6LoWPAN multi-layered security protocol based on IEEE 802.15.4 security features

Ghada Glissa
NOCCS Laboratory
National Engineering School of Tunis
University of Tunis-El Manar, Tunisia
Email: ghadaglissa@gmail.com

Aref Meddeb
NOCCS Laboratory
National School of Engineering
University of Sousse, Tunisia
Email: Aref.Meddeb@infcom.rnu.tn

***Abstract*—Security should be an integral part of IoT communication stack facing vulnerabilities imposed by protocol diversity. In this paper, we propose a new multilayer security protocol based on the security specifications of the IEEE 802.15.4 standard, operating at both the MAC and the 6LoWPAN adaptation layers in order to ensure all essential security aspects to broad public and industrial acceptance. Measurements demonstrate that this alternation between end-to-end and hop-by-hop security protects the entire network against internal and external attacks with minimum overhead, energy consumption, and delay; and a robust hardware implementation.**

***Index Terms*—6LoWPAN, IEEE 802.15.4, Internet of Things, WSNs, Security, AES-CCM, Contiki OS.**

I. Introduction

Wireless Sensor Networks (WSNs) are the heartbeat and the vital nerve of the Internet of Things world, thus they are on permanent standby anticipating environmental events, providing continuous, flexible, and reliable remote monitoring services and participating in various automation systems.

6LoWPAN (IPv6 over Low Power Wireless Persona Area Networks) [1] is the most promising technology for IoT, enabling IP-based connection between smart objects and devices, yielding autonomous Internet links without using centralized architecture. Recent developments are mainly focused on the IEEE 802.15.4-based devices given that this standard offers the fundamental lower network layers (PHY and MAC layers) compatible with the wireless personal area network (WPAN) [2]. The 6LoWPAN Border Router (6LBR) is then the gateway responsible for handling traffic between IPv6 and IEEE 802.15.4 interfaces, by allowing frames fragmentation, reassembly, and header compression features.

IPv6-enabled WSNs remain an open research area with several unspecified and unstudied security flaws reflected in threats and lack of trust. To overcome the vulnerabilities of the 6LoWPAN-based systems, we propose a new security protocol named ”Combined 6LoWPSec” operating alternately at the MAC and at the adaptation layers, offering both end-to-end and hop-by-hop security features and coping with attacks mainly caused by IPv6 hosts and also those specific to the local network. This alternation respects well-defined duration norm favoring end-to-end data protection due to its major importance in characterizing the network effectiveness. The hop-by-hop security is permanently arranged but for a limited period in order to maintain a convenient equilibrium with the quality of services. This solution therefore benefits from the hardware ciphering and verification structures offered by the AES-CCM algorithm. With regard to simulation experiments, we provide insight into the performance behavior of our new security proposal through the Contiki embedded OS, using different security settings and various attack scenarios.

The paper is organized as follows. Section II describes the state of the art 6LoWPAN security solutions. In Section III, we highlight different 6LoWPAN attacks. An elaborated description of the our security protocol is given in Section IV. In Section V, we discuss the performance of our protocol in terms of energy consumption, packet delivery ratio, end-to-end delay, and security overhead. Finally, Section VI concludes the paper.

II. State of the art

6LoWPAN is a promoting IoT technology, standardized by the IETF [1] for achieving the suitability of IPv6 for IEEE 802.15.4 networks, which are characterized by scarce resources in memory, power, throughput and data processing skills. 6LoWPAN network security continues to be a vexing problem since the number of constraints coming from its ability to integrate into the Internet besides the limitations imposed by the LoWPAN itself. Security protocols have been elaborated for various layers in the 6LoWPAN stack. IEEE 802.15.4 MAC security sublayer assures the hop-by-hop security of the wireless medium, whereas upper layer security is outlined to perform end-to-end security between two distant peers [3]. In this section, we detail several researches addressing both hop-by-hop and end-to-end security mechanisms, then we give an overview concerning routing solutions operating through 6LoWPAN networks.

1) End-To-End security: End-to-End (E2E) approaches provide the benefit of enabling secure communications between IPv6 enabled sensor networks and the Internet. So in order to promote E2E security to constrained devices, diverse studies have explored lightweight solutions centering around upper layer features.

To take advantage of the already existing IPv6 security infrastructure, authors in [4][5] propose a compressed version of IPSec protocol enabling IPv6 packet to support lightweight

978-1-5090-4372-9/17/$31.00 ©2017 IEEE

security extension as Authentication Header (AH) and Encapsulation Security Payload (ESP). Lightweight IPSec deployment is feasible into LoWPAN, however, ciphering operations and available security services such as confidentiality, integrity, and authentication are widely heavy for such constrained battery and memory networks. In addition, the IKE (Internet Key Exchange)[6] secret key exchange mechanism adopted by IPSec will inject additional package costs incurred general packet IKE exchange.

In order to integrate compressed security features through the transport layer, authors in [7] [8] [9] alleviate the Datagram Transport Layer Security (DTLS), originally designed to work on top of UDP protocol and to protect web application services, to provide authentication, key exchange mechanisms and application data protection for such restricted devices. However, its real deployment is critical due to the additional ROM and RAM overhead (about 21 KBytes). To cope with these limitations, Han et al [10] propose a new Back-end Offload security architecture allowing a constrained-node CN to establish a secure session between a remote end-point, without the burden of deploying heavy security modules. This architecture introduces the back-end offloader (BeO) security contexts handling using trust association manager (TAM). BlinkToSCoAP [11] is a new end-to-end security framework for the Internet of Things operating across the CoAP application layer. It ensures the transmission of encrypted CoAP messages over 6LoWPAN networks using the interconnection of various TinyOS components which employ lightweight versions of DTLS. Furthermore, Lithe [12] is also a Lightweight Secure CoAP solution providing a lightweight CoAP depending on compressed DTLS protocol with 6LoWPAN header compression mechanisms.

All the previously cited E2E security solutions perform a software ciphering and verification processes without referring to robust hardware deployment that will be the main goal of our contribution.

2) Hop-By-Hop security: This security category provides hop by hop secure communication between neighboring sensors in order to cover all links resilience. Thus the IEEE 802.15.4 security sublayer [2] ensures radio medium security by allowing hop by hop aggregation for encrypted data until being recovered by the sink. While setting the SecurityEnabled field an Auxiliary Security Header will be attached to the MAC frame (see Figure 1). It has a variable length, encompassing a SecurityControl field, a FrameCounter field, and a KeyIdentifier field. The Security Control field affords general information about the security level and the operation mode. It consists of a Security Level subfield, a Key Identifier Mode subfield and reserved bits for future need. The Frame Counter is a 4-octet field, incremented while securing the outgoing frame to provide semantic security and replay protection services. The Key Identifier field with its Key Source and Key Index subfields furnish details about the generated key reference. Moreover, the IEEE 802.15.4 link layer security features defines eight types of security based on the AES (Advanced Encryption Standard) with the CCM* block cipher mode given variable MIC (Message Integrity Code) size. Bootstrapping phase and key management are driven by high layer decisions.

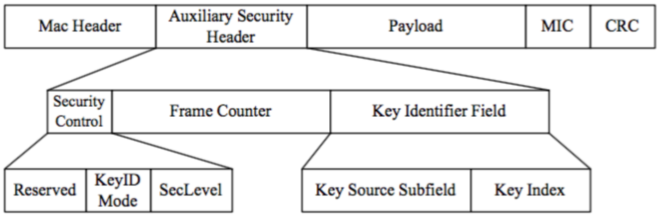


Fig. 1: IEEE 802.15.4 MAC and Auxiliary Security Header Format

Focusing on evaluating IEEE 802.15.4 security performances, many research studies[13][14] introduced simulation models, evaluation techniques and experimental measurements. TinySec [15] is the appropriate example of link layer security architecture, implemented in TinyOS and providing two different modes: authenticated encryption (TinySec-AE) and authentication only (TinySec-Auth). Encryption is deployed using the Skipjack algorithm. Besides, LLSEC [16] is an IEEE 802.15.4 layer security designed for the Contiki/Cooja simulation environment. The deployment of this security architecture proves its feasibility for such constrained devices operating system. ContikiSec [17] is also a link layer security design, influenced by TinySec architecture, then supporting three security modes: confidentiality-only (ContikiSecEnc), authentication-only (ContikiSec-Auth), and both authentication and encryption (ContikiSec-AE). Contiki/COOJA simulation environment evinces its efficiency during introducing security features. Regarding its portability and modularity, Contiki OS remains the best development environment for our new security protocol.

3) 6LoWPAN Routing: Routing schema in 6LoWPAN networks could influence the security methodology decision since different layers could be responsible for building paths. We distinguish two basic routing schema operating in distinct levels, which are mesh under and route over. Mesh under routing is performed by the adaptation layer, forwarding the packet fragments towards the destination without resorting to the network layer. However, route-over schema is managed by IPv6 layer, then each node acts as a router. LOADng routing (Lightweight Ad hoc On-Demand-Next Generation) [18] is a reactive routing protocol intended to mesh-under scheme and derived from AODV. Its basic operations include the generation of Route Requests (RREQs) by an originator node when discovering a route to a destination. Forwarding RREQs until reaching the destination introduces the generation of Route Replies (RREPs) upon its receipt by the indicated mote. LOADng routes are maintained for a period of time, unlike RPL (Routing Protocol for Low Power and Lossy Networks)[19] which is desired to be a route-over scheme achieving routing discovery procedure based on directed acyclic graph (DAG). This tree-based routing focuses on the construction of a stable route framework using a metric value called Rank and exchanging several control messages. In our security approach, we adopt mesh-under routing and specially LOADng structure in order to reach medium layer end-to-end security and then preventing each node to act as a final destination able to authenticate and decrypt data.

III. 6LoWPAN security attacks

The migration of sensor networks into the IP domain transforms traditional tools, nodes to intelligent objects. However, this migration to 6LoWPAN networks generates an accumulation of attacks related to IP architecture and others related to low-power radio networks. Our attack model is built to classify 6LoWPAN security threats into hop-by-hop and end-to-end attacks. Since 6LoWPAN is a combination of two systems, in this section we analyze the different possible attacks from the two sides that target all layers of the 6LoWPAN stack.

1) Hop-by-hop attacks: 6LoWPAN networks can suffer from several attacks caused by internal malicious nodes that aim to cause a direct damage to the network. Threats affecting physical links, radio hops and routing discovery, give rise to malfunction and resources exhausting. Jamming attack disrupts nodes' signal by increasing its power spectral density. This frequency perturbation generates thus physical links interruption and eventual collisions. In Tampering attack, malicious node captures and isolates non-protected equipments and then retrieves stored hardware information such as secret keys. In addition, Battery exhaustion attack causes energy depletion by sending repetitive request messages and forcing compromised node to respond continuously. A Sybil attack aims to create dissociative disorder and forge multiple identities for the same malicious node in peer-to-peer networks. Moreover, in Wormhole attack the malicious node creates a false path to disturb the routing within the network. The Spoofing attack goal is falsifying routing information such as the rank metric for RPL routing. In Black hole attack, adversary node aims to block or drop all received/generated packets instead of forwarding them. Likewise, Selective forwarding attack consists in dropping or delaying arbitrary a part of the packets received by attackers.

2) End-to-end attacks: WSN IPv6-based networks are susceptible to various attacks related to external unauthorized devices. The destruction of end-to-end links causes the deterioration of the whole network, then damages will not be restricted to a local area. End devices perform packet fragmentation and reassembly in IPv6, thus end-to-end security is indispensable to prevent modifying or rebuilding packet fragmentation. Flooding attack forces node to react with synchronization messages imitating error messages by the De-synchronization attack. In addition, by generating huge traffic to the Edge Router, Path-based DoS attack aimed to deplete nodes' resources when injecting false messages and then interrupting the communication with the border router. Otherwise end-to-end attacks could be similar to hop-by-hop attacks only occurring between the 6LoWPAN border router and IPv6 end hosts.

IV. Protocol Description

A. Motivation

In order to overcome the security threats engendered by the amassing of the shortcomings related to both LoWPAN and IPv6 environments, we have proposed a combined 6LoWPAN security protocol named the Combined 6LoWPSec mainly aiming to put an end to attacks exerted on end-to-end IPv6 communications and, to a lesser extent, radio medium attacks. Our proposal is based on the existing IEEE 802.15.4 security features proposed as an extension of the MAC sublayer. This hardware deployment of the AES-CCM* ciphering algorithm will be valuable in terms of data confidentiality, integrity, authentication, availability and malicious intrusion detection.

B. Details of the Proposed Protocol

To upgrade the security functionality of the 6LoWPAN networks, the Combined 6LoWPSec scheme is designed to function through multi-levels, more precisely the MAC and the adaptation layers. It is arranged to operate using the LOADng routing. This mesh under routing strategy allows low level E2E security implementation since fragments are gathered at the end device and not at each node hop. During exchange data messages between nodes, our security protocol should ensure the good running of the communication process within and outside the LoWPAN. Firstly, security mechanism will be addressed along the adaptation layer enabling E2E security between 6LoWPAN nodes and IPV6 hosts. Then data encryption/decryption, authentication/verification has to be handled only via end devices without interfering with relaying motes and routers. Afterwards, for protecting the LoWPAN and preventing the intrusion of the attacker motes or the malfunction of the already existing motes, our new mechanism enables, therefore a secure hop-by-hop data exchange.

Algorithm 1 Combined 6LoWPSec

```
Require: $SecuretyEnabled = TRUE$
Require: $SecLevel > 0$
  while $SecuretyEnabled$ do
    $E2ESecT = n * (MaxE2EDelay + SecDelay)$
    $HbHSecT = MaxHopNum * (HbHDelay + SecDelay)$
    while $E2ESecT$ do
      $E2ESecEnabled = TRUE$
      $E2ESecOperations()$
      $E2ESecT - -$
    end while
    $E2ESecEnabled = FALSE$
    while $HbHSecT$ do
      $HbHSecEnabled = TRUE$
      $HbHSecOperations()$
      $HbHSecT - -$
    end while
  end while
```

According to the Combined 6LoWPSec algorithm (see Algorithm 1), by activating the SecurityEnabled field and by setting the SecurityLevel field greater than zero, the security features of the IEEE 802.15.4 security sublayer will be carried out to achieve data protection between the different 6LowPAN entities. First, it enables separately the HbHSecEnabled by setting the macSecurityEnabled field to 1 as well as the E2ESecEnabled when setting the reserved field of the FrameControl to 1. Subsequently, our proposed protocol will operate alternately between the adaptation and the MAC layers respecting two security times: E2ESecT and HbHSecT. The E2E security duration should be broadly higher than the Hop-by-Hop security duration. It is defined depending on a favor criterion n multiplied by the max E2E delay (MaxE2EDelay) coupled with the security operations delay (SecDelay). Hop-by-Hop security intervenes for a short time (HbHSecT) to check the reliability of the existing nodes. It is calculated according to the one hop and the Security delays multiplied by the maximum number of hops to reach the 6BR. Our proposal gives favor to the E2E security by choosing a very high value of n parameter. It therefore offers a robust hardware implementation of the AES-CCM* ciphering algorithm using different MIC lengths. Data will therefore be encrypted and authenticated by each transmitter node, verified and decrypted either by the next hop or by the end point while respecting to the protocol alternation.

V. Evaluation

A. Testbed platform and experimental setup

In order to evaluate the Combined 6LoWPSec performance, we have used the COOJA network simulator for Contiki OS. Contiki is an open source operating system for the Internet of Things, written in C development language that makes it easy and flexible to introduce new characteristics and more precisely to extend the security features defined by the IEEE 802.15.4 standard, deployed in both MAC and adaptation layers. The deployment of such protocol requires the modification of the existing Contiki rime stack, that accommodate mesh-under routing, to support LOADng routing protocol with respect to [20] and also to promote the use of IEEE 802.15.4 MAC security specifications at both the MAC and the adaptation layers. Measures are made trough Tmoste Sky node which is a hardware platform with a 16-bit msp430 MCU, a 48kB of ROM, a 10 kB of RAM, an external Flash memory, a CC2420 radio transceiver, and different sensing features.

Our simulation topology, as shown in Figure 2, consists of ten Sky motes (yellow color) connected to an IPv6 host (purple color) through a 6LoWPAN Border Router (green color). The operation of these nodes will be disrupted due to the presence of attacking nodes (red color) inside and outside the LoWPAN. Nodes 17 and 18 apply selective forwarding attack respectively between end-to-end and peer-to-peer devices. These malicious elements behave like normal relay/node and selectively or randomly drop packets with the aim of exhausting resources and degenerating the quality of services. So we have considered three different metrics to demonstrate the efficiency of our proposal: the memory allocation,the energy consumption and the packet delivery ratio (PDR).

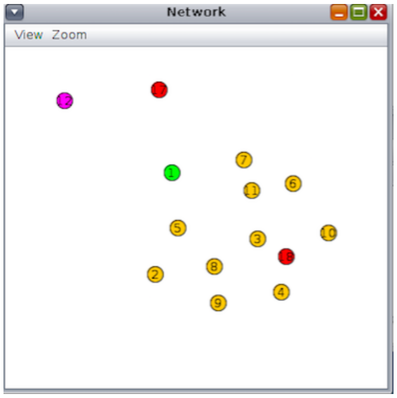


Fig. 2: Simulation Topology

B. Analyze memory allocation

To examine the memory footprint of various security levels applied to the 6LoWPAN network, we evaluate the program memory overhead regarding to the 6LoWPAN motes and the border-router.

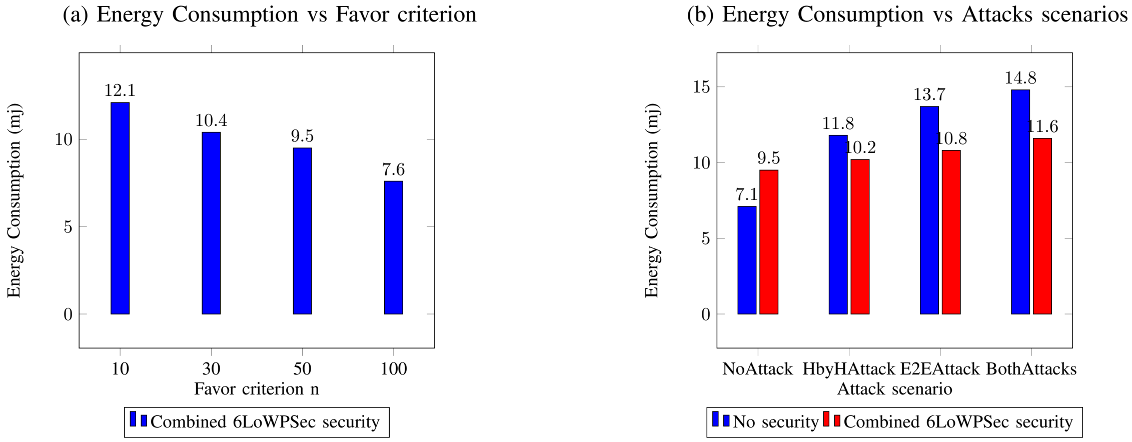
Combined 6LoWPSec Mode	Border Router	6LoWPAN mote
Nullsec	40.48 kB	39.97 kB
MIC-32	41.38 KB	40.53 KB
MIC-64	41.92 KB	41.21 KB
MIC-128	42.22 KB	41.61 KB
ENC	40.93 KB	40.11 KB
ENC-MIC-32	42.08 KB	41.58 KB
ENC-MIC-64	42.77 KB	42.38 KB
ENC-MIC-128	43.21 KB	42.73 KB

TABLE I: Program Memory In Kilobytes

Table I focuses on the impact of our proposed security protocol on memory consumption for different security levels and MIC sizes. We observe that the security overhead may be acceptable for some security modes, but critical for others with high MIC and key lengths. For such constrained devices with limited memory of 48kB, it is preferable to deploy low security level when activating hop-by-hop security and high security when enabling end-to-end protection. Therefore, for the following experiments, we adopt this best configuration of 40.53 KB of memory for 6LoWPAN motes (CBC_MAC 4 mode) and 43.21 KB for border router (CCM 16). Thus, this choice is made to decrease the security overhead since the repetitive exchange of messages between the different 6LoWPAN nodes, however, communication with a distant IPV6 host requires high security.

C. Analyze energy consumption

The energy consumption problem continues to remain one of the biggest issues in wireless sensor network for challenge barrier of battery capability. Thus to keep the trade-off between providing security functionality and limiting energy consumption, it is essential to maintain the security configuration of the previous subsection. Measurements are captured during a period of 30 min for different scenarios in the presence and the absence of attack. They are also intended to evaluate the



(a) Energy Consumption vs Favor criterion

(b) Energy Consumption vs Attacks scenarios

Fig. 3: Energy consumption for variable favor criterion values and through different security scenarios

impact of alternating between E2E and hop-by-hop security while taking into consideration different values of the favor criterion n.

Figure 3a demonstrates how security features and malicious behaviour influence the power consumption. In Figure 3a we measure the impact of the favor criterion n on energy. In fact, this metric has a direct effect on the end-to-end and hop-by-hop security durations. By choosing a high n value E2E security is privileged, otherwise HbyH security will be selected. Then to calculate E2ESecT and HbHSecT we define the SecDelay= 0.068ms, the MaxE2EDelay= 0.21ms, MaxHopNum= 6 and HbHDelay= 0.018ms, thereafter the n parameter is varied. The experiment measures show that by promoting hop-by-hop security, the energy consumption reaches its maximum (12.1mJ) since packets are checked and deciphered at each node jump, in contrast to end-to-end security where data is decrypted and verified at the end device. To balance the alternation between these two modes required by our new security protocol, we choose subsequently n = 50 which corresponds to 9.5mJ of energy consumption.

Figure 3b proves the importance of our proposal, in terms of energy consumption, to deal with the attacks. The Selective forwarding attack is manipulated in both inside and outside the LoWPAN. HbyH attack affects a very limited zone of motes, unlike E2E attack affects the whole network and obliges all the nodes to retransmit the dropped messages leading then to battery exhausting. These two threats will be corrected thanks to our Combined 6LoWPSec security protocol.

D. End-to-End delay

End-to-end delay is interpreted as the time taken for a packet to reach across a network from source to destination. In our case, it is evaluated for different security configurations, and while transmitting packets with varied data lengths.

By alternating between the two modes of security, Figure 4 shows that privileging the hop-by-hop mode leads to an increase of the E2E delay which can reach 0.62ms for 16byte of data. This results from the additional security delay related to the ciphering operations processed at each hop. However, by promoting end-to-end security the E2E delay seems relatively acceptable given that the security compromise is achieved between two end devices.

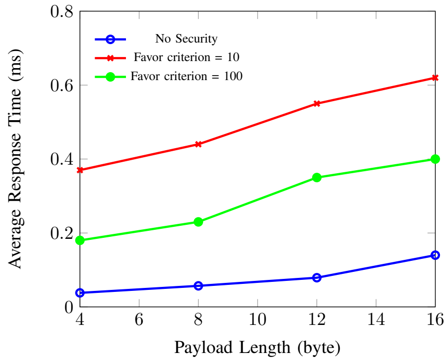


Fig. 4: End-To-End delay for different security modes

It is therefore essential to ensure a balance between the different security parameters in order to achieve better quality of services. Favoring of the E2E security generates a proper functioning of the entire network while alternating with hop-by-hop security prevents the appearance of intruder nodes inside the LoWPAN.

VI. Conclusion

Needless to say, security is critical in 6LoWPAN networks. In this paper, we examined the need for alternating between hop-by-hop and end-to-end security for such networks. Based on the IEEE 802.15.4 security features, we proposed a Combined security protocol addressing attacks inside and outside the LoWPAN. Simulations are accomplished through the Contiki operating system. Results demonstrate the effectiveness of our proposal in terms of memory overhead, energy consumption, and end-to-end delay.

References

[1] N. Kushalnagar, G. Montenegro, and C. Schumacher, “Ipv6 over low-power wireless personal area networks (6lowpans): overview, assumptions, problem statement, and goals,” Tech. Rep., 2007.

[2] I. . W. Group *et al.*, "Ieee standard for local and metropolitan area networkspart 15.4: Low-rate wireless personal area networks (lr-wpans)," *IEEE Std*, vol. 802, pp. 4–2011, 2011.

[3] T. Heer, O. Garcia-Morchon, R. Hummen, S. L. Keoh, S. S. Kumar, and K. Wehrle, "Security challenges in the ip-based internet of things," *Wireless Personal Communications*, vol. 61, no. 3, pp. 527–542, 2011.

[4] P. Varadarajan and G. Crosby, "Implementing ipsec in wireless sensor networks," in *2014 6th International Conference on New Technologies, Mobility and Security (NTMS)*. IEEE, 2014, pp. 1–5.

[5] J. Granjal, E. Monteiro, and J. S. Silva, "Enabling network-layer security on ipv6 wireless sensor networks," in *Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE*. IEEE, 2010, pp. 1–6.

[6] C. Kaufman, "Internet key exchange (ikev2) protocol," 2005.

[7] S. Raza, D. Trabalza, and T. Voigt, "6lowpan compressed dtls for coap," in *2012 IEEE 8th International Conference on Distributed Computing in Sensor Systems*. IEEE, 2012, pp. 287–289.

[8] Y. Maleh, A. Ezzati, and M. Belaissaoui, "An enhanced dtls protocol for internet of things applications," in *Wireless Networks and Mobile Communications (WINCOM), 2016 International Conference on*. IEEE, 2016, pp. 168–173.

[9] G. L. dos Santos, V. T. Guimaraes, G. da Cunha Rodrigues, L. Z. Granville, and L. M. R. Tarouco, "A dtls-based security architecture for the internet of things," in *Computers and Communication (ISCC), 2015 IEEE Symposium on*. IEEE, 2015, pp. 809–815.

[10] J. Han and D. Kim, "A back-end offload architecture for security of resource-constrained networks," in *Network Computing and Applications (NCA), 2016 IEEE 15th International Symposium on*. IEEE, 2016, pp. 383–387.

[11] G. Peretti, V. Lakkundi, and M. Zorzi, "Blinktoscoap: An end-to-end security framework for the internet of things," in *2015 7th International Conference on Communication Systems and Networks (COMSNETS)*. IEEE, 2015, pp. 1–6.

[12] S. Raza, H. Shafagh, K. Hewage, R. Hummen, and T. Voigt, "Lithe: Lightweight secure coap for the internet of things," *IEEE Sensors Journal*, vol. 13, no. 10, pp. 3711–3720, 2013.

[13] S. M. Sajjad and M. Yousaf, "Security analysis of ieee 802.15. 4 mac in the context of internet of things (iot)," in *Information Assurance and Cyber Security (CIACS), 2014 Conference on*. IEEE, 2014, pp. 9–14.

[14] Y. Xiao, H.-H. Chen, B. Sun, R. Wang, and S. Sethi, "Mac security and security overhead analysis in the ieee 802.15. 4 wireless sensor networks," *EURASIP Journal on Wireless Communications and Networking*, vol. 2006, no. 1, p. 093830, 2006.

[15] C. Karlof, N. Sastry, and 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.

[16] I. Halcu, G. Stamatescu, and V. Sgârciu, "Enabling security on 6lowpan/ipv6 wireless sensor networks," in *Electronics, Computers and Artificial Intelligence (ECAI), 2015 7th International Conference on*. IEEE, 2015, pp. SSS–29.

[17] L. Casado and 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.

[18] T. Clausen, J. Yi, and A. C. De Verdiere, "Loadng: Towards aodv version 2," in *Vehicular Technology Conference (VTC Fall), 2012 IEEE*. IEEE, 2012, pp. 1–5.

[19] T. Winter, "Rpl: Ipv6 routing protocol for low-power and lossy networks," 2012.

[20] A. C. Martnez, "Implementation and testing of loadng: a routing protocol for wsn," in *Bachelor of Science Thesis Telecommunication Engineering*, 2012.