End-to-end transparent transport-layer security for Internet-integrated mobile sensing devices

Jorge Granjal
DEI/CISUC, University of Coimbra
Polo 2, Pinhal de Marrocos, 3030-290
Coimbra, Portugal
jgranjal@dei.uc.pt

Edmundo Monteiro
DEI/CISUC, University of Coimbra
Polo 2, Pinhal de Marrocos, 3030-290
Coimbra, Portugal
edmundo@dei.uc.pt

***Abstract*—End-to-end communications with Internet-integrated sensing devices will contribute to the enabling of many of the envisioned IoT applications. Communication technologies with this purpose are currently being designed based on the 6LoWPAN adaptation layer, and of particular interest is CoAP (Constrained Application Protocol). The support of security in end-to-end CoAP communications with mobile Internet-integrated sensing devices is currently a challenge, in particular because of the high cost of performing ECC computations in constrained wireless sensing devices. Other important aspects to consider are the incompatibility of end-to-end security with CoAP proxies and the usage of mobile sensing devices.**

The mechanisms described in the article offer a practical solution to the previous challenges. We propose a transparently mediated DTLS handshake with mutual authentication and mobility support, with the goal of releasing constrained sensing devices from the burden of having to support costly ECC computations. We employ pre-shared key authentication in sensing devices, together with an authentication protocol for mutual authentication and confidentiality in the WSN side of end-to-end communications. From our experimental evaluation on the impact of the proposed mechanisms on the energy and computational effort required from sensing devices, we are able to verify that the proposed approach is viable in various usage scenarios. Overall, the proposed approach works transparently for the applications running on the Internet clients and sensor devices. It is our goal that, with the proposed mechanisms, distributed IoT applications may benefit from pervasive and transparent end-to-end security, irrespective of the static or mobile nature of the sensing devices employed. Ours is, as far as our knowledge goes, the first proposal with such goals.

Keywords—End-to-end transport-layer security, DTLS mobility, delegated public-key authentication, ECC, 6LoWPAN, DTLS, CoAP

I. Introduction

Most of the applications envisioned for the Internet of Things (IoT) are critical in respect to security, either of its users or of the data stored and transferred between devices. On the other hand, researchers know very well that the constraints in resources of sensing devices difficult the employment of traditional security approaches and mechanisms. This remains true if we focus on end-to-end communications with Internet-enabled devices employing 6LoWPAN-based communication technologies. In fact, technologies such as 6LoWPAN [1-3] and CoAP [4,5] are being designed precisely to enable the usage of constrained sensing devices as full Internet citizens, but challenges remain in what concerns security, in particular for end-to-end communications with such devices and when such communications are with devices that by nature are mobile.

In this article we start by proposing a model for the interconnection of low-energy wireless communication domains with the Internet, and in the context of this model we propose a set of mechanisms designed with the purpose of supporting end-to-end security with mobile sensing devices. The proposed mechanisms allow us to offer practical and effective solutions to three aspects currently representing research challenges in the area: the high cost of end-to-end transport-layer security for constrained wireless sensing devices, the incompatibility of end-to-end security with the usage of proxies, and the lack of mechanisms to abstract end-to-end communications and security from the movement of sensing devices. Our proposals address the previous challenges, while guaranteeing total compatibility with the mechanisms already adopted.

The article is structured as follows. In the next Section we discuss our motivations, and Section III presents the proposed integrated model for end-to-end security with mobile devices. The mechanisms proposed in the context of this model are discussed in Section IV and experimentally evaluated in Section V. Section VI discusses related work and Section VII finally concludes the article.

II. Motivation

Contrary to the perception of researchers a few years ago, the emergence of 6LoWPAN-based communication technologies [1-3] is enabling Internet communications with constrained sensing platforms. Distributed IoT applications may employ CoAP [4,5] at the application-layer, in order to retrieve resources from sensing devices, or for autonomous communications between WSN and Internet devices. CoAP is being designed to enable application-layer RESTful communications with such sensing platforms, and it promises to be a cornerstone for the support of future IoT applications. The addressing of security in

ISBN 978-3-901882-83-8 © 2016 IFIP

the context of CoAP is thus of major importance although, as we discuss next, various issues still complicate effective security.

The current CoAP specification adopts DTLS (Datagram Transport Layer Security) [6] at the transport-layer security with the goal of transparently securing CoAP communications at the application-layer. DTLS provides security that, by nature, is end-to-end, but in reality conflicts with another functionality designed in CoAP: the usage of proxies to assist communications between the Internet and WSN communication domains. Another aspect currently motivating research efforts is that DTLS, as adopted for CoAP, requires the usage of public-key authentication using ECC (Elliptic Curve Cryptography) for authentication and key agreement. ECC is well know to be too resource demanding in constrained sensing devices, further complicating the adoption of DTLS in practical applications. Another aspect is that many IoT applications may employ devices that by nature move from one WSN domain to another, even if between WSN domains under the same administrative control. Thus, mechanisms are also required to support inter-WSN mobility in the context of end-to-end communications and security, as we address in this article. We address the previous aspects in an integrated fashion, proposing a coherent solution to address the limitations of CoAP security.

As already discussed, DTLS is currently mandatory for CoAP, the same applying to the support of ECC public-key cryptography. It is well accepted that ECC is still too costly for sensing platforms such as the TelosB [7], and this aspect currently motivates various research proposals, as we discuss in Section VI. Our proposal consists in the offloading of costly computations related with the handshake to a more capable device, at the same time guaranteeing total transparency from the point of view of the communicating entities and applications. In particular, we extend our previous proposal on DTLS authentication with mediation [8] to include support for mobile sensing devices. The costliest phase of DTLS is the initial authentication and key agreement handshake, and our proposal not only supports the offloading of ECC computations to a router, but also works side-by-side with our mobility model, allowing for inter-WSN movement of CoAP sensing devices.

As previously referred, DTLS as currently considered for CoAP conflicts directly with the usage of CoAP proxies, either in reverse or forward mode. This is in fact a concern, as CoAP proxies are useful and a necessity in many scenarios. By intercepting and mediating the DTLS handshake our model offers an effective solution to the support of CoAP proxies, since the same entity can support all functionalities.

Regarding the mobility of sensing devices, our goal is to propose mechanisms that can abstract IoT applications, and also end-to-end communications and security, from the actual position of a device inside a WSN administrative domain. A device may roam between different WSN domains inside a given administrative domain (e.g. in medical applications, where patients in an hospital carry a sensing platform and may move between different networks, or in industrial monitoring and control applications), while applications still are able to establish end-to-end communication and secure sessions with the device. We note that mobility will be in fact an important requirement of many IoT applications, for example, sensors may be attached to moving machinery in a factory or building, or to a vehicle moving around in a plant, or even used for biometric purposes and attached to persons. Our proposal considers that mobility is a reality, and also that end-to-end communications between Internet hosts and CoAP devices must be maintained for sensing devices moving in the same administrative domain. Thus, even with security such devices are able to keep serving CoAP requests from Internet hosts, in the context of the application.

Overall, the contributions in this article belong in the context communication and security technologies based on 6LoWPAN, that are already contributing to the formation of an IoT communications stack as analysed in [9]. More precisely, our aim is to contribute to security in the context of this stack, and offer what we believe are effective solutions to the problems previously identified.

III. An Integration Model for End-to-End Security with Mobile Sensing Devices

The model considered throughout the article for the support of end-to-end communications and security with mobility is illustrated in Figure 1. In this model we consider the existence of two or more 6LoWPAN WSN under the same administrative domain, interconnected with the Internet via 6LoWPAN border routers (6LBR). As illustrated, sensing devices are free to move between WSN in the same administrative domain.

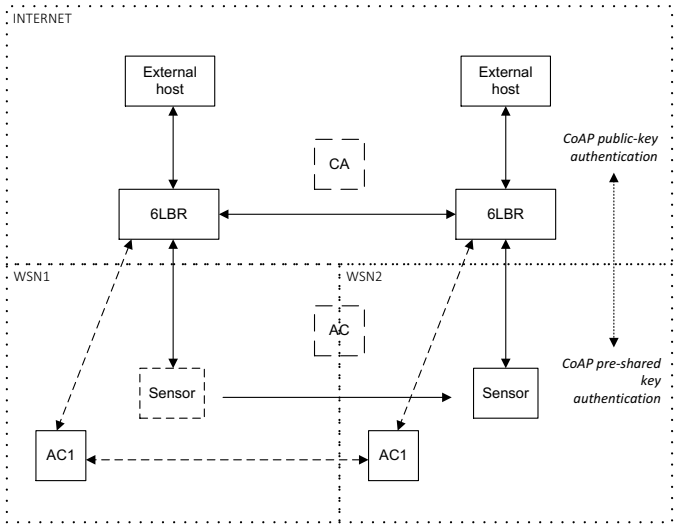

Figure 1 – An integration model for transparent end-to-end transport-layer security with Internet-integrated mobile sensing devices

As illustrated in Figure 1, end-to-end communications and security sessions can be established at the transport-layer, between external (Internet) entities and a mobile sending device, via any of the 6LBR in the scenario. As we discuss in detail in the next Section, a 6LBR is able to transparently intercept and mediate the DTLS authentication and key negotiation phase, at the same time supporting the role of CoAP proxy. As is visible in the previous figure, we consider the usage of different authentication strategies, in the context of a single end-to-end session. From the perspective of an external entity this session is being authenticated using the CoAP security mode providing the highest security: public-key authentication with certificates

(using the CoAP *Certificates* [4] security mode). On the other hand, mobile sensing devices may employ a much lighter and realistic authentication strategy: based on pre-shared keys (using the *PreSharedKey* CoAP security mode). We must note that our goal is to be able to this with total transparency to the communicating parties, and thus, neither the sensing device nor the Internet client are aware that the other party doesn't support the same authentication strategy.

Another important aspect of the proposed integration model can be found in the support of mobility, which works in tandem with a protocol we introduce to support authentication in the WSN domain. For the purpose of supporting authentication and mobility, we consider the usage of a Certification Authority (CA) and of Access Control (AC) entities. The CA attests the validity of the various communicating entities by issuing certificates, while AC servers assist in mobility and authenticating the WSN communicating parties, in the context of end-to-end Internet communications. Although in the previous figure AC servers apply to a particular WSN domain, we can also consider multihoming, with a single AC server supporting authentication and mobility for the various WSN in the administrative domain.

In order to provide effective security, we need to address the trust model considered in the integration scenario. Trust is established between AC servers on different WSN domains, in order to support end-to-end security with mobility, as we discuss later in the article. We also assume that a 6LBR trusts its AC server, the same applying to the mobile sensing device. Trust is configured in the form of shared cryptographic keys during the configuration or network bootstrap phase, as we discuss later in the context of the proposed authentication and mobility procedures. Finally, we also assume that the 6LBR, AC and CA devices are without the constrains in resources of mobile sensing platforms, and thus are able to support the proposed end-to-end security, authentication and mobility mechanisms. Regarding the threat model considered, we note that our focus is on providing security against external attacks, and in particular in enabling fundamental security properties as confidentiality, integrity, authentication and non-repudiation to end-to-end communications with constrained sensing devices, using the mechanisms we proceed to describe.

IV. Mechanisms towards transparent end-to-end security with mobility

As per the goals of this article, in the context of the interconnection model previously discussed we propose a mechanism to assist in the support of effective end-to-end security, in the presence of mobile sensing devices. We begin by describing our approach to DTLS transparent interception and mediation, and later we present the protocol responsible for the support of authentication and confidentiality in the WSN part of the end-to-end security session. Finally, we address the support of mobility between WSN domains. Overall, it is our goal that the proposed mechanisms work in tandem to provide effective end-to-end security with mobility, in a completely transparent fashion to communicating parties and applications, and at the same time with total compatibility with CoAP security as current defined for the IoT.

A. DTLS transparent interception and mediation

The first challenge we address is to release constrained sensing devices from the burden of having to support costly ECC computations in the context of the initial DTLS handshake. We must note that the handshake is the problematic part of end-to-end security, as after authentication and key negotiation end-to-end security may be addressed in the sensing device efficiently, if AES/CCM encryption is employed. As we also note later in the article, the transparent interception and mediation of DTLS also provides advantages other than the enabling of ECC encryption to support high security with CoAP.

The DTLS handshake is an important part of end-to-end security, as it allows for mutual authentication and key agreement between both communicating parties. Not only we want to offload such costly computations, we want to do it in a completely transparent fashion to such parties and applications. We also need to support sensing devices that may freely move between different WSN domains, as previously discussed and illustrated in Figure 1. We guarantee that, in the context of a given IoT application, CoAP resources residing on sensing devices are reachable securely, irrespective of the current position of the device, and at the same time not requiring any modification to CoAP and DTLS as supported on such devices. The preservation of total compatibility with DTLS and CoAP specifications is of cornerstone importance in our proposal.

The proposed mediated DTLS handshake supports delegated ECC public-key mutual authentication between mobile sensing devices and other external (Internet entity), as illustrated in Figure 2. We note that the interception of the DTLS handshake at the 6LBR allows us to control how the handshake is performed with the two end parties, in a completely transparent fashion to such entities. Thus, from the point of view of the Internet client and CoAP server (as considered in Figure 2), the handshake is performed accordingly to the rules defined for DTLS [6], which basically adapts TLS (Transport Layer Security) [10] for performing over UDP (as employed in 6LoWPAN environments).

Considering the integration model illustrated in Figure 1, the interception and mediation of messages is performed in the 6LBR, which also supports Internet communications between the WSN and Internet domains and, if required, a CoAP proxy in either reverse or forward mode. On the Internet side, a CoAP client wants to retrieve information from the CoAP server running on the sensing device and connects via the 6LBR. Such communications are intercepted at the 6LBR and the router is able to expose authentication and key negotiation differently towards the WSN side, in communications with the sensing device. We also allow the opposite usage scenario, meaning that the client may be on the WSN domain connecting to a CoAP server on another WSN network or on the Internet. As illustrated, AC servers are also part of the handshake for the purpose of supporting authentication between the 6LBR and the sensing device.

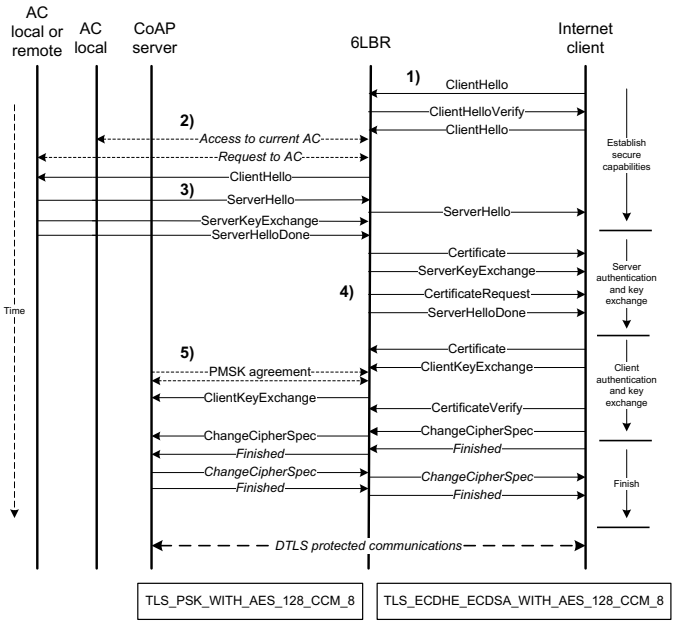

Figure 2 – Transparently mediated DTLS handshake with mutual authentication and mobility support

On the Internet side we allow for the usage of authentication using ECC cryptography and certificates, thus supporting the *Certificates* CoAP security mode [4,5], while on the WSN we employ the much lighter *PreSharedKey* CoAP security mode, certainly more aligned with the real capabilities of constrained sensing devices. In line with the CoAP security modes supported, on the Internet side we consider the usage of TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8, while on the WSN domain we employ pre-shared key authentication with TLS_PSK_WITH_AES_128_CCM_8.

A DTLS security session requires the two communicating parties to agree on the cipher suite and encryption keys employed. The DTLS handshake transports the information required to derive such secret keying material. The encryption keys required to secure transport-layer communications are obtained from a master key that the client and server must share after the completion of the handshake and, on the other hand, this master key is obtained by both parties using a pair of client and server random values plus a pre-master secret key. We must note that client and server random values are exchanged during the handshake, while the way the pre-master shared key is obtained depends on the cipher suite employed. With cipher suites employing public-key authentication, the client is allowed to generate the pre-master shared key and send it to the server encrypted with the server's public-key. Thus, this is true for TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8, which we support in communications with the Internet side, while for pre-shared key suites (TLS_PSK_WITH_AES_128_CCM_8) this is not supported, mainly because at an initial stage the two entities are unable to support the secure transmission of the pre-shared secret. In order to circumvent this limitation, TLS_PSK_WITH_AES_128_CCM_8 is modified in our proposal in order to allow the 6LBR to transmit the pre-master secret to the sensing device. The pre-master secret key received from the Internet client is forwarded to the CoAP server, and in order to guarantee appropriate security for WSN communications, we introduce an authentication and encryption protocol, described later in the article.

Referring again to Figure 2, the following are the main phases or message flights of the mediated DTLS handshake:

1) The initial *ClientHello* is intercepted by the 6LBR, and the router answers with a *ClientHelloVerify* as a measure of protecting the WSN domain against DoS attacks [6]. The *ClientHello* message returned by the Internet client transports the client random value, together with the protocol version and the list of supported cipher suites.
2) Using the proposed WSN authentication protocol (discussed later in the article) the 6LBR obtains an initial ticket from the AC server together with information about the AC to contact for the purpose of obtaining access to the destination sensing device. Here the AC in the same WSN domain as the 6LBR is identified as the "local AC", whereas the AC in the domain to which the sensing device is currently attached to is the "remote AC". From the remote AC the 6LBR obtains a ticket for the CoAP service, information about the cipher suites supported by the sensor, as well as its digital certificate and current IPv6 address.
3) The original *ClientHello* message is forwarded to the destination CoAP device with a request for pre-shared key-based authentication. The *ServerHello* response is forwarded back to the Internet client, this time acknowledging public-key authentication. The *ServerKeyExchange* message forwarded in this flight transports the server random value.
4) In order to guarantee mutual authentication as per our goals, the 6LBR client is authenticated by requesting its certificate. The *ClientKeyExchange* message sent by the client transports the random value and the pre-master secret key generated by the client.
5) The WSN authentication protocol allows us to obtain a secret key to be shared between the 6LBR and the destination CoAP sensing device. We use this key to secure the transmission of the pre-master secret key to the server. The next message flight allows to finalize the handshake between the client and device. After this stage end-to-end communications proceed normally, and the 6LBR is also in possession of the required cryptographic material to support other security mechanisms, as we address at the end of the article.

The WSN authentication and confidentiality protocol is of major importance in the proposed mediated DTLS handshake. This protocol not only supports mobility by informing the 6LBR of the current position and of the AC responsible for the destination sensing device, but also guarantees appropriate high security for WSN communications between the 6LBR and that

device, in the context of the handshake. After the destination sensing device has received the *ClientKeyExchange* message, both communicating parties are now in possession of the same pair of random values and pre-master secret key. This is the information required for both parties to compute the DTLS master key as in the current specification [6], and from this master key to obtain the secret material for DTLS security.

B. WSN authentication and confidentiality

The authentication and confidentiality protocol proposed is responsible for guaranteeing appropriate security in the WSN domain, during communications between the 6LBR and the destination sensing device in the context of the handshake. This protocol also plays an important part in the support of mobility. We illustrate the proposed protocol in Figure 3, noting that it inherits characteristics from the Kerberos authentication protocol [11], while supporting other characteristics designed to support our end-to-end mediation approach, as well as mobility.

As in Kerberos, this protocol considers the usage of two security-related data structures: tickets and authenticators. In generic terms, considering a client named *c* and a destination service named *s*, a ticket $T_{c,s}$ and an authenticator A_c are defined as follows:

$$T_{c,s} = \{ s, c, addr_c, timestamp, life, K_{c,s} \}K_s$$
$$A_c = \{ c, addr_c, timestamp \}K_{c,s}$$

A ticket authenticates a client to a service, in our authentication protocol to authenticate the 6LBR to the remote AC server and to the final CoAP service running on the sensor. As the ticket is opaque to the client, it is transmitted as is to its destination. An authenticator is generated by the client and allows security against replay attacks. The following are the main phases of the authentication protocol:

1) The 6LBR requests, from its local AC server, a ticket and information about the remote AC. The remote AC is the server to contact to request a new ticket for the destination CoAP service.

2) The 6LBR contacts the remote AC server and requests a ticket for the destination CoAP service. This reply, in addition to the ticket itself, transports information on the capabilities of the sensor, its certificate and the current IPv6 address.

3) Finally, the 6LBR authenticates with the destination CoAP service. After authentication, the 6LBR and the sensor share a secret key that they use to secure the transmission of the pre-master shared key, in the context of the DTLS handshake.

As already referred, we assume that trust is established between the various communicating parties previously to communications and end-to-end security. As illustrated in Figure 3, secret keys are shared and used to secure communications between the 6LBR and the AC server ($K_{c,ac}$) and between the AC server and the constrained sensing device (K_s). Trust relationships are also established between AC servers on different WSN domains. This is required to extend the trust model and security from one WSN domain to another, as required to support mobility. Such keys allow a client to obtain, from its local AC server, a key to request, from a remote AC, a ticket for the destination CoAP device. We also assume that, contrary to communications to and from sensing devices, communications between 6LBR, AC and CA entities run over a communications medium without the limitations of the WSN. For each registered sensor the AC servers store its X.509 ECC certificate, the list of supported ciphers and compression methods, the name of the AC server for the WSN domain where the sensing device is currently located, and its current IPv6 address.

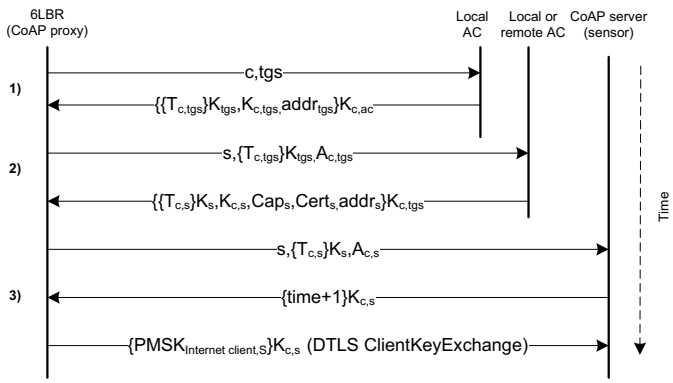

Figure 3 - Authentication protocol for mutual authentication and confidentiality in the WSN domain

The list of supported ciphers allows our model to be applied with other ciphers on the WSN side, although we are currently considering, in this article, the usage of TLS_PSK_WITH_AES_128_CCM_8, as previously discussed. The certificate represents the device and this model alleviates the device from the burden of having to store it in its memory, given that we are performing ECC computation on the 6LBR via delegation. Compression negotiation is supported by the DTLS handshake and also with the mediated DTLS handshake. The name of the AC server of the network to which the sensing device is currently attached to, together with its current IPv6 address, allow any 6LBR to remotely contact the device and activate end-to-end security, as required for devices that are mobile.

C. Support for inter-WSN mobility

One main motivation of our proposal is to address mobility in the context of transparent end-to-end security. In this context, we consider the mobility model illustrated in Figure 4. In this model a sensing device is free to move between different WSN domains (inside the same administrative domain) while being able to accept and maintain active end-to-end security

associations at the transport-layer, transparently from the point of view of applications.

For the purpose of dealing with security, we consider the support of mobility side-by-side with network configuration and ND (Neighbor Discovery) procedures, as currently defined for 6LoWPAN [12]. In this context, a change in the IPv6 address of a sensing device, either due to movement, or when the device wakes up in a different WSN, is fired up by the procedures defined in the context of ND. Such procedures may be related with Neighbor Unreachability Detection (NUD), the reception of a Router Advertisement (RA), or in consequence of a Router Solicitation (RS) message sent. In all situations, the IPv6 address of the sensor is updated, based on its link-local address. The mobility model illustrated in Figure 4 consists of the following main phases:

1) A change in the IPv6 address of the device takes place, based on its link-local address and according to ND procedures optimized for 6LoWPAN [12]. In this context, ND messages are exchanged between the device and the 6LBR, in particular RS, RA, Neighbor Solicitation (NS) and Neighbor Advertisement (NA).

2) The 6LBR is responsible for updating information on the new location of the sensor in the local AC server.

3) The 6LBR is also responsible for informing other 6LBR on the new location of the device. For this purpose, we assume the usage of a broadcast-capable shared communications medium.

4) AC servers in the remaining WSN domains under the same administrative domain see their information on the sensor updated by its local 6LBR.

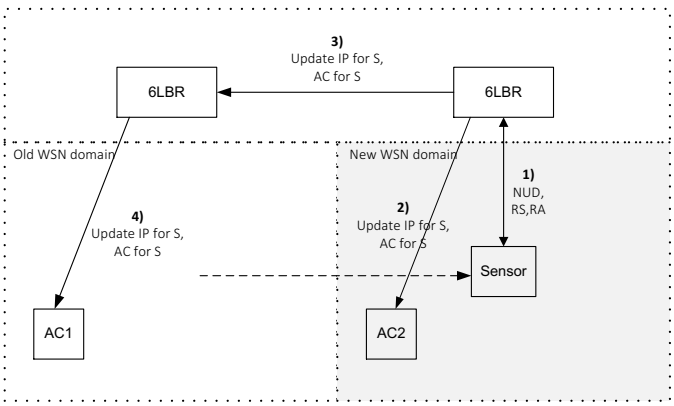

Figure 4 – Mobility and update of information regarding the sensor's current network of attachment

As per the mobility model and the authentication protocol previously discussed, the information on the current position of the sensing device is updated and stored in the various AC servers of the domain. We note again that such procedures also apply in case a multi-homed AC server is employed.

V. Experimental evaluation

We evaluate the previously described security and mobility mechanisms experimentally, looking in particular for two aspects we consider critical for the effectiveness of any proposal on security for constrained wireless sensing environments: the impact on energy and computational effort.

A. Experimental evaluation setup

The integration model illustrated in Figure 1 is considered again, this time for the purpose of evaluating the proposed mechanisms. For this purpose, we employ TelosB [7] sensing devices running the TinyOS operating system [13], and also Linux hosts, for the roles of 6LBR, AC, CA, and Internet client. We employ TinyOS with support for the 6LoWPAN stack, CoAP and also the proposed security and mobility-related procedures. For the purpose of symmetric encryption, we also benefit from the usage of standalone AES/CCM encryption available at the hardware in the TelosB, using code appropriate for this purpose [14]. ECC cryptography is supported using code based on TinyECC [15], and the Internet CoAP client uses *libcoap* [16] integrated with DTLS. Measurements on energy were obtained by measuring the voltage across a current resistor, placed in series with the battery pack of the sensor, while the computational effort was derived directly from the system clock of the sensing device.

B. Lifetime of sensing applications

Our first goal is to evaluate the impact of the proposed mechanisms on energy, as this may directly dictate the potential lifetime of the device and consequently any IoT application depending on it. We measured the energy required to support applications employing the mediated DTLS handshake with sensing devices moving between different WSN domains. For both aspects, we measure energy required for processing headers, security and communications, considering the employment of 102-bytes 6LoWPAN packets. As per our evaluation, the proposed mediated DTLS handshake requires a total of 20 6LoWPAN messages (including the messages required for the WSN authentication protocol) and a total of 0.0013 mJ (millijoules) from the energy available in the TelosB. As expected, the original DTLS handshake is much more demanding, as it requires a total of 39 6LoWPAN messages and 54.4 mJ of energy from sensing devices. Regarding DTLS encryption with standalone AES/CCM on the sensing device, it requires 0.0002 mJ, in deep contrast with 10.89 mJ required to support public-key ECC digital signing, as required with TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8. We may clearly observe the impact of ECC on constrained sensing devices with the characteristics of the TelosB. We note that the previous values are total, measured from the reception of a 6LoWPAN packet to the time when cryptography finished processing the packet on the sensor. As such, we are capturing the total energetic effort to process end-to-end security for a packet. We also consider the energy required for the processing of a packet and related security headers, measured as 0.007 nJ (nanojoules).

Another important aspect considered in our evaluation is the impact of the proposed mobility model and procedures on the energy available on sensing devices. For this purpose, mobility is conjugated with ND mechanisms as previously discussed, and we evaluate the energy required for ND, reception of information from the 6LBR and derivation of a new IPv6 address from the link-local address of the device. Regarding security in the context of ND, we consider the usage of AES/CCM encryption to protect ND-related messages, as defined in [12]. Overall, the total energy cost of supporting communications and security on the TelosB was measured as 0.001mJ.

The previously discussed values obtained experimentally allow us to derive analytically the predictable lifetime of an application using the proposed security and mobility mechanisms. Without considering mobility, it is clear that the proposed mediated DTLS handshake always provides greater lifetime values [8], given that in the original DTLS handshake sensing devices are required to support costly ECC computations during session establishment.

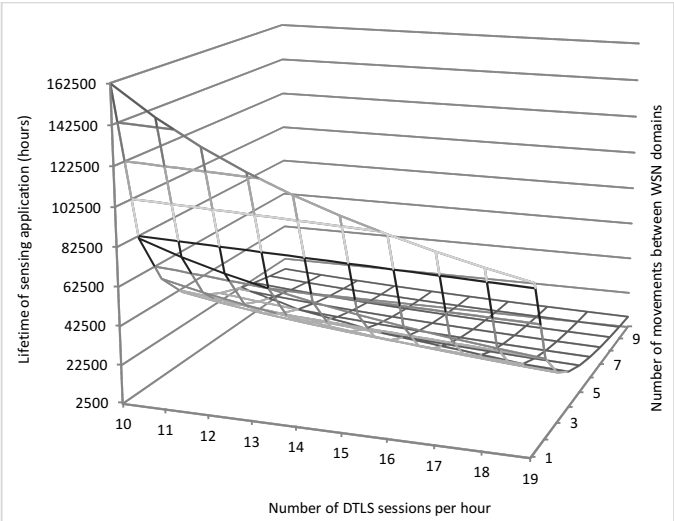

Figure 5 - Impact of end-to-end security on the lifetime of sensing applications, with mobility

We next evaluate the impact of the delegated DTLS handshake in conjugation with mobility, as illustrated in Figure 5. In this figure we illustrate the predictable lifetime (in hours) in respect to the number of DTLS sessions established with a sensing device, and also to the number of movements of the device between WSN domains. We also consider that a CoAP request (consisting of two 102-bytes 6LoWPAN packets, one containing a confirmable request and the other the corresponding reply) is served every time the sensor moves to a new WSN. The values represented in Figure 5 consider the usage of the TelosB sensing device powered by two new AA LR-6 batteries.

Even for the worst scenario (in this case 19 DTLS sessions per hour, 10 movements between WSN domains per session and 1 CoAP request per visited WSN) the expected lifetime remains above 8500 hours. It is clear that for less demanding scenarios in respect of mobility, we are able to obtain much better values. For example, when considering 14 DTLS sessions per hour and 5 movements between WSN domains, the predictable lifetime is around 23 thousand hours, thus 3 times over the previous calculation. We also observe an expressive decline in the expected lifetime when mobility requires more changes in the WSN, during the lifetime of a DTLS session. This is due to the fact that we are securing mobility-related communications with AES/CCM, and as the number of movements increases the impact of AES/CCM security is larger than that of supporting the DTLS handshake. Overall, from our previous evaluation, we are able to confirm that the proposed security and mobility mechanisms are able to provide viable lifetime values is all of the considered usage scenarios.

C. *Maximum communications rate*

Wireless sensing devices as the TelosB don't possess mechanisms such as multi-threading, and as such the computational time required to support security directly influences the maximum communications rate that a sensing device may support. IoT applications may thus suffer if security is too resource demanding, also from the perspective of its computational requirements.

As for energy, we experimentally measure the computational time required to support the proposed mechanisms. As expected, the time required to support the mediated DTLS handshake (15.39ms) is much lower than to support the original handshake (10.09s), again due to the computational impact of ECC [8]. We are able to analytically derive the maximum number of CoAP requests per hour that a device is able to sustain, in the presence of end-to-end security and mobility, as illustrated in Figure 6.

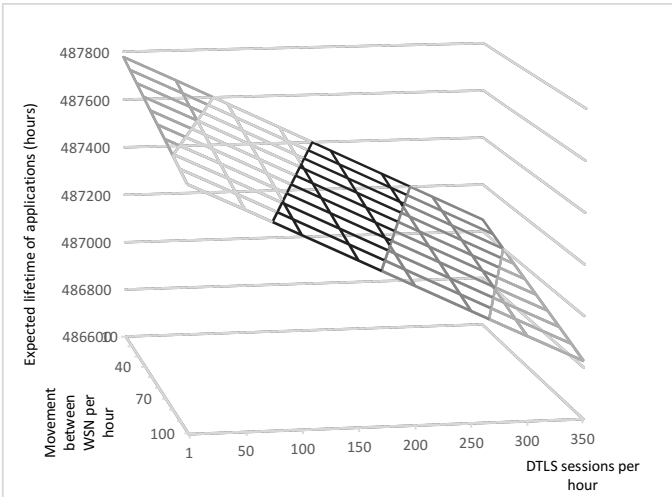

Figure 6 - Impact of end-to-end security and mobility on the communications rate of sensing applications

We must note that mobility also impacts on CoAP communications, as while processing mobility-related procedures the sensing device is unable to accept and serve CoAP requests. As we may observe in Figure 6, the proposed security and mobility mechanisms are able to still guarantee appropriate communication rates. We may note that for

example in the worst case scenario (as considered, for 350 DTLS sessions established per hour, or around 10 sessions per second, and 100 movements of a device to a new WSN domain), a sensing device would be able to still serve over 480 thousand requests during one hour, or over 133 per second. We may objectively consider this to be well above what would be required from a sensing device constrained in terms of energy, in a real application scenario. If one compares end-to-end security with mobility against the usage of DTLS as currently proposed we observe that, even with the added cost of dealing with mobility, the solution proposed in this article performs better. Due to the cost of supporting ECC encryption, the original DTLS handshake as proposed for CoAP is only viable up to 356 DTLS sessions per hour.

VI. Related Work

The employment of DTLS to secure CoAP communications raises various issues, as addressed throughout the article, that are also recognized and the focus of research. As previously discussed, ECC as proposed to provide security to CoAP is too resource demanding, and in this context alternatives approaches are being proposed. The impact of ECC cryptography, as well as the efficiency of AES/CCM to support pre-shared key authentication, is also verified in other works [17][18][19]. Other aspects complicating the adoption of DTLS are the need to store and process public-keys and certificates on constrained sensing devices, and the inadequateness of the protocol when CoAP proxies are employed. As previously observed, those are aspects that also contribute to motivate our approach.

Some authors address the proposal of usage profiles for DTLS, in order to better cope with the employment of 6LoWPAN and the characteristics of constrained wireless sensing platforms, as in [20]. Others propose modifications to the standard itself, for example the adoption of 6LoWPAN IPHC compression as a way to reduce the size of DTLS headers [21]. An alternative proposal in this context consists in the usage of CoAP communications to support costly DTLS handshake operations [22]. Overall, such proposals to do not solve the problem of effectively supporting ECC-based authentication and key negotiation on constrained sensing devices, nor address the need to cope with mobility.

More close to our approach in this article, authors in [23] propose a mechanism based on a proxy to support sleeping devices. In this work a mirroring mechanism is employed to serve data on behalf of sleeping smart objects. We also note that this proposal does not offer a solution to address true end-to-end security, the same applying to mobility. In [24] an end-to-end architecture supporting mutual authentication with DTLS is proposed, employing specialized trusted-platform modules (TPM) supporting RSA cryptography on sensing devices. Thus, RSA is adopted with the help of specialized hardware devices, rather than supporting ECC public-key cryptography as currently required for CoAP. Although this proposal addresses end-to-end security, it does not provide compatibility with the current CoAP specification nor does it address mobility.

Overall, we observe that none of the previous proposals offers a solution to effectively support ECC cryptography in the context of end-to-end DTLS security with Internet-integrated sensing devices, in a transparent fashion to the communicating entities and applications, and also supporting mobile devices.

VII. Conclusions and Future Work

In this article we propose mechanisms for the support of end-to-end security with Internet-integrated mobile sensing devices, in the context of an integration model that, in practice, supports various usage scenarios and applications. As previously discussed, we focus on addressing three important aspects that, in the context of real applications, difficult the employment of CoAP with end-to-end DTLS security. One is to offer an effective and transparent solution to the problem of supporting ECC authentication and key agreement, one important goal to support CoAP communications with a high degree of security. Other aspect is the incompatibility of DTLS with the usage of CoAP proxies, which may be supported at the security gateway (6LBR) in our model, while also implementing other security policies. Finally, we also address mobility, and propose a way to abstract end-to-end communications and security from the movement of sensing devices.

The proposed mechanisms were evaluated experimentally considering two main aspects: the impact of such mechanisms on the energy of sensing devices, and also the computational cost. We consider such two aspects to be fundamental in evaluating the effectiveness of any proposal on security for constrained wireless sensing platforms.

It is our goal that the proposed security and mobility mechanisms may provide useful contributions, in the context of the communications and security stack currently being formed to support future IoT applications. As future research objectives, we will target the design of additional security mechanisms based on the integration model considered in this article. One aspect we plan to focus on in the near future is that of intrusion detection or content filtering for CoAP communications. From the proposed mediated DTLS handshake we note that, after the handshake has finalized, the 6LBR may also be in possession of the security data required to compute the cryptographic material used for end-to-end security with DTLS. This opens to door to the design of filtering or intrusion detection mechanisms for CoAP, based on 6LBR devices that, by nature, are placed strategically to protect Internet-integrated WSN domains from abusive CoAP requests or other external threats.

References

1. Kushalnagar N et al. IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals. *RFC 4919*, 2007.
2. Montenegro G et al. Transmission of IPv6 Packets over IEEE 802.15.4 Networks. *RFC 4944*, 2007.

3. Hui J et al. Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks. *RFC 6282*, 2011.
4. Shelby Z et al. Constrained Application Protocol (CoAP). draft-ietf-core-coap-13, 2012.
5. Shelby Z. Constrained RESTful Environment (CoRE) Link Format. *RFC 6690*, 2012.
6. Rescorla E et al. Datagram Transport Layer Security Version 1.2. *RFC 6347*, 2012.
7. TelosB Mote Platform, http://www.memsic.com/userfiles/files/Datasheets/WSN/telosb_datasheet.pdf (accessed Mar 2016).
8. Granjal J, Monteiro E and Silva J. "End-to-end transport-layer security for Internet-integrated sensing applications with mutual and delegated ECC public-key authentication." *IFIP Networking Conference, 2013*. IEEE, 2013.
9. Granjal J, Monteiro E and Silva J. "Security in the integration of low-power Wireless Sensor Networks with the Internet: A survey." *Ad Hoc Networks* 24 (2015): 264-287.
10. Dierks T, Rescorla E. The Transport Layer Security (TLS) Protocol, Version 1.2. *RFC 5246*, 2008.
11. Neuman B, Ts'o T. Kerberos: an authentication service for computer networks. *IEEE Communications Magazine,* 1994, 32(9), 33-38, DOI: 10.1109/35.312841.
12. Shelby Z et al. Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs). *RFC 6775*, 2012.
13. TinyOS Operating System, http://www.tinyos.net/ (accessed Mar 2016).
14. Standalone hardware AES Encryption using CC2420, http://cis.sjtu.edu.cn/index.php/The_Standalone_AES_Encryption_of_CC2420_(TinyOS_2.10_and_MICAz) (accessed Mar 2016).
15. Liu A, Ning P. TinyECC: A Configurable Library for Elliptic Curve Cryptography in Wireless Sensor Networks. Proceedings of the 7th h international conference on Information processing in sensor networks (IPSN '08), 2008.
16. LibCoAP, http://sourceforge.net/projects/libcoap/ (accessed Mar 2016).
17. De Meulenaer, G. et al. On the energy cost of communication and cryptography in wireless sensor networks. Networking and Communications, 2008. WIMOB'08. IEEE International Conference on Wireless and Mobile Computing,. IEEE, 2008.
18. M. Botta, M. Simek and N. Mitton, "Comparison of hardware and software based encryption for secure communication in wireless sensor networks," *Telecommunications and Signal Processing (TSP), 2013 36th International Conference on*, Rome, 2013, pp. 6-10. doi: 10.1109/TSP.2013.6613880
19. Raza, Shahid, et al. "Secure communication for the Internet of Things—a comparison of link-layer security and IPsec for 6LoWPAN." *Security and Communication Networks* 7.12 (2014): 2654-2668.
20. Tschofenig H, Fossati T. TLS/DTLS Profiles for the Internet of Things. Constrained Application Protocol (CoAP). draft-ietf-dice-profile-17.txt, 2015.
21. Shahid R, Daniele T and Voigt T. 6LoWPAN compressed DTLS for COAP, 8th IEEE International Conference on Distributed Computing in Sensor Systems (DCOSS), 287-289 2012 doi: 10.1109/DCOSS.2012.55.
22. Brachmann M et al. End-to-end transport security in the IP-Based Internet of Things. 21st International Conference on Computer Communications and Networks, 1-5 2012 doi: 10.1109/ICCCN.2012.6289292.
23. Sethi M, Jari A and Ari K. End-to-end security for sleepy smart object networks, 37th IEEE Local Computer Networks Workshops, 964-962 2012 doi: 10.1109/LCNW.2012.6424089.
24. Kothmayr T et al. DTLS based Security and Two-Way Authentication for the Internet of Things, Ad Hoc Networks, 11 (8) 2710-2723 (2013) doi: 10.1016/j.adhoc.2013.05.003.