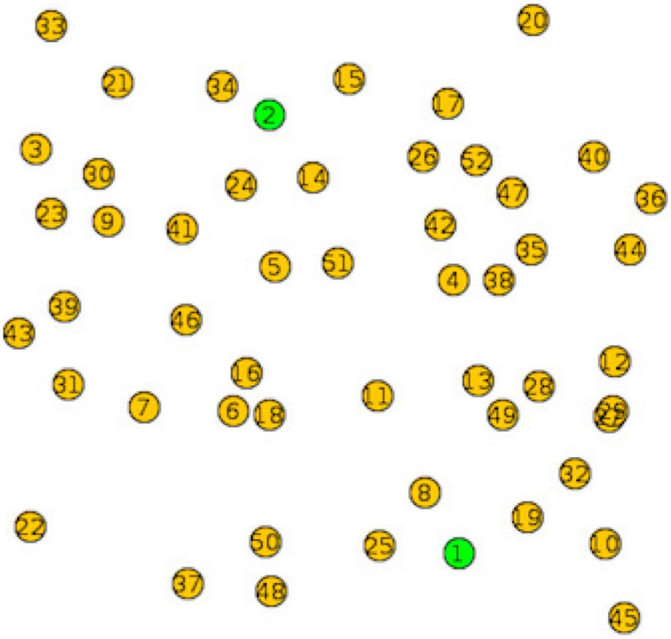


Fig. 14. Simulation topology: 2 6LBR and 50 sky motes.

Table 3 gives the overheads assuming a 512 bytes application data per fragment. When IPSec (native and compressed) is used, we assumed that IEEE 802.15.4 security is disabled. Since 6LowPSec applies the same security services as IEEE 802.15.4, we only add one byte of security overhead for the FID (4 bits) and Key numbering (4 bits).

Note that at the small average packet sizes, typical in today's converged networks, IPSec overhead reaches 40 to 50 percent of total bandwidth; while actual measurements have shown up to 90 percent overhead. Furthermore, note that despite IPSec header compression, we are still dealing with significant overhead. As suggested in, "when you're working with nodes that send very small messages and maximum frame sizes of 128 bytes (including link headers), every byte counts."

Further, recalling that 6LowPSec only requires security treatment at the end devices, overhead, computation, and processing power are significantly reduced in intermediate nodes.

4.3. Energy consumption

Securing the 6LoWPAN networks has an added cost in terms of energy usage. Thuse, we evaluate the energy overhead of

Table 3
Comparing IPSec, 6LowPSec AND MACSEC overhead (BYTES).

IEEE 802.15.4	Uncompressed IPSec	Compressed IPSec	6LowPSec
AES-CTR	AES-CBC	AES-CBC	AES-CTR
5	18	12	$5+1=6$
AES-CBC-MAC- 96	HMAC-SHA1-96	HMAC-SHA1-96	AES-CBC- MAC-96
12	24	16	$12+1=13$
AES-CCM-128	AES-CBC and HMAC-SHA1-96	AES-CBC and HMAC-SHA1-96	AES-CCM- 128
21	30	24	$21+1=22$

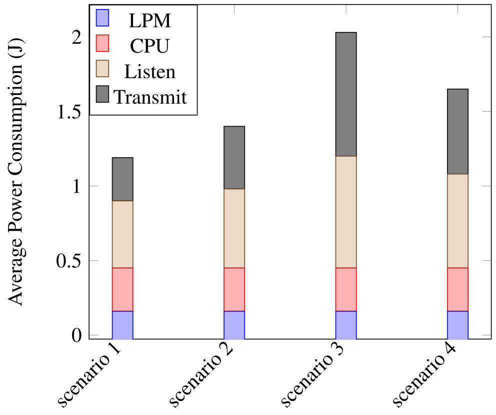


Fig. 15. Comparison of power consumption over one hour, during scenario1 No security + RPL routing, scenario2 No security + LOADng routing, scenario3 IPSec + RPL routing, scenario4 6LowPSec + LOADng routing.

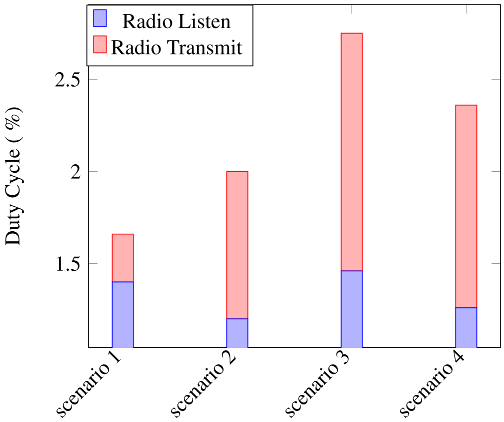


Fig. 16. Comparison of duty cycle during scenario1 No security + RPL routing, scenario2 No security + LOADng routing, scenario3 IPSec + RPL routing, scenario4 6LowPSec + LOADng routing.

the available security options on the Tmote Sky using Contiki integrated energy estimator. To evaluate the energy consumption rate, we proceed measures in terms CPU, LPM (Low Power Mode), Transmit and Listen modes existing on the Contiki Powertrace.

Fig. 15 depicts the power consumption evolution for different security scenarios of LOADng and RPL routing without security, IPSec coupled with IPV6 layer routing and 6LowPSec using adaptation layer routing. This evaluation is supported by measurement of the duty cycle as described in Fig. 16 that expresses the percentage of time during which devices are active.

These results demonstrate that LOADng is more energy-intensive than RPL routing since nodes are in permanent transmission of packets fragments and paths' discovery unlike RPL routing which builds the routes at the beginning, following a DODAG graph. This is reflected by the difference in duty cycle that seems remarkable for LOADng routing. Nevertheless, this equation will be overthrown by the introducing of security features in different network and adaptation layers.

On the other hand, we can notice that the energy consumption with IPSec is significantly higher than with 6LowPSec since it requires authentication and encryption at each hop and imposes complicated security processing than 6LowPSec. 6LowPSec, which that takes advantages of the MAC security sublayer; consumes less power and less calculation time.

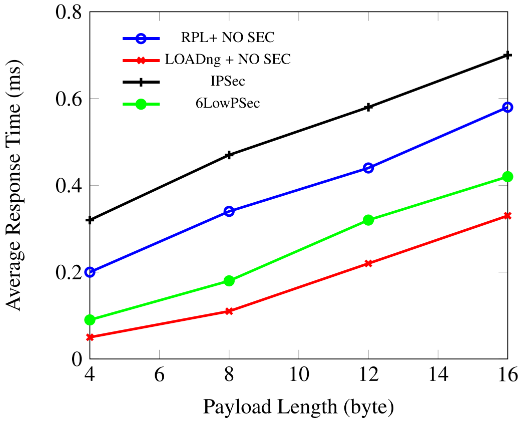


Fig. 17. Comparison of the average response time of RPL without attack scenario, a selective forwarding and increased rank attack scenario and a Secure-RPL scenario during 30 min.

4.4. System-wide response time overhead

Latency or response time is the delay of data transmission between a sensor node and an IPv6 host. This simulation factor is important to evaluate the network performance. We conduct experiments using a fixed routing distance of four hops and different payload lengths that vary between 4 and 16 bytes.

Fragmentation and packet reassembly is one of the most crucial considerations that influence response time. In fact, fragmentation is needed when the IP datagram size is too large to fit a single IEEE 802.15.4 packet, the reassembly process and its delay differs from one routing protocol to another which is very noticeable in Fig. 17. RPL routing requires packet reassembly at each hop and obviously encryption and authentication of the global information, contrary to LOADng that ensures packet reconstruction and security measures at end points.

We can notice that the Response Time overhead grows linearly with datagram sizes but it is much higher with IPSec than 6LowPSec. This is due to the adapted routing protocol as well as to the security algorithms used for each end-to-end security mechanism. Thus, 6LowPSec yields lower latency, which will have a good impact on the number of received messages, as we will illustrate below.

4.5. Packet Delivery Ratio

Packet Delivery Ratio(PDR) is defined as the ratio between received packets by the destination (the wired host) and generated packets by the source (6LoWPAN motes).

In the experiments, two kinds of end-to-end security protocols are used based on two different routing mechanisms RPL and LOADng. LOADng is faster than RPL in terms of latency, but this rapid progress may affect the efficiency of the global network since it requires the retransmission of packet in case of loss of fragments when gathering them at the destination node.

Fig. 18 shows that this trade off is no longer valid with the use of security mechanisms. The introduction of security features at the adaptation layer reduces the loss of fragments by precluding intruder or non-trusted end devices from falsifying the datagram_tag or the datagram_offset thus increasing the delivery ra-

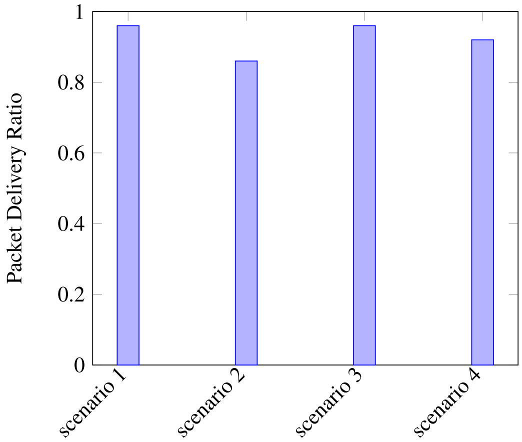


Fig. 18. Comparison of packet delivery ratio: scenario 1 No security + RPL routing, scenario 2 No security + LOADng routing, scenario 3 IPSec + RPL routing, scenario 4 6LowPSec + LOADng routing.

Table 4
Sent and received data messages during one simulation hour.

Protocol	RPL	LOADng	Compressed IPSec	6LowPSec
Sent	295	485	140	320
Received	271	368	129	288

tion of the network. The use of IPv6 security improves relatively the PDR value to reach hence its maximum, nevertheless this does not reflect the network freshness in terms of the number of exchanging packets. Indeed, Table 4 indicates that the number of sent secured messages using 6LowPSec, during one hour of stimulation, is more important than using lightweight IPSec. Then, despite the approximation of the PDR values of the two security protocols, our new security approach presents more updated sensing measures.

5. Security analysis

The variety of application domains that take benefit from the 6LoWPAN networks, gives rise to several security threats and concludes to various security needs. In this section, we analyse the robust security features of our 6LoWPSec protocol, we identify the considered countermeasures and recommendations to deal with various attack scenarios and then we emphasize the importance of the hardware E2E security.

5.1. Robust security features

6LoWPSec proposal offers four main security services in order to achieve high network protection. First, it is able to limit the network access and the data manipulation to only authorized users when imposing authentication and key exchange processes. Using the CCM* cryptographic block cipher mode, our security protocol enables the message sender to generate an encrypted authentication tag U described in Algorithm 1 and using the accurate key specified during the association and key management phase. Thus, for a confidentiality measures, the message receiver has access to the message content only when verifying the identity between its generated tag MACTag and the sender Tag T defined respectively in Algorithms 2 and 1.

Algorithm 1: CCM*: The sender side.

```
Require: EndToEndSecurityEnabled= TRUE
         $SecurityLevel > 0$
Input  : Key
         $AddAuthData = l\|MHR\|OpenPayloadfield$
         PlaintextData=Unsecured Private Payload field
         $AuthData = AddAuthData\|PlaintextData$
Output : Ciphertext
         U
while TRUE do
    $AuthData = B1\|B2\|\ldots\|Bt$
    for (x=0 ; x ≤ t; x++) do
        $X_{i+1} := E(Key, X_i \oplus B_i)$
    end
    $T = X_{t+1}\&((1 << 8 \times m) - 1)$
    $PlaintextData = M_1\|\ldots\|M_t$
    for (x=0 ; x ≤ t; x++) do
        $A_i = Flags\|NonceN\|Counter_i$
        $C_i = E(Key, A_i) \oplus M_i$
    end
    $Ciphertext = C_1\|\ldots\|C_t\&((1 << 8 \times l) - 1)$
    $S_0$:= E(Key, $A_0$)
    $U = (S_0\&((1 << 8 \times m) - 1)) \oplus T$
end
```

Algorithm 2: CCM*: The receiver side.

```
Require: EndToEndSecurityEnabled= TRUE
         $SecurityLevel > 0$
Input  : Key
         Ciphertext
         U
Output : Valid/Invalid
while TRUE do
    $Ciphertext = M_1\|\ldots\|M_t$
    for (x=0 ; x ≤ t; x++) do
        $A_i = Flags\|NonceN\|Counter_i$
        $P_i = E(Key, A_i) \oplus M_i$
    end
    $UnCiphertext = P_1\|\ldots\|P_t\&((1 << 8 \times l) - 1)$
    $S_0$:= E(Key, $A_0$)
    $MACTag = (S_0\&((1 << 8 \times m) - 1)) \oplus U$
end
```

Likewise, this verification process defends the reliability of the data transmitter, then making sure about its trustworthiness.

In addition, our security scheme offers integrity by preventing data modification during transmission between the transmitter and the receiver. It therefore ensures the data encryption thanks to the Advanced Encryption Standard (AES). This block cipher algorithm, with variable MIC length, shall guarantee the data encryption through the originator device (the Ciphertext in Algorithm 1) and the data decryption at the end device (the UnCiphertext in Algorithm 2).

Moreover, the malicious intrusion detection is a major criterion of our 6LoWPSec protocol. It prevents then several attacks such as Replay attack, Deny of Service attack, black-hole attack, etc. from

Octets: 8	4	1
Source address	Frame counter	Security level

Fig. 19. CCM* Nonce.

exercising data espionage or network serious damage.This will be analyzed in the following subsection.

With:
MHR: MAC header
T, MACTag: the authentication tag
U: the encrypted authentication tag
Ciphertext: the encrypted message
UnCiphertext: the decrypted message
E: the AES block cipher encryption function
Key: the encryption key
X_i, A_i: intermediate value of CBC-MAC
B_i, P_i: the Input block for CBC-MAC
m: number of octets in authentication field
l: number of octets in payload field

5.2. Threat analysis

Security threats observed in 6LoWPAN network could be limited thanks to the 6LoWPSec efficiency. Then, protecting communication between 6LowPAN motes and IPv6 hosts in the presence of attacks shall ameliorate the network quality of services.

5.2.1. Replay attack

Repay attack is a breach of security in which unauthorized information is maintained and then retransmitted to trick the addressed node into unauthorized operations such as false identification or a duplicate transaction. The presence of Nonce, Fig. 19, as a special marker, or a timestamp or a counter provides a mechanism for preventing intruders from replaying unauthorized message. Nonce is refreshed after each session expiration. The AH security header of the lightweight IPSec includes protection against replays, but gives rise to extra overhead.

5.2.2. Deny of service attack (DoS)

The DoS attack is considered as one of the most destructive attack since it acts directly on QoS. Its main aim is the disruption of services by limiting the access to a key device as the border router in our case (6BR) and then rendering the whole network unable to furnish normal progress. Analysis of this kind of attack is made via the Contiki OS while introducing an attacker node, connected directly to the 6BR and attempting to delaying collected messages at this gateway device. By launching repeated request message, the adversary node absorbs the bandwidth and overload the target node. Fig. 20 demonstrates the degradation of the network performances during the increasing of the traffic load. It has a direct impact on the average transmission delay. The 6LoWPSec protocol considers this node as an intruder and hinders it to communicate with the network, hence the amelioration of the transmission delay. Nevertheless, the compressed IPSec stops this type of attack, but it needs more time to achieve its additional computing security instructions.

5.2.3. Data loss attack

This attack results in black-hole or selective forwarding attack when respectively, messages could be totally or partially dropped.

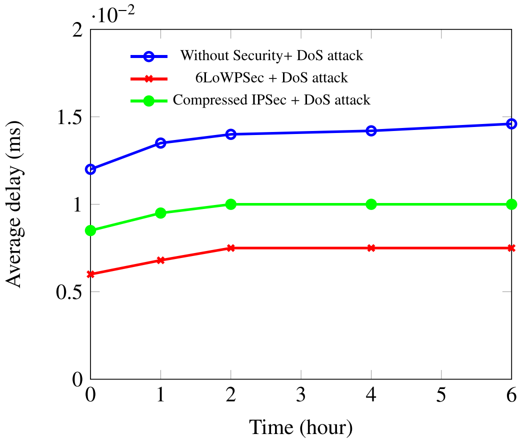


Fig. 20. Average delay with/without security in presence of DoS attack.

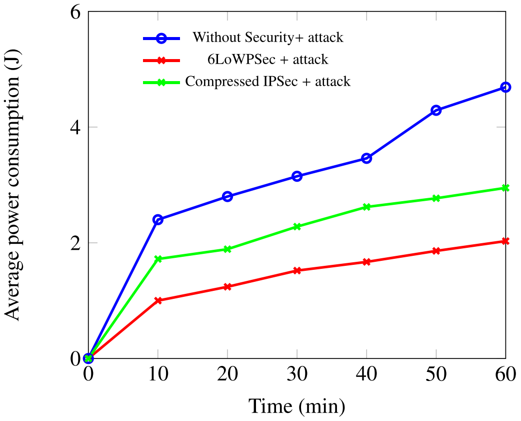


Fig. 21. 6BR average power consumption with/without security in presence of ping of death attack.

Since our security architecture offers a challenge-response mechanism, irregular forwarding or dropping of packets could be rapidly detected.

5.2.4. Battery exhaustion attack

The energy depletion attack aims to force power consumption and thereafter reduces the node lifetime. Our attack scenario consists in injecting an intruder node between the LoWPAN and the wireless host that enchains the sending of ping of death messages. Fig. 21 shows the battery exhaustion of the 6BR in the absence of security mechanism, nevertheless this unauthorized device will be stopped while adopting 6LoWPSec security for reasons of incompatible authenticity. It furthermore presents more energy consumption moderation than the compressed IPSec during detecting the adversary device.

5.3. Hardware E2E security

As a hardware solution, 6LoWPSec offers embedded E2E security services. This unique feature makes it robust against network attacks. It limits, then stealing the cryptographic material during message exchange. The hardware key storage and the embedded ciphering operations are unbeatable in the presence of intrusions.

Then, the IEEE 802.15.4 MAC security sublayer adopted by our proposal needs a hardware deployment. Thus, nowadays, several commercial solutions present secure architectures with a limited number of tiny electronic components.

6. Conclusion

We have introduced 6LowPSec, a novel end-to-end security protocol for 6LoWPAN, which operates at the adaptation layer. 6LowPSec alleviates the need for upper layer security mechanisms and allows hardware implementation of end-to-end security. The proposed solution has been implemented and tested through Contiki operating system. It has proven its efficiency compared with upper layer security solutions such lightweight IPSec. Thus, we can confirm that 6LowPSec behaves quite well with respect to latency and memory footprint. The impact of the security solution into the global system is acceptable while assuming the presence of favorable conditions such as mesh-under routing (LOADng) and existing security features of the MAC IEEE 802.15.4 layer.

As future work, we need to propose the hardware deployment of our solution on real sensor devices. Furthermore, it is envisaged to evolve our key management proposition.

Supplementary material

Supplementary material associated with this article can be found, in the online version, at doi:10.1016/j.adhoc.2018.01.013.

References

[1] J. Ko, A. Terzis, S. Dawson-Haggerty, D.E. Culler, J.W. Hui, P. Levis, Connecting low-power and lossy networks to the internet, IEEE Commun. Mag. 49 (4) (2011).
[2] C. Bormann, M. Ersue, A. Keranen, Terminology for Constrained-Node Networks, Technical Report RFC 7228, 2014.
[3] K. Pister, P. Thubert, S. Dwars, T. Phinney, Industrial Routing Requirements in Low-Power and Lossy Networks, Technical Report RFC 5673, 2009.
[4] N. Kushalnagar, G. Montenegro, C. Schumacher, IPv6 over low-power wireless personal area networks (6LoWPANs): overview, assumptions, problem statement, and goals, Technical Report, 2007.
[5] I. W. Group, et al., Ieee standard for local and metropolitan area networks part 15.4: low-rate wireless personal area networks (lr-wpans), IEEE Std. 802 (2011) 4–2011.
[6] L.M. Oliveira, J.J. Rodrigues, A.F. de Sousa, J. Lloret, A network access control framework for 6lowpan networks, Sensors 13 (1) (2013) 1210–1230.
[7] K. Seo, S. Kent, Security Architecture for the Internet Protocol, Technical Report RFC 4301, IETF Network Working Group, 2005.
[8] T. Dierks, The Transport Layer Security (TLS) Protocol Version 1.2, Technical Report RFC 5246, 2008.
[9] S. Raza, S. Duquennoy, T. Chung, D. Yazar, T. Voigt, U. Roedig, Securing communication in 6lowpan with compressed ipsec, in: 2011 International Conference on Distributed Computing in Sensor Systems and Workshops (DCOSS), IEEE, 2011, pp. 1–8.
[10] S. Raza, S. Duquennoy, G. Selander, Compression of IPsec AH and ESP Headers for Constrained Environments draft-raza-6lowpan-ipsec-01, Technical Report, Internet-Draft, 2013.
[11] J.-C. Park, A.-H. Jun, A lightweight ipsec adaptation for small devices in ip-based mobile networks, in: 2006 8th International Conference Advanced Communication Technology, 1, IEEE, 2006, p. 5.
[12] S. Raza, T. Voigt, V. Jutvik, Lightweight ikev2: a key management solution for both the compressed ipsec and the ieee 802.15. 4 security, in: Proceedings of the IETF workshop on smart object security, 23, 2012.
[13] T. Kothmayr, C. Schmitt, W. Hu, M. Brünig, G. Carle, Dtls based security and two-way authentication for the internet of things, Ad Hoc Netw. 11 (8) (2013) 2710–2723.
[14] S. Raza, H. Shafagh, K. Hewage, R. Hummen, T. Voigt, Lithe: lightweight secure coap for the internet of things, IEEE Sens. J. 13 (10) (2013) 3711–3720.
[15] H. Kim, Protection against packet fragmentation attacks at 6lowpan adaptation layer, in: Convergence and Hybrid Information Technology, 2008. ICHIT'08. International Conference on, IEEE, 2008, pp. 796–801.
[16] R. Hummen, J. Hiller, H. Wirtz, M. Henze, H. Shafagh, K. Wehrle, 6lowpan fragmentation attacks and mitigation mechanisms, in: Proceedings of the Sixth ACM Conference on Security and Privacy in Wireless and Mobile Networks, ACM, 2013, pp. 55–66.
[17] G. Mulligan, The 6lowpan architecture, in: Proceedings of the 4th Workshop on Embedded Networked Sensors, ACM, 2007, pp. 78–82.
[18] J.W. Hui, D.E. Culler, Extending ip to low-power, wireless personal area networks, IEEE Internet Comput. 12 (4) (2008) 37–45.
[19] J. Granjal, E. Monteiro, J.S. Silva, Security in the integration of low-power wireless sensor networks with the internet: a survey, Ad Hoc Netw. 24 (2015) 264–287.
[20] K. Zhao, L. Ge, A survey on the internet of things security, in: Computational Intelligence and Security (CIS), 2013 9th International Conference on, IEEE, 2013, pp. 663–667.
[21] R. Daidone, G. Dini, M. Tiloca, On experimentally evaluating the impact of security on ieee 802.15. 4 networks, in: Distributed Computing in Sensor Systems and Workshops (DCOSS), 2011 International Conference on, IEEE, 2011, pp. 1–6.
[22] T. Heer, O. Garcia-Morchon, R. Hummen, S.L. Keoh, S.S. Kumar, K. Wehrle, Security challenges in the ip-based internet of things, Wirel. Pers. Commun. 61 (3) (2011) 527–542.
[23] A.H. Chowdhury, M. Ikram, H.-S. Cha, H. Redwan, S. Shams, K.-H. Kim, S.-W. Yoo, Route-over vs mesh-under routing in 6lowpan, in: Proceedings of the 2009 International Conference on Wireless Communications and Mobile Computing: Connecting the World Wirelessly, ACM, 2009, pp. 1208–1212.
[24] A. Perrig, J. Stankovic, D. Wagner, Security in wireless sensor networks, Commun. ACM 47 (6) (2004) 53–57.
[25] R.H. Weber, Internet of things–new security and privacy challenges, Computer law & security review 26 (1) (2010) 23–30.
[26] Y.H. Hwang, Iot security & privacy: threats and challenges, in: Proceedings of the 1st ACM Workshop on IoT Privacy, Trust, and Security, ACM, 2015. 1–1.
[27] S. Babar, P. Mahalle, A. Stango, N. Prasad, R. Prasad, Proposed security model and threat taxonomy for the internet of things (iot), Recent Trends Netw. Secur. Appl. (2010) 420–429.
[28] Y. Xiao, H.-H. Chen, B. Sun, R. Wang, S. Sethi, Mac security and security overhead analysis in the ieee 802.15.4 wireless sensor networks, EURASIP J. Wirel. Commun. Netw. 2006 (1) (2006) 093830.
[29] S. Raza, T. Voigt, U. Roedig, 6lowpan extension for ipsec, in: Proceedings of the IETF-IAB International Workshop on Interconnecting Smart Objects with the Internet, 2011.
[30] P. Thubert, J.W. Hui, Compression Format for IPv6 Datagrams Over IEEE 802.15. 4-Based Networks, Technical Report, 2011.
[31] S. Misra, S. Goswami, Routing in 6lowpan, in: Network Routing: Fundamentals, Applications, and Emerging Technologies, 2017, pp. 327–348.
[32] A. Verdiere, Y. Igarashi, T. Lys, C. Lavenu, J. Yi, U. Herberg, H. Satoh, A. Niktash, T. Clausen, J. Dean, The Lightweight On-demand Ad hoc Distance-vector Routing Protocol-Next Generation (LOADng), Technical Report, 2016.
[33] T, P. Winter, A. Thubert, J. Brandt, R. Hui, K. Kelsey, R. Pister, J.P. Struik, Vasseur, R, Alexander, RPL: IPv6 Routing Protocol for Low-power and Lossy Networks, Technical Report RFC 6550, IETF, 2012.
[34] T. Clausen, J. Yi, U. Herberg, Lightweight on-demand ad hoc distance-vector routing-next generation (loadng): protocol, extension, and applicability, Comput. Netw. 126 (2017) 125–140.
[35] T. Clausen, J. Yi, A.C. De Verdiere, Loadng: towards aodv version 2, in: Vehicular Technology Conference (VTC Fall), 2012 IEEE, IEEE, 2012, pp. 1–5.
[36] I. Recommendation, 9903 narrowband orthogonal frequency division multiplexing power line communication transceivers for g3-plc networks, 2017. https://www.itu.int/rec/T-REC-G.9903.
[37] S. Park, K. Kim, W. Haddad, S. Chakrabarti, J. Laganier, IPv6 Over Low Power WPAN Security Analysis, Technical Report, 2011.
[38] J. Zhou, Y. Qiu, F. Bao, Lightweight Key Establishment and Management Protocol in Dymanmic Sensor Networks (KEMP), Technical Report, 2010.
[39] C. Karlof, N. Sastry, D. Wagner, Tinysec: a link layer security architecture for wireless sensor networks, in: Proceedings of the 2nd international conference on Embedded networked sensor systems, ACM, 2004, pp. 162–175.
[40] L. Casado, P. Tsigas, Contikisec: A secure network layer for wireless sensor networks under the contiki operating system, in: Nordic Conference on Secure IT Systems, Springer, 2009, pp. 133–147.
[41] A. Dunkels, B. Gronvall, T. Voigt, Contiki-a lightweight and flexible operating system for tiny networked sensors, in: 29th Annual IEEE International Conference on Local Computer Networks, IEEE, 2004, pp. 455–462.
[42] A.C. Martinez, Implementation and testing of loadng: a routing protocol for WSN, in: Bachelor of Science Thesis Telecommunication Engineering, 2012.
[43] Z1 datasheet, zolertia, (http://www.zolertia.com/), Accessed: March 2010.
[44] M.-P. Uwase, N.T. Long, J. Tiberghien, K. Steenhaut, J.-M. Dricot, Outdoors Range Measurements with Zolertia Z1 Motes and Contiki, in: Real-World Wireless Sensor Networks, Springer, 2014, pp. 79–83.
[45] K. Rantos, A. Papanikolaou, C. Manifavas, Ipsec over ieee 802.15. 4 for low power and lossy networks, in: Proceedings of the 11th ACM International Symposium on Mobility Management and Wireless Access, ACM, 2013, pp. 59–64.

Ghada Glissa was born in Sousse (Tunisia) in 1989. She received the degree of engineer of computer science and embedded systems from the National School of Engineering of Sousse, Tunisia, in 2013. She is currently pursuing the Ph.D. degree in networked objects and communication technologies with the National Engineering School of Tunis, University of Tunis-El Manar, Tunisia. Her research interest lies in the field of Internet of Things, with emphasis on security of wireless sensor networks.

Aref Meddeb obtained his Engineers degree from ENIT, Tunisia, in 1992, and both his M.S. and Ph.D. degrees from Ecole Polytechnique, Montreal, Canada, in 1995 and 1998, respectively. He worked with Alcatel, INRS-Telecom, Teleglobe, and Nortel. He was associate professor and vice director at ISITCom, Tunisia, where he also headed the Telecommunications Department. He is currently full Professor and Director of the National School of Engineering, University of Sousse where he also was Director of Study. He also heads the Networked Objects, Control and Communication Systems (NOCCS) research Laboratory. His research interests include Internet of Things, Wireless Sensor Networks, RFID with focus on Security, QoS, Routing, and Design.