JITEL 2017
XIII Jornadas de Ingeniería Telemática
27-29 Septiembre 2017, Valencia (España)

Actas de las XIII Jornadas de Ingeniería Telemática (JITEL 2017), Valencia (España), 27-29 de Septiembre de 2017.

ISBN: 978-84-9048-595-8
DOI: http://dx.doi.org/10.4995/JITEL2017.2017.6491

Feasibility assessment of a fine-grained access control model on resource constrained sensors

Mikel Uriarte, Jasone Astorga, Eduardo Jacob, Maider Huarte
Departament of Communications Engineering,
University of the Basque Country UPV/EHU
Bilboko Ingenieritza Eskola, Urkixo Zumarkalea S/N, 48013 Bilbo, Bizkaia
muriarte@nextel.es, jasone.astorga@ehu.eus, eduardo.jacob@ehu.es, maider.huarte@ehu.es

***Resumen*—Upcoming smart scenarios enabled by the Internet of Things (IoT) envision smart objects that expose services that can adapt to user behaviour or be managed for higher productivity. In such environments, smart things are cheap and, therefore, constrained devices. However, they are also critical components because of the importance of the information they provide. Therefore, strong security is a must, but not all access control models are feasible. In this paper, we propose the feasibility assessment of an access control model that deals with a hybrid architecture and a policy language that provides dynamic fine-grained policy enforcement in the sensors, which requires an efficient message exchange protocol called Hidra. This experimental performance assessment conveys a prototype implementation, a performance evaluation model, the measurements and the related discussions, which demonstrate the feasibility and adequacy of the analysed access control model.**

***Palabras Clave*—access control, authorization policy language, constrained device, Internet of Things, security**

I. INTRODUCTION

The Internet of Things (IoT) concept conceives an interconnected network of things, the smarter the better, contributing to a higher awareness, enhanced decision making, and more adaptive behaviour of systems supporting any business process integrating pervasive and ubiquitous ICT technologies. IoT also implies a massive deployment of sensors and actuators, which, aiming at being cheap, are implemented in a range of constrained devices, constrained device sensors (CDSs) from now on, classified according to IETF [1], from severely constrained C0 to less constrained C2. Moreover, depending on the use case and location, they may require power autonomy, and therefore, require low power consumption mechanisms.

In such IoT applications, security (more specifically, access control) remains an insufficiently solved problem since existing approaches are challenged by divergent properties as tightness and feasibility. Consequently, in this paper, we propose the feasibility assessment of an access control model based on an expressive policy language enabling tight enforcement in CDSs. Such access control model includes a protocol that enables secure provisioning and enforcement of dynamic security policies as well as an audit trail, and this protocol is the subject of the performance evaluation driven through a prototype implementation.

Beyond the traditional producer behaviour of CDSs, which publish measurements and events to message brokers, in more advanced IoT scenarios, CDSs behave as tiny information servers. Specifically, requesting clients directly query the tiny CDS servers, establishing a secure end-to-end (E2E) communication. These exposed services enable usage, operation, maintenance and manageability of CDSs over their entire life-cycle and protect the value stream of the connected objects. For example, an end-user can access directly to tune personal parameters such as gender, age, weight, etc. in a health constant monitoring sensor. Moreover, the use of intermediary proxies is avoided because on one hand, they are specific for each protocol or application and are not flexible enough, and on the other hand, breaking the security association into two or more sub-transmissions might not be considered acceptable from a security point of view.

Fig. 1 shows an IoT schema that conveys different roles in various domains, operating, monitoring and controlling related business process through applications and fully aligned with the functional decomposition view of the IoT architecture reference model (ARM) [2].

In this context, the accuracy and correctness of the information exchanged with CDSs is crucial. Protecting this information requires the implementation of appropriate security mechanisms that include fine-grained access control mechanisms based on expressive policies and that can guarantee essential security properties such as confidentiality, integrity, availability, authenticity and non-repudiation [3], [4], [5]. However, implementing these appropriate security mechanisms in resource-constrained CDSs is not straightforward. Currently, one of the key challenges for enabling broader adoption of smart things is

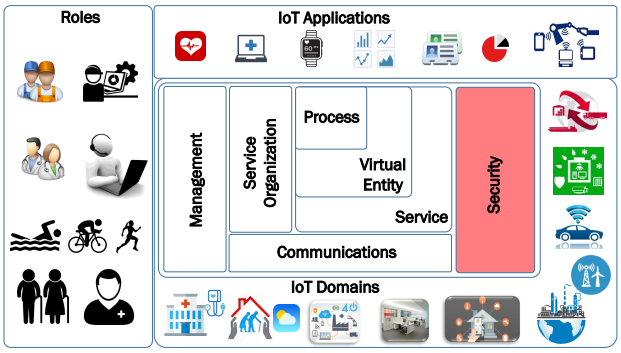


Fig. 1: Scenario schema where several stakeholders playing different roles access IoT applications on different IoT domains. The core shows the functional decomposition view of the IoT reference architecture, where security functional group is highlighted.

the availability of feasible access control solutions. Moreover, due to the extremely dynamic nature and purpose of applications based on services in sensors, policy-based security must be enforced locally in the CDSs, where resources are scarce.

The main contribution of this paper is a feasibility assessment of such a highly expressive E2E access control model in severely constrained devices (C0 and C1 CDSs), based on an experimental performance evaluation.

The rest of the paper is organized as follows. Related works are presented in Section II as the state of the art. The proposed access control model is specified in Section III. The performance evaluation conveying an experimental prototype is discussed in Section IV. Finally, the main conclusions of the paper are presented in Section V.

II. STATE OF THE ART

In the last years, the research area related to security in IoT has received a significant attention, dealing with the design of different architectures, security protocols and policy models. But security still remains as the main obstacle in the development of innovative and valuable services [3]. In fact, traditional security countermeasures cannot be applied directly to CDSs in IoT scenarios, because they are too resource consuming and not optimized for resource deprived devices. Additionally, existing feasible E2E access control approaches do not implement an expressive and therefore fine-grained and tight security policy enforcement [6].

For feasibility reasons, a centralized architecture based on traditional standards and protocols, where a central access control server (ACS) with no resource constraints makes authorization decisions for each access request, could be initially a possible option. But this approach does not consider local context conditions in CDSs, and it implies high energy consumption as well as network overhead due to continuous communications between the CDSs and the ACS.

A recent alternative approach is the distributed capability based access control (DcapBAC) [7], where an unforgeable token exchangeable as a capability, grants access to its holder in a more agile way. However, the token is designed in a XML schema and it has not been validated in constrained devices.

In any case, this approach has been adopted by some other designs involving technologies specifically defined for IoT, which enable CDSs to make local authorization decisions based also on local conditions [8], since the capabilities might include conditions represented as tuples (type, name, value). Per contra, this approach is based on public key cryptography (PKC) which is heavier than symmetric key cryptography (SKC) by means of resource consumption. Additionally, the conditions are limited to matching because the approach does not support expressions. Moreover, its syntax is not optimized by means of codification since it uses JSON, it does not support the enforcement of additional obligations and it has been validated in not so constrained C2 devices.

In this line, the delegated CoAP [9] authentication and authorization framework (DCAF) [10] defines a token to distribute pre-shared keys, and if authorized, a handshake is done to establish a DTLS channel. Local authorization policies are specified as conditions serialized in a concise binary object representation (CBOR), instead of JSON, aiming at compacted payloads in CoAP protocol. But CBOR is a general purpose serialization solution [11] and the resulting compression is not sufficiently optimized for security policies in very constrained C0 and C1 devices, where fine-grained access control is aimed through a higher but feasible policy language expressiveness, beyond the conditions consisting of simple constant matching of existing local attributes.

In other line, the usage control model and the attribute based policy schema [12] extend traditional access control systems to a continuous protection of the resource during access by the definition of obligations to enforce usage control. However, there is not an approach addressing the feasibility in CDSs.

Finally, attending to the protocols for the instant provisioning of the policy during the E2E security association in a secure session, Ladon [13], which is inspired in Kerberos, is susceptible to be evolved for that purpose. In fact, Ladon is specifically designed for very constrained devices, but it does not directly support the provisioning of an expressive policy.

Consequently, currently no suitable solution exists to provide authentication and fine-grained authorization processes in the envisioned scenarios of constrained but manageable sensor networks, and additionally, neither of the above considered approaches implements any accounting feature.

III. ACCESS CONTROL MODEL

The E2E access control model subject of feasibility assessment is based on an efficient policy language and codification, which are specifically defined to gain expressiveness in the authorization policies and to keep the viability in very constrained devices. Besides the

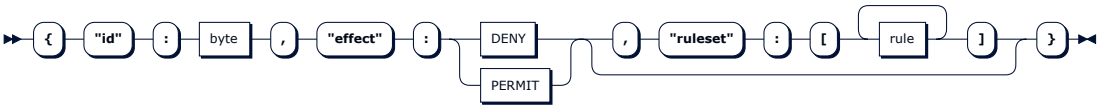


Fig. 2: Policy construct definition.

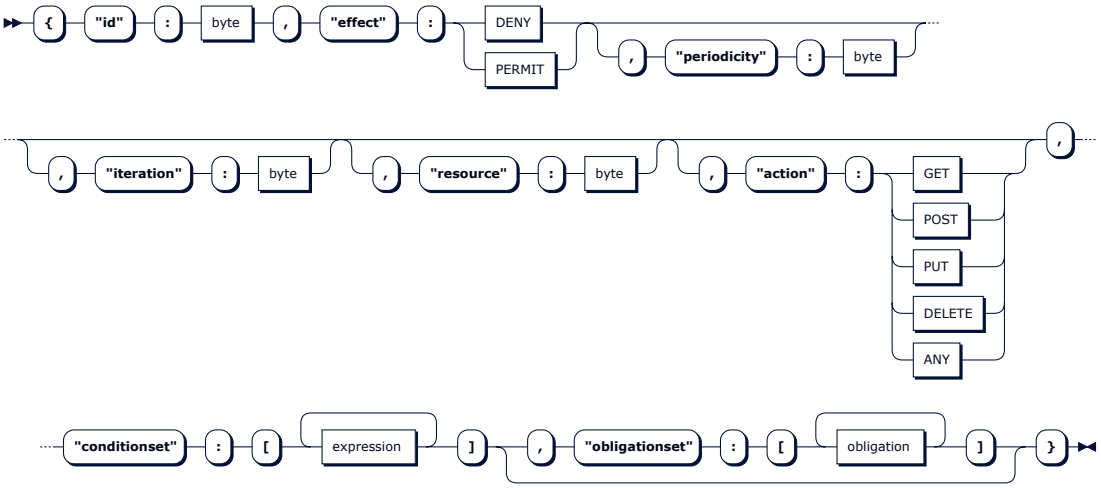


Fig. 3: Rule construct definition.

policy language, the access control model conveys the E2E feasible security association between two mutually authenticated peers, and consists of an architecture to enable multi-step authorization as well as a protocol for the provisioning and enforcement of a dynamic security policy in the CDSs.

A. Authorization policy language and codification

In this section, an expressive policy language is briefly presented. The goal of this policy language is to enable the enforcement of tighter access control policies in CDSs, overcoming the resource constraints. In fact, this policy language definition enables both to make granting decisions based on local context conditions, and to react accordingly to the requests by the execution of additional tasks defined as obligations.

A resulting policy instance is defined, like in the general event-condition-action approaches, as an optional set of rules, which specifies both the conditions to be checked and the related reactions, in enforcement time. Specifically, this policy language stands for a sequence of constructs with particular meaning in the decision making and enforcement time.

Some of the constructs are defined as mandatory, and some others as optional, enabling to shorten the length of the policy when a simple policy is enough. Additionally, some constructs are extended through other nested constructs, and some of them can be instantiated many times within a container construct. Related to this elasticity feature, the more constructs, the higher the expressiveness of the policy, so the more granular the policy is, and consequently, the tighter the enforcement is. Consequently, the challenge to overcome is to be feasible even in the most expressive use-case.

The policy language enables a policy instantiation through the *policy* construct, with three nested constructs as depicted in Fig. 2. First of all, a policy instance identification, *id*, is specified for logging, tracking and auditing purposes. Then, a default policy granting *effect* is specified. This effect will prevail in the case of absence of rules, or any rule evaluation conflict. Lastly, optionally, an array of rules may be instantiated as a *ruleset* to specify the conditions and related reactions. Each *rule* in the array is an extensible construct.

The *rule* construct depicted in Fig. 3 is defined as a sequence of eight nested constructs, where the order is crucial. Some of them, such as *id*, *effect*, and *conditionset* are mandatory, and the rest named *periodicity*, *iteration*, *resource*, *action* and *obligationset* are optional. The *conditionset* and the *obligationset* are arrays of expressions and obligations respectively. These repeatable and extensible *expression* and *obligation* constructs are defined in a similar way enabling the instantiation of rich expressions on attributes declared as inputs as well as reactive tasks declared as obligations.

The length of any policy instance, in a human readable format, grows proportionally with the aimed tightness, and it would impact negatively in the performance. So a specific policy instance codification is considered, distinguishing from existing ones that serialize policy instances through standardized generalist solutions such as CBOR.

The considered policy codification serializes each construct and concatenates them in a bit stream. In fact, it takes profit of beforehand knowledge of the defined sequence of the constructs, and their format. An additional crucial factor is the injection of some agreed bit masks,

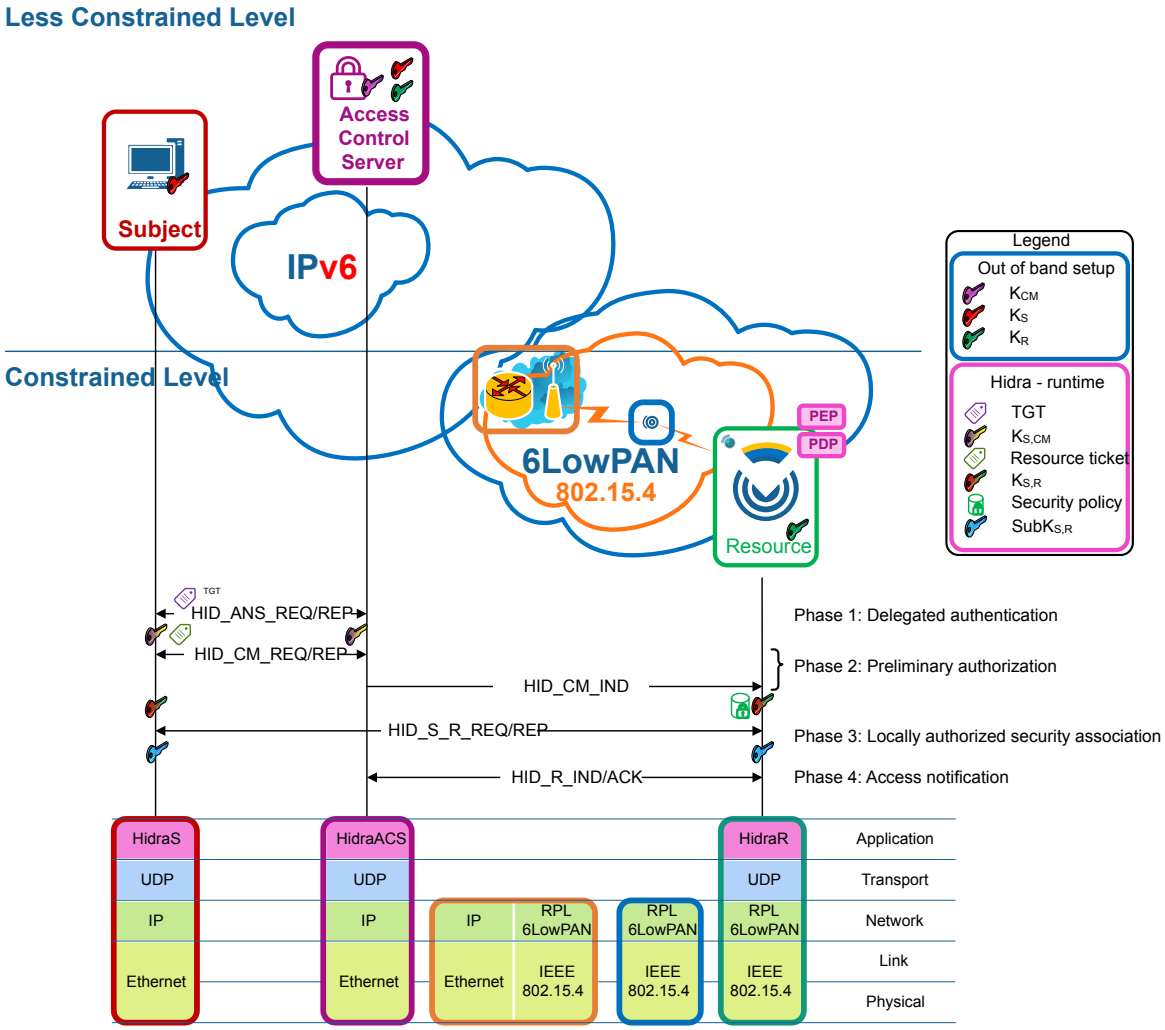


Fig. 4: Performance evaluation scenario. Hidra protocol messages and security association establishment related authentication, authorization, key exchange and notifications.

to specify the existence or not of optional constructs. It enables to deal optimally with the elasticity defined in the policy language, avoiding unused but expected fields of expressive policies, greatly reducing the length.

With respect to covered policy formats, this policy codification can easily be applied to any original policy instance format (XACML, JSON, *etc.*), from textual files to structured policy instance representations. For example, four different instances of sample policies in the testlab, represented in JSON with lengths of 23, 118, 174 and 554 bytes, which are codified in CBOR with lengths of 14, 81, 123 and 391 bytes respectively, are notably reduced to 2, 7, 9, and 32 bytes using the considered codification.

B. Hidra messaging protocol

In order to efficiently convey the presented access control policies to the CDSs, the Hidra protocol is considered. Hidra, depicted in Fig. 4, is based on a three parties architecture, and provides authentication, authorization in two steps, dynamic policy provisioning and accounting.

Hidra is based on Ladon [13], which is a validated solution for the establishment of E2E security associations, through pair-wise keys, guaranteeing mutual authentication and authorization in very CDSs.

Both Hidra and Ladon are based on symmetric key cryptography and they assume that each endpoint owns a secret key shared with the ACS. The operation is based on the use of tickets, a capability distributed by the ACS that contains a proof of the identity of the subject that requests it. Tickets are encrypted so that only the entities which they are intended for, are able to decrypt them.

After a successful authentication in the ACS (Phase 1) the subject that wants to access a service in the CDS obtains a ticket granting ticket (TGT). This TGT is used by the subject to obtain resource tickets (Phase 2) required to access any resource on the CDSs.

This approach enables the attribute based access control (ABAC) authorization enforcement in two steps. On the first one, as condition to release any resource ticket, fine-grained preliminary access control is performed in the ACS (Phase 2), focusing on the attributes of the subject, resource and expected actions. If this first authorization step is successful, the ACS sends a message to the subject including a resource ticket, and also sends a message

to the CDS conveying an expressive authorization policy instance. This instantaneous custom policy provisioning avoids permanent policies' storage in the CDS and reduces network overhead comparing with approaches enclosing the policy in the resource ticket.

On the second authoritative step, once the subject has obtained a resource ticket, the local context based access control is performed in the CDS (Phase 3). First, the proper rule is evaluated to make the granting decision, and then the corresponding reactive actions are enforced. In a positive authorization case, the result is a shared session key to be used on further E2E resource access exchanges.

Another novelty of Hidra with respect to Ladon is the addition of a pair of messages to enable precise accounting (Phase 4). By means of these messages, the CDS will notify details like who performed what, where and when in each and every access request received from the subject. These notifications are gathered, normalized, and treated properly by the ACS. Additionally, the ACS can react and send a related policy message, enabling the dynamic delegation, request, cancellation and revocation of permissions.

Then, while the security association is not finalized, the access control is enforced in the CDS autonomously in each and every further request attempt, since the received expressive policy (Phase 2) includes related rules.

Consequently, unified, coherent and adaptive management of the policies by the ACS is achieved. Additionally, the proposed Hidra protocol and the adopted architecture enable to rely the most expensive features on the ACS, which entails the usage of standard security and access control technologies in the non constrained interactions. It also achieves that most unauthorized access attempts are refused before reaching the CDS, avoiding unsuccessful message exchanges and thus, saving energy in the CDS, which is a crucial aspect.

IV. PERFORMANCE EVALUATION

In this section, the experimental performance analysis of an access control model for E2E security in CDSs is carried out conveying the establishment of a security association between a requesting subject and a CDS. For performance analysis there are three main options: analytical evaluation, specific network simulation and prototype implementation. Even though this third one is more complex and expensive, this proposal conveys an Hidra protocol implementation prototype in order to present more accurate and realistic performance results. Therefore, the performance analysis covers the measuring and evaluation of the crucial performance parameters of such resource constrained sensing environments.

First, the reference scenario, some assumptions and its implementation through software codification and configurations are discussed. Then, the crucial performance parameters are identified, and their measurement methods and computation are described. Finally, an analysis of the measurements is presented, describing and discussing the evaluation results.

The overall goal is to demonstrate the suitability of the designed access control model for CDSs in the envisioned scenarios.

A. Test-bed implementation

The testing scenario for the performance evaluation is graphically depicted in Fig. 4. In this scenario, a subject is connected to the Internet and establishes an E2E connection with a resource running on a CDS in an IEEE 802.15.4 network. A 6LoWPAN router (in orange) acts as the LowPAN coordinator and connects a beacon-enabled lineal structure to the Internet. The IEEE 802.15.4 network is 2-hops deep, which is considered significantly large for validation purposes. The PAN router coordinator has a child coordinator implemented in a TelosB [14] sensor, which controls one leaf node. In this node the CDS exposes resources as management services, and it is implemented in an C0 hardware platform IRIS [15] sensor with Contiki OS [16].

In the implementation two aspects are distinguished: on one hand, network protocols and connectivity, and on the other, Hidra messaging protocol as an application.

Fig. 4 shows implemented protocol stacks in all entities involved in the performance evaluation scenario. The implemented network enables E2E IPv6 connectivity through a multi-hop IEEE 802.15.4 sensor network, in 2.4 GHz band. Note that IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL) [17] is configured to set a multi-hop hierarchical node network with neighbour discovery functionalities within the IEEE 802.15.4 network. The network configuration is done through sensor *ID* setting and registration as a first step, and then UDP messaging module is installed.

Then, Hidra messaging protocol application is made by different software modules covering different functions in each of the three parties involved in the protocol: subject, ACS, and sensor.

Hidra in the sensor side, which means the biggest impact, is codified and installed as a server application on top of Contiki OS. In fact, it receives an indication and a policy from the ACS, and a request from the subject. So it checks the validity of the messages, the identities and the service ticket, prior to evaluating the policy locally and making a granting decision related to the security association establishment requested by the subject. Finally, it notifies any activity to the ACS through log messages for further tracking and auditing.

This sensor side Hidra module implements also an unique UDP socket to wait for any of the possible messages in order to be more efficient in memory footprint. Once a received message is identified, it is parsed and proper protocol related checks, validations and reactions are performed following an specific flow.

During development some design decisions were made. Specifically, where message authentication codes (MACs) are 16 bytes long; message cyphering is done with AES-128 and it is combined with Ciphertext Stealing algorithm to avoid size increments with respect to cleartext

messages. Cryptographic libraries are TomCrypt and tiny-AES-128 [18].

B. Performance modelling

To conduct a performance evaluation of the proposed access control model for E2E security in CDSs, the experimental performance model focuses on three critical parameters: (1) the response time of the access control model to establish an authorized E2E secure session, (2) the energy cost of this model for the protected CDS running on finite batteries, (3) the model's impact on the local storage on the CDS and memory footprint.

The response time needs to be below an accepted value if the proposal is to be useful, and the energy consumption, local storage, and memory footprint, due to the nature of the CDSs and their constraints on resources, cannot exceed rational and proportional limits.

1) Response time: During the establishment of a security association, five messages are exchanged, as detailed in Section III.B. This response time includes the steps where the subject requests and obtains the service ticket, the notification that the ticket is granted, policy provisioning in the CDS by the ACS, and the security association request and response between the subject and the CDS.

In order to measure this time, some few code lines are inserted in the subject's side software code, setting two timestamps: one at the beginning of the security association establishment and the other at the end of this establishment.

2) Energy consumption: Regarding the energy cost measurement, the energy consumed by the transmission and reception of bits over the air and the message processing are considered.

For the measurement of the processing energy consumption, two timestamps are inserted in the sensor's side, at the beginning and the end of the message processing software code. Once measured the time to process each message, a constant instantaneous power consumption (P_C) provided by the manufacturer in the datasheet is considered in order to compute the energy consumption of each message.

For the computation of the power consumption due to the transmission and reception of each message, involved message lengths in bytes and packet fragmentation are computed (considering 50 bytes of longest IEEE 802.15.4 plus UDP/6LowPAN headers). According to Ladon protocol message lengths [13], in which Hidra protocol is based, the lengths of the messages exchanged during the authentication and authorization protocol range from 15 to 63 bytes. Enclosing the policy in the HID_CM_IND message (33 bytes), which is one of the smallest, implies the minimum fragmentation of 6LowPAN IPv6 packets over IEEE 802.15.4 links. This design decision makes a difference with respect to the approaches for enclosing the policy in the ticket, which is included with larger request messages. Therefore, it can be anticipated a proportional and optimized impact in the length of a message from injecting the compressed policy into the shortest one. In particular, the length of the instantiated policy in this proposal is 2 bytes and consequently, the total length of the HID_CM_IND message is 35 bytes.

Tabla I: Parameters used to characterise the energy consumption of sensor nodes

Name	Description	Value
B_N	Effective network wireless link data bit rate	70Kbps
P_{RX}	Power consumption in reception mode	48 mW
P_{TX}	Power consumption in transmission mode (3dBm)	51 mW
P_C	Power consumption in message processing mode	8 mW

Additionally, constant reception and transmission power consumption rates provided by the manufacturer in the data-sheet and a constant propagation bit rate are also considered. Table I shows testlab real-conditions (non-optimal) network data bit rate and the different instantaneous power consumption values used for the analysis. Note that these power consumption values correspond to a MEMSIC IRIS mote (XM2110CA) powered with a $3V$ power supply [15].

Finally, the power consumption is calculated as the sum of the individual power consumptions of each of the involved messages in the sensor.

3) Storage and memory footprint: In this subsection, the increase of permanent storage and the memory footprint generated by the proposed access control model are considered. Specifically, the storage and memory footprint for the instant provisioning of a received access control policy and the code needed to parse it, as well as the data blocks related to the messages of the Hidra protocol, are considered together.

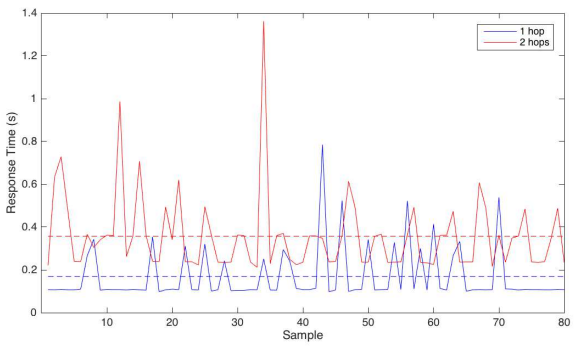
On one hand, regarding the permanent storage for the mentioned entities, the symmetric key shared with the ACS, the access control policy, the code to parse the received policy and the code to run the Hidra protocol are considered the additional minimum entities that should be permanently stored in a CDS along with some original resources and sensing applications.

On the other hand, regarding the memory footprint, the data required for the Hidra protocol message exchange are considered: namely, the session keys shared with the subject, the subject identity, the different data needed to identify the messages and to guarantee their freshness, the lifetime of the security association, and the log of each access provisionally wrapped until the reception of the acknowledgement from the ACS. However, some of these values are loaded and erased during the reception, processing and transmission of relatively consecutive messages.

Measurement of code plus data storage and memory footprint is done through a particular command (*size*), which provides with both static and dynamic occupied memory amounts.

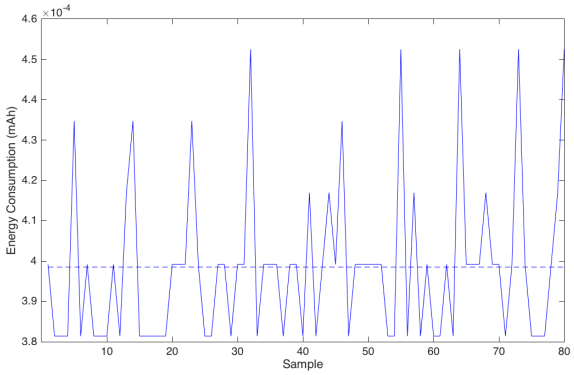
C. Performance analysis

In this section, the measurement results obtained on the experimental prototype described in the previous section are used to analyse the mean response time and energy consumption to establish a secure session, as well as the impact on the local storage and memory footprint. Response time and energy consumption have been measured



	Average (s)	Median (s)	St. Dev. (s)	95 % Conf. Int. (s)
1 hop	0.1689	0.1080	0.1293	(0.1405,0.1972)
2 hops	0.3576	0.3440	0.1834	(0.3174,0.3978)

Fig. 5: Response time of security association establishment considering 80 requests in two network configurations: one and two hops.



	Average (µAh)	Median (µAh)	St. Dev. (µAh)	95 % Conf. Int. (µAh)
1 hop	0.3985	0.3992	0.0199	(0.3941,0.4029)

Fig. 6: Energy consumption in security association establishment considering 80 requests in an one-hop network configuration.

by 80 samples, so potential measuring error is reduced. Additionally, response time has been measured with two different configurations: one hop and two hops respectively, so the impact of the intermediate node insertion can be measured.

1) Response time: First, impact of Hidra on performance is conveyed measuring response time of 80 subject's security association establishment requests, considering both network configurations: with one and two hops.

Fig. 5 shows that the maximum response time, even with a non-optimal network bit rate, is below $420ms$ and $637ms$ in both network configurations. This value is very good, considering that the maximum acceptable delay in interactive E2E data transactions specified by Stallings [19] is $1000ms$.

Fig. 5 showing a composition of the measurements with two configurations, points out that a second hop increases proportionally $200ms$ on average. This value could also be considered as referential increment per hop for further estimations aiming at large scale deployments.

Additionally, one related comparable response time value has been found in the literature, although there is no mention of additional performance indicators such as energy consumption. At the C2 level, [20] reveals that the comparable measured response time for the authorization response starting when the subject sends the request is $480.96ms$ (with one hop). The response time of Hidra is lower even with a worse network bit rate and, therefore, better.

2) Energy consumption: Attending to the impact of Hidra protocol on the energy consumption Fig. 6 shows measured values of power consumption related to each of 80 requests as well as the average.

This figure shows that the measured average value of power consumption is $0,3985\mu Ah$, which is a very low value. This very good result means that impact of Hidra in energy consumption is very low. In the case of two AAA batteries of $900mAh$, suming up to $1800mAh$, considering a 95% of battery performance, makes a real capacity of $1710mAh$. Therefore, more than 4 millions (4,291,006) of requests could be handled during the battery life.

In the envisioned scenario, the CDS is accessed by the subject to perform tasks such as personalization, parametrization, updating, upgrading, maintenance, and so on. These types of interactions do not occur often. As the most exigent scenario, we can consider one that requests access every hour to tune the user experience in an application where the users change hourly.

In this most exigent scenario, a subject making one request per hour, 24 per day, 8760 per year, could get response for approximately 490 years (489.840) of the battery life. Therefore, Hidra's energy consumption could be deprecated, and the battery life would depend basically on the main purpose application of the CDS.

3) Storage and memory footprint: Finally, from the storage point of view, at the CDS, the amount of RAM memory is the most limiting aspect, compared with permanent storage, which is usually an order of magnitude larger.

Assuming that measures are dependent on programming style, measurements of storage occupancy are 20836 bytes, and memory footprint is 1440 bytes. Therefore, the impact is considered acceptable considering available 128KB and 8KB of flash and RAM memory in so constrained devices such as the ones used in the implementation [15].

V. CONCLUSION

Incoming smart scenarios enabled by IoT envision smart objects exposing services to be adapted to user experience or to be managed aiming at higher productivity, often in multi-stakeholder applications. In such environments, smart things are cheap, therefore constrained devices, but they are also critical components, so security is a must. Existent approaches coping with the principle of least privilege, based on the expressiveness and updating of the policy to be enforced in the sensors, are challenged by feasibility constraints.

The proposed performance evaluation is focused on an innovative access control model dealing with a hybrid architecture and a policy language for dynamic fine-grained policy enforcement in the sensor. Such policy enforcement is based on local context conditions and correspondent obligations, not only during secure session establishment but also afterwards while the security association is in use, in order to control the behaviour of the access. Such a dynamic policy cycle avoiding local storage, is enabled by an efficient message exchange protocol, named Hidra. Actually the Hidra protocol assures the mutual authentication, the expressive policy injection, the tight policy enforcement in the secure association establishment and the derived resource access, as well as the accounting for further tracking and auditing purposes.

The proposed feasibility assessment is based on a prototype implementation of such an innovative access control model in very constrained devices. The experimental performance analysis focusing on three key performance indicators such as the response time, the power consumption and the memory footprint outcomes remarkable results. Based on these measurements, the performance evaluation of this proposal concludes the feasibility of this analysed access control model on resource constrained sensors.

REFERENCIAS

[1] C. Bormann, M. Ersue, and A. Keranen, "Terminology for constrained-node networks," Internet Requests for Comments, RFC Editor, RFC 7228, May 2014, http://www.rfc-editor.org/rfc/rfc7228.txt.

[2] F. Carrez, M. Bauer, M. Boussard, and N. Bui, "Final architectural reference model for the iot v3.0," http://www.iot-a.eu/public/public-documents/d1.5/at_download/file, July 2013.

[3] S. Sicari, A. Rizzardi, L. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," *Computer Networks*, vol. 76, pp. 146 – 164, 2015.

[4] K. T. Nguyen, M. Laurent, and N. Oualha, "Survey on secure communication protocols for the internet of things," *Ad Hoc Networks*, vol. 32, pp. 17 – 31, 2015, internet of Things security and privacy: design methods and optimization. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1570870515000141

[5] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things," *Computer Networks*, vol. 57, no. 10, pp. 2266 – 2279, 2013, towards a Science of Cyber SecuritySecurity and Identity Architecture for the Future Internet.

[6] Z. Yan, P. Zhang, and A. V. Vasilakos, "A survey on trust management for Internet of Things," *Journal of Network and Computer Applications*, vol. 42, pp. 120 – 134, 2014.

[7] S. Gusmeroli, S. Piccione, and D. Rotondi, "A capability-based security approach to manage access control in the Internet of Things," *Mathematical and Computer Modelling*, vol. 58, no. 5ï¿½6, pp. 1189 – 1205, 2013, the Measurement of Undesirable Outputs: Models Development and Empirical Analyses and Advances in mobile, ubiquitous and cognitive computing.

[8] J. L. Hernández-Ramos, A. J. Jara, L. Marın, and A. F. Skarmeta, "Distributed capability-based access control for the internet of things," *Journal of Internet Services and Information Security (JISIS)*, vol. 3, no. 3/4, pp. 1–16, 2013.

[9] Z. Shelby, K. Hartke, and C. Bormann, "The constrained application protocol (coap)," Internet Requests for Comments, RFC Editor, RFC 7252, June 2014, http://www.rfc-editor.org/rfc/rfc7252.txt.

[10] S. Gerdes, O. Bergmann, and D. C. Bormann, "Delegated CoAP Authentication and Authorization Framework (DCAF)," Internet Engineering Task Force, Internet-Draft draft-gerdes-ace-dcaf-authorize-04, oct 2015, work in Progress.

[11] C. Bormann and P. Hoffman, "Concise binary object representation (cbor)," Internet Requests for Comments, RFC Editor, RFC 7049, October 2013.

[12] Z. Su and F. Biennier, "On attribute-based usage control policy ratification for cooperative computing context," *CoRR*, vol. abs/1305.1727, 2013. [Online]. Available: http://arxiv.org/abs/1305.1727

[13] J. Astorga, E. Jacob, M. Huarte, and M. Higuero, "Ladon: end-to-end authorisation support for resource-deprived environments," *IET Information Security*, vol. 6, no. 2, pp. 93–101, June 2012.

[14] MEMSIC's TelosB mote (TPR2420CA) datasheet. [Online]. Available: http://www.memsic.com/userfiles/files/Datasheets/WSN/telosb_datasheet.pdf

[15] "MEMSIC's IRIS mote (XM2110CA) datasheet," http://www.memsic.com/userfiles/files/Datasheets/WSN/IRIS_Datasheet.pdf.

[16] Contiki: The Open Source OS for the Internet of Things. [Online]. Available: http://www.contiki-os.org/

[17] T. Winter, P. Thubert, A. Brandt, J. Hui, R. Kelsey, P. Levis, K. Pister, R. Struik, J. Vasseur, and R. Alexander, "Rpl: Ipv6 routing protocol for low-power and lossy networks," Internet Requests for Comments, RFC Editor, RFC 6550, March 2012, http://www.rfc-editor.org/rfc/rfc6550.txt. [Online]. Available: http://www.rfc-editor.org/rfc/rfc6550.txt

[18] Tiny AES128 in C. [Online]. Available: https://github.com/kokke/tiny-AES128-C

[19] W. Stallings and T. Case, *Business Data Communications: Infrastructure, Networking, and Security*, 7th ed. Pearson Education Limited, 2013, no. draft-ersue-constrained-mgmt-03, internet-draft 2, pp. 57–84.

[20] A. F. Skarmeta, J. L. Hernandez-Ramos, and M. V. Moreno, "A decentralized approach for security and privacy challenges in the Internet of Things," in *Internet of Things (WF-IoT), 2014 IEEE World Forum on*, March 2014, pp. 67–72.