Trust Extension Protocol for Authentication in Networks Oriented to Management (TEPANOM)

Antonio J. Jara

Trust Extension Protocol for Authentication in Networks Oriented to Management (TEPANOM)

Antonio J. Jara
University of Applied Sciences Western Switzerland (HES-SO)
Institute of Information Systems
3960, Sierre, Switzerland
jara@ieee.org

Abstract. Future Internet of Things is being deployed massively, since it is being already concerned deployments with thousands of nodes, which present a new dimension of capacities for monitoring solutions such as smart cities, home automation, and continuous healthcare. This new dimension is also presenting new challenges, in issues related with scalability, security and management, which require to be addressed in order to make feasible the Internet of Things-based solutions. This work presents a Trust Extension Protocol for Authentication in Networks Oriented to Management (TEPANOM). This protocol allows, on the one hand, the identity verification and authentication in the system, and on the other hand the bootstrapping, configuration and trust extension of the deployment and management domains to the new device. Thereby, TEPANOM defines a scalable network management solution for the Internet of Things, which addresses the security requirements, and allows an easy, and transparent support for the management, which are highly desirable and necessary features for the successful of the solutions based on the Internet of things. The proposed protocol has been instanced for the use case of a fire alarm management system, and successfully evaluated with the tools from the Automated Validation of Internet Security Protocols and Applications (AVISPA) framework.

Keywords: Sensor Networks Management, Security, Management Architecture, Internet of Things, Future Internet.

1 Introduction

The number and diversity of sensors and devices deployed is growing tremendously thanks to their capacities to offer low cost air-interfaces which allow an easy and quick deployment, the suitability of them to support an extended range of solutions, the infrastructure capacities to provide an Internet access to these networks, which is becoming ubiquitous to all the environments and users, and accessible for the sensors with the evolution of technologies such as IPv6 Low Power Wireless Personal Area Networks (6LoWPAN), and finally with the definition of In numerous this extension of the Internet to smart things is estimated for reaching by 2020 between 50 to 100 billion of devices defining the called Internet of Things.

A new generation of services where all the devices around the user are connected presents challenges for security management in aspects such as bootstrapping, privacy, confidentiality and trust.

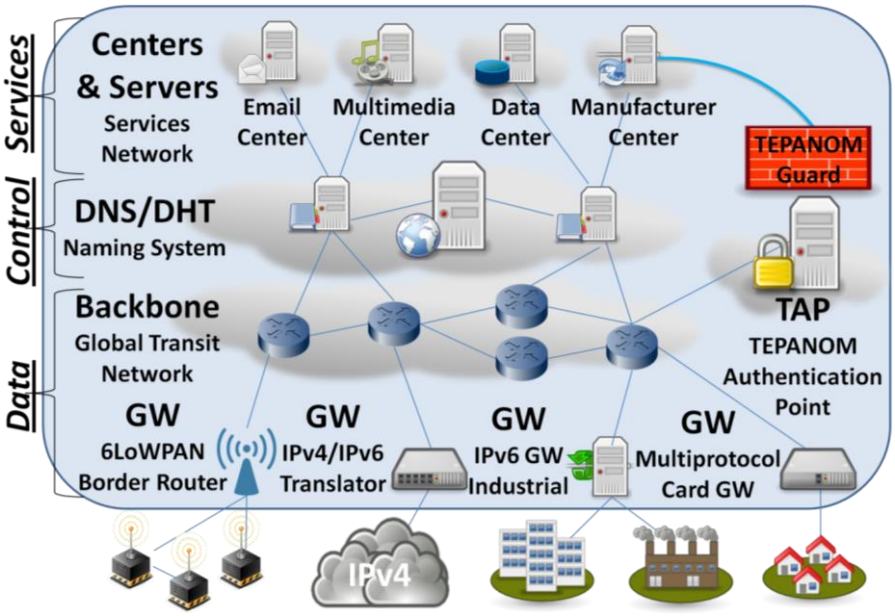

Fig. 1. TEPANOM Architecture.

This security management cannot be addressed with the traditional out-of-band and centralized techniques, which are usually considered, designed and definitively added to the service in a final stage of the solution development. This requires a definition of the management issues at the design phase, since this requires a higher level of discussion, scalability and considerations in order to solve the requirements for scalability, which present the need of manage millions of devices, for that reason it is required a new management paradigm to cope with those new challenges, since out-of-band management is not able to setup a large number of device. It is required an in-band management, with semi-automatic configuration, bootstrapping online, assisted deployment of keys, i.e. key management protocols, and authentication of devices based on identity instead of simple identifiers.

For that reason, this work is focused on offer a scalable and secure management protocol, which allows, on the one hand, the identity verification and authentication of the new devices deployed in a network, and on the other hand, the extension of the trust domain to these new devices. Thereby, with this semi-automatic bootstrapping and configuration of the new devices is more feasible, scalable and extensible the deployments based on Internet of Things. This protocol addresses the requirements from the novel services, where security is highly required and desirable, such as authentication for home automation solutions.

The major novelty from this authentication protocol is that it is focused to the manufacturer, assuming that it is the common ***trustable*** previous "control point" to the initial installation for new devices. Therefore, it is the point where it can be pre-configured a set of credentials, which can be used after to verify the identity (type of device, family, features etc.) for the devices.

In addition, this kind of identity verification allows, on the one hand, make simpler and more automatic the bootstrapping, and on the other hand to authenticate the originality from a product face to guarantee the quality from an installation. This a high requirement assuming security deployments such as fire alarms.

2 TEPANOM Architecture

The architecture considered to extend for the entities defined by the Trust Extension Protocol for Authentication in Networks oriented to Management (TEPANOM) is based on the current Internet Architecture. The layout of the considered architecture is presented in the Fig 1.

The architecture is based on the domain names and locators of the current Internet. The role of the domain/device name and locator are:

- **Domain name** represents "whose it is", are usually denoted by Uniform Resource Locator (URL) such as the used for the WEB, e.g. lab.um.es.
- **Device name** represents "who it is", are usually denoted by variable-length strings e.g. Uniform Resource Name (URN), or a human readable and remembered name such as a Network Access Identifier (NAI), e.g. *temp_sensor- 2C91@*lab.hevs.ch, which represents a sensor called *temp_sensor- 2C91* inside the mentioned domain. This name is what can be used as a base-name to access specific web services and properties/methods with technologies such as by Simple Network Management protocol (SNMP) for management, or RESTFul from a more focused Internet of Things point of view, with the Web of Things.
- **Locator** is used to represent the location of an object in the network; it usually uses the IPv6 address.

The architecture is composed by the signaling control network, which mainly defines the mentioned mapping between the domain names and its locators, the interworking infrastructure with the routers and interconnection systems for the global transit networks, and the gateways, proxies and translators for the edge networks.

2.1 Signaling control network

The roles of the entities from the signaling control network are presented in Fig. 1.

- **Domain Name System (DNS):** This offers a mapping between the hostname and domain name which a particular host or device belongs to. This stores the binding between a domain and the manager of that domain, servers and resources centers. DNS have a hierarchical structure; thereby they can be effectively organized into a hierarchical logical network. As alternative to the DNS, it can be found several solutions for the location of host and devices in the network such as Distributed Hash Tables, ID/Locator split architectures, and finally, in order to make the name/locator mapping more secure it can be also considered for this part of the architecture security extensions for DNS, i.e. DNSSEC (Domain Name System Security Extension), or for the mentioned ID/Locator architecture.
- **TEPANOM Authentication Point (TAP):** This entity is used to validate new devices/entities. This is a **Trust point**, following a similar idea to other entities such as the Trust Resolution Handlers (TRHs) defined in Data-Oriented Network Architecture (DONA) , where data needs to be registered in TRHs to validate the content and provider. In our approach, instead of data the registered entities are devices and the TAP is offered by the devices providers such as the manufacturer considered for the use case described in this work for security deployment of fire detection systems. Thereby, they can be dynamically registered and authenticated, where is presented the protocol proposed to reach this scalable security support.

2.2 Global Transit Network

This is a collection of networks and physical routers which interconnect the public organizations, research centers, and end users through Internet Service Providers around the entire world. This is composed of routers, backbones, servers, systems and agents of some of the entities mentioned from the signaling control network. The DNS and TAP are physically connected to this global transit network to store the records of host and device information, and make feasible a global access to the services of hostname resolution and provide global mobility capabilities.

2.3 Edge Networks

The edge networks provide access to the end systems such as hosts and clients through wired or wireless links. Examples can be any of the current industrial networks such as Control Area Networks (CAN), vehicular networks and hospital networks. These networks are connected to the Global Transit Network via one or more gateways. Thus a GW has at least two network interfaces, one connected to the edge network and the other to the global transit network, see Figure 1. Examples of gateways are:

- **Multiprotocol cards and adaptors:** The current situation of the Internet of Things can be compared to an archipelago, where the devices can interact with other devices from their own island, but not with devices from outside. A solution for this heterogeneity is found ins solutions such as Universal Device Gateway (UDG), or Multi-protocol cards which provide physical connectivity through various communication protocols, such as KNX and X10 from building automation.
- **Translators:** IPv4 to IPv6 translators for networks which are not adapted.
- **IPv6 gateways:** GW for networks with IPv6 support, it is the link between the ISP and the client/end user.
- **6LoWPAN Border Router:** Adapt the IPv6 packet to the defined in the 6LoWPAN standard (RFC 4494) for making IPv6 headers size feasible for constrained Low Power Wireless Personal Area Networks (LoWPANs).

3 TEPANOM Protocol

The Internet of Things deployments are being considered solutions with hundreds to thousands of nodes, what is defining a new dimension of the monitoring and control capabilities for solutions such as home automation, healthcare monitoring, and the use case considered in this work fire detectors monitoring, such as mentioned, this high capacity is presenting a critical challenge for managing in order to reach a scalable and safe management, offering a framework able to unify the functions of bootstrapping, configuration, set up, operation, check resource availability, administration and maintenance of all elements and services deployed.

The solution proposed on this work is TEPANOM, which is originally the gate guard in the temples in the islands of Thailand. It was chosen since the current

internet is presented as an archipelago formed by several islands/networks with multi-technologies and multi-domains.

The three domains involved in the process for deployment, authentication, bootstrapping and configuration of a new device are presented in Fig. 1. They are, first, the factory domain, which is the domain for the provider or manufacturer from that device. Second, the manager domain for the remote monitoring station in solutions oriented to management, and finally the deployment domain, which refers to the domain where the new device to be monitored is being deployed.

The goals of TEPANOM protocol are:

- Verify that the new device belongs to an island, network or domain which is trustable from the gateway/platform where the new device is being deployed.
- Authenticate to the new device from its factory domain, e.g. provider or manufacturer.
- Optionally this also allows to send the identity of the device from the factory domain to the manager and deployment domains, e.g. technical specification and available resources/methods for consumer devices.
- Finally, this extends the trust domain from the deployment network to that new device.

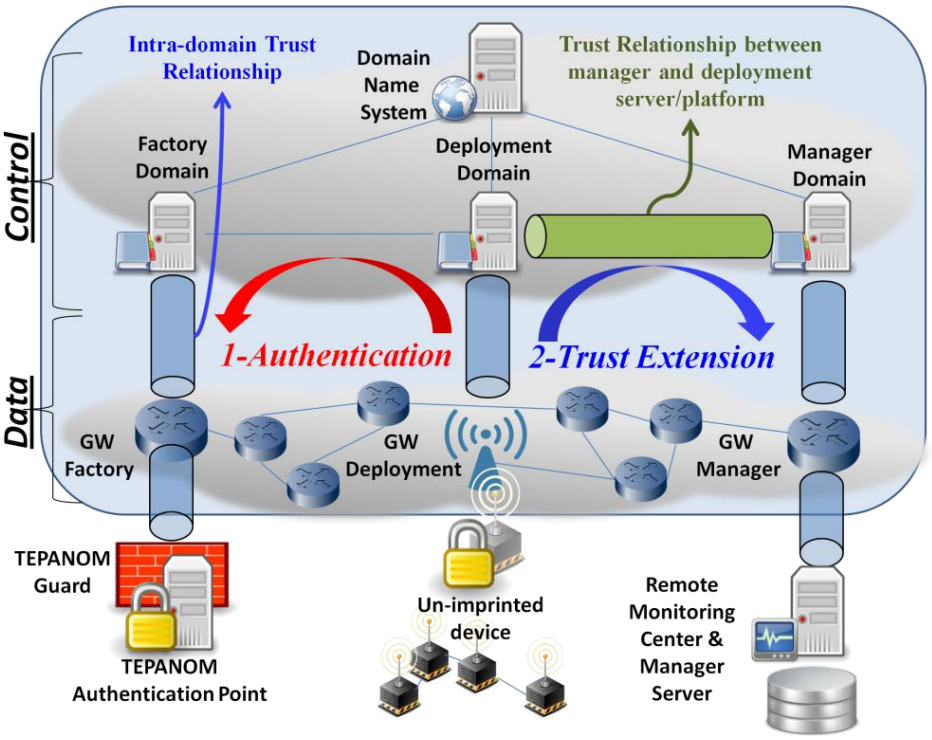

Fig. 2. TEPANOM environment and domains.

The architecture defines two planes, on the one hand the signaling control plane composed by the DNS for naming resolution, and the servers and deployed platform, for the control, and on the other hand, the data plane, which is composed by the backbone and gateways, which offer the connectivity to the signaling control network and edge networks.

In the signaling control plane, it has been defined the existence of a trust relationship between the deployment platform and the manager server, this relationship is established during the deployment of the client/user side platform, e.g., the deployment of the residential platform for home automation solutions (see green tunnel in Fig. 2). In addition, it has been defined intra-domain trust relationships for each one of the domains, considering that the local communication between devices and its platform, and servers is safe (see blue tunnels in Fig. 2).

The TEPANOM protocol defines two phases, a first phase for the authentication with the manufacturer, where the new device must prove to its gateway in the deployment environment that it is a proper device, with a profile, resources, services and quality adequate for the client and manager requirements. and a second phase for the trust extension and registration with the manager/remote monitoring center. The next subsections describe the protocol for each one of the phases.

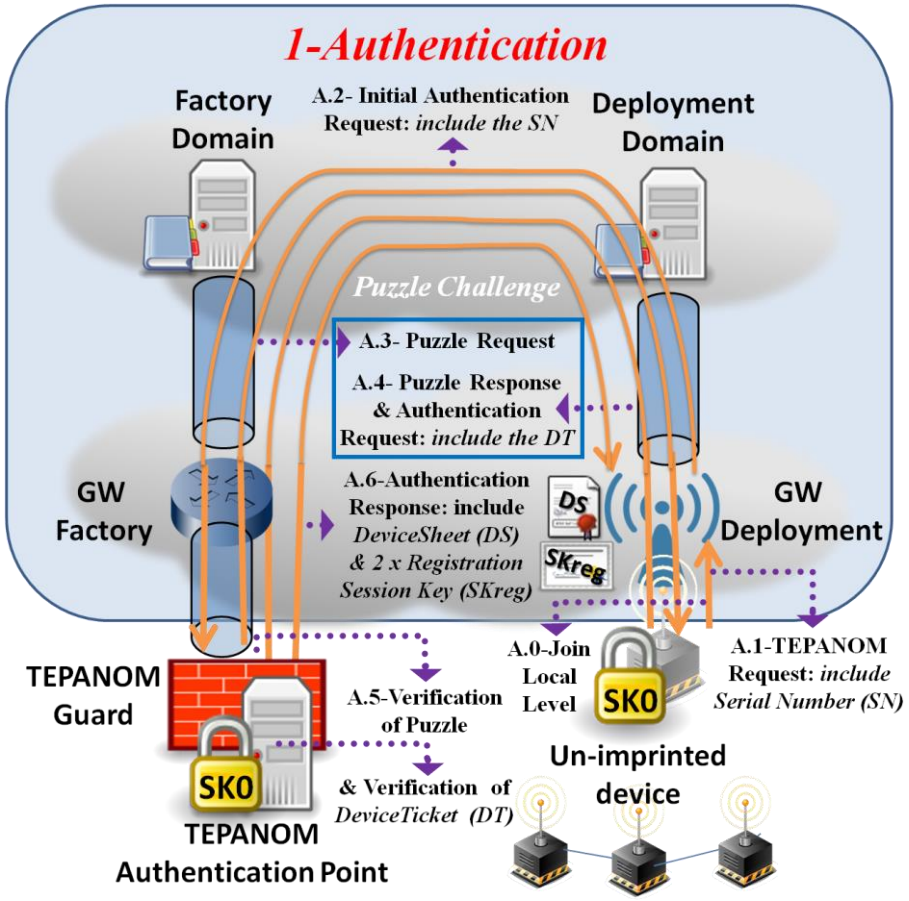

Fig. 3. TEPANOM Authentication Phase.

3.1 Authentication Phase

The authentication of the device and its features is carried out with the services offered by the manufacturer through the manufacturer authentication agent, which has been denominated TEPANOM Authentication Point (TAP). The new device must prove to the TAP that it is the same entity they manufacture, requiring for that goal the use of cryptographic identities defined during the manufacturing phase, it is predefined the Factory Shared Key (SK0) in conjunction with the already defined devices such as MAC and Serial Number.

The authentication is carried out with the Factory domain, where are deployed the TEPANOM Guard and TEPANOM Authentication Point.

The TEPANOM Guard protects of the Denial-of-Service (DoS) attacks to the TEPANOM Authentication Point, since it is one of the most important challenges from the current Internet and Future Internet of Things, where the majority of the deployed protocols in Internet are vulnerable to DoS attacks.

The exchanged messages for the Authentication phase presented in the Fig. 3 are:

A.0) At the beginning the new device joins to the network in a local level.

A.1) Then this starts the TEPANOM protocol sending the TEPANOM Request, this includes the Serial Number, which can be required for the Puzzle election.

DeviceTicket (DT) = {Serial Number | Time Stamp}_SK0

A.2) The gateway of the deployment, which is considered an intelligent platform such as the multiprotocol cards, starts the authentication process with the factory domain, through the Initial Authentication Request message, which includes the Serial Number.

A.3) In the Factory domain, in order to avoid the DoS attacks, it is found the TEPANOM Guard, which asks a puzzle challenge to the new device, in order to verify its real interest and delay the DoS attacks, for example the time for resolving a puzzle by the end node can be a task which takes several seconds. Therefore, it cannot flood the TAP, since it is limited to a query each several seconds. This puzzle can be based on functions such as the found for HIP, which asks to the node look for a number which carrying out a set of calculus with the offered number get a result with a specific properties, e.g. a defined number of zeros in the tail. The puzzle is solved in a period of a few seconds, e.g. between 5 and 300 seconds. This needs to be understood, that it is an operation which is only carried out for the bootstrapping, therefore it is not impacting a high time, and this requires to be heavy and expensive enough, in order to avoid that high performance CPUs can solve it is few milliseconds, which means that they are able to flood the TAP. For that reason, it is looked for a tradeoff between the time required for the sensor node and a high performance CPU. Complexity can be chosen in function of the device capacities, for that reason it is asked the Serial Number, since it could be optionally be used for the Puzzle selection.

A.4) The new device resolves the puzzle and this sends the response with the Authentication Request for the TAP, this includes its credential, i.e. DeviceTicket (DT). DT is a token used for the verification of the new device by the TAP; this includes a timestamp to prevent replay attacks.

DeviceTicket (DT) = {Serial Number | Time Stamp}_SK0

A.5) The TEPANOM Guard and TAP verify the Puzzle and DT respectively.

A.6) In case that the verification is satisfied, TAP sends the DeviceSheet (DS), which includes an extended description of the devices resources, methods and capabilities for its set up in the manager. This also includes the Registration Session Key (SKreg), which is sent in two versions, on the one hand, SKreg and a timestamp protected with SK0, which is sent to the new device in an unprotected medium in the deployment domain, because new device is not sharing any initial secret with the deployment GW, and this initial secret is required for the safe SK1 establishment.

$$\textbf{SKreg\_device} = \{\textbf{SKreg} \mid \textbf{Time Stamp}\}\_\textbf{SK0}$$

On the other hand, SKreg is sent protected with the public key of the deployment GW. Thereby, it cannot be intercepted in the originally unprotected route from the factory domain to the manager domain.

Finally, the deployment GW keeps the DS, SKreg, and SKreg_device, this last until that it is registered in the manager. The technique used for sending SKreg_device is comparable to the technique used to make the ticket in Kerberos, which permits to send SKreg encrypted end-to-end, being forwarded by intermediate nodes which cannot understand it.

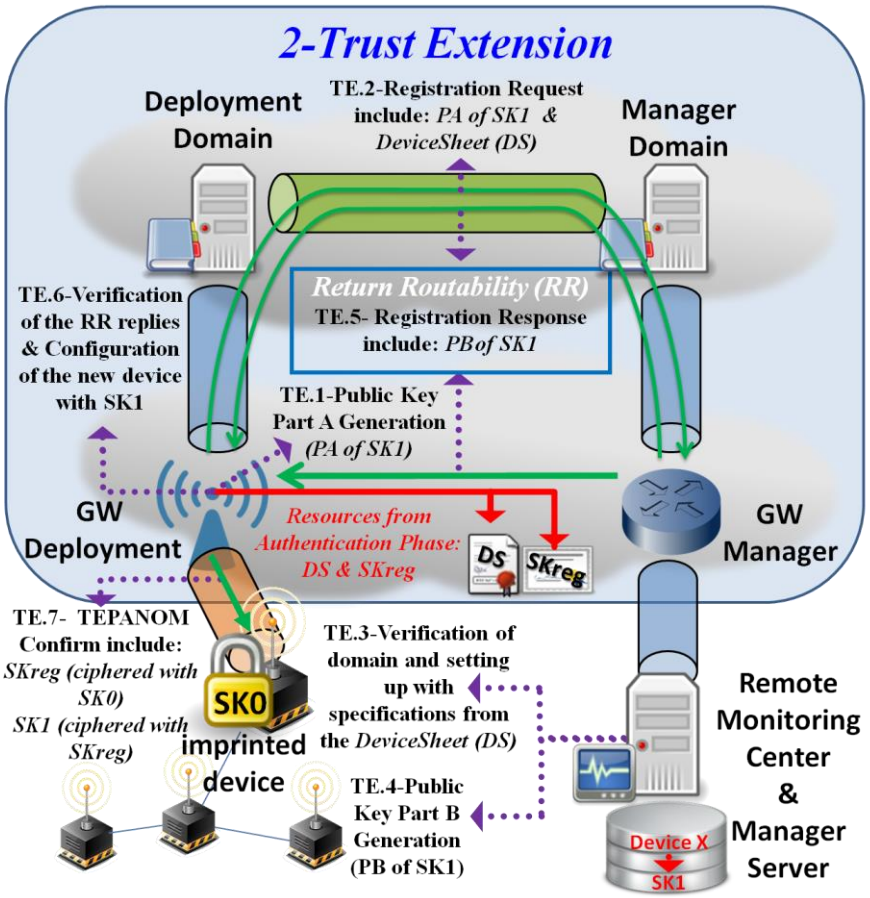

Fig. 3. TEPANOM Trust Extension Phase.

3.2 Trust Extension Phase

The Trust Extension part is composed of the activities for the registration in the manager of the methods and resources from the new device specified in its DS, and the establishment of a new shared key between the manager, deployment domain and new device, which is SK1. For that purpose the deployment GW keeps the SKreg key in its two ciphered versions, and the DeviceSheet (DS) from the Authentication Phase.

The exchanged messages for the Trust Extension phase presented in the Fig. 4 are:

TE.1) At the beginning the deployment GW generates the Part A for the Diffie-Hellman Key exchange of SK1. (nA: private part, and PA: public part), PA=nA*G, where G is the generator of the curve.

TE.2) Then the deployment GW sends to the remote monitoring center the Registration Request with PA and DS.

TE.3) The remote monitoring center verifies the authenticity of DS through the signature included by the TAP, in order to check that it has been really generated by the indicated manufacturer.

TE.4) Generation of the Part B of SK1 (nB: private part, and PB: public part), for the Diffie-Hellman Key exchange, PB=nB*G, and SK1=nA*PB=nB*PA=nA*nB*G. Then this registers SK1 for the indicated device in the manager server.

TE.5) Return Routability Process. Remote Monitoring Center sends the PB through the trust chain defined by the control entities, which has a trust relationship established during the set up of the deployment GW, and this also sends the same message directly through the data plane.

TE.6) The deployment GW verifies through the RR process that there is not an intruder (man-in-the-middle) distorting or blocking the inter-domain communications in the data plane. Then this forms SK1 with the received PB.

TE.7) The deployment GW sends to the new device the TEPANOM confirm, indicating that it has been sucessfuly verified by the TAP in the Factory domain and registred by the remote monitoring center and manage server in the management domain. Finally, this sends SKreg encrypted with SK0, and SK1 encrypted with SKreg. Thereby, it can get SK1 in a secure way, and establish SK1 for its communications with the manager and deployment domain. Thereby, it is extended the trust domain.

3 Conclusions

Internet of Things offers a new dimension of technologies and capabilities for the development of a new generation of solutions to be used in the industry, healthcare, transport, houses and our daily life. This new generation also is presenting several challenges and open problems that need to be investigated. We have focused on, on the one hand, security and privacy for the authentication and protection of those

networks, and on the other hand, management of those networks for configuration, bootstrapping addressing the scalability and security requirements.

There are several significant differences in the management of traditional networks and the defined by the Future Internet of Things. For that reason, it has been proposed a different management architecture, where are considered the found features, requirements and constrains.

Finally, with distributed resource repositories and the required functionalities such as: scalable look up, discovery of "Internet of Things" resources and services, context-awareness, reliability, self-management, self-configuration, self-healing properties.

Acknowledgements

The author would like to thank to the HES-SO and the Institute of Information Systems funding and support, and the European Project "Universal Integration of the Internet of Things through an IPv6-based Service Oriented Architecture enabling heterogeneous components interoperability (IoT6)" from the FP7 with the grant agreement no: 288445.

References

1. Sundmaeker, H.; Guillemin, P.; Friess, P.; Woelfflé, S.; “Vision and Challenges for Realising the Internet of Things”. European cluster CERP-IoT, European Union, ISBN: 978-92-79-15088-3, 2010.
2. Atzori, L.; Iera, A.; Morabito. G.; “The Internet of Things: A survey”. Comput. Netw. Vol. 54, No. 15, pp. 2787-2805, 2010.
3. Rodrigo Roman sobre el impacto de Internet en Smart devices
4. Zamora, M.A.; Santa, J.; Skarmeta, A.F.G.; “An integral and networked Home Automation solution for indoor Ambient Intelligence”, IEEE Pervasive Computing, Vol. 9, pp. 66--77, 2010.
5. Kafle, V.P.; Otsuki, H.; Inoue, M.; "An ID/locator split architecture for future networks", Communications Magazine, IEEE, vol. 48, No. 2, pp. 138-144, 2010.
6. Koponen, T.; Chawla, M.; Chun, B.-G.; Ermolinskiy, A.; Kim, K.H.; Shenker, S.; Stoica, I.; “A data-oriented (and beyond) network architecture”, SIGCOMM Comput. Commun. Rev. 37, 4 pp. 181-192, 2007.
7. Mukhtar, H.; Kim Kang-Myo; Chaudhry, S.A.; Akbar, A.H.; Kim Ki-Hyung; Seung-Wha Yoo; , "LNMP- Management architecture for IPv6 based low-power wireless Personal Area Networks (6LoWPAN)," Network Operations and Management Symposium, 2008. NOMS 2008. IEEE , vol., no., pp.417-424, 7-11 April 2008. doi: 10.1109/NOMS.2008.4575163
8. Schonwalder, J.; Fouquet, M.; Rodosek, G.; Hochstatter, I.; , "Future Internet = content + services + management," Communications Magazine, IEEE , vol.47, no.7, pp.27-33, July 2009 doi: 10.1109/MCOM.2009.5183469
9. Ruiz, L.B.; Nogueira, J.M.; Loureiro, A.A.F.; , "MANNA: a management architecture for wireless sensor networks," Communications Magazine, IEEE , vol.41, no.2, pp. 116- 125, Feb 2003 doi: 10.1109/MCOM.2003.1179560
10. Rodrigo Roman, Cristina Alcaraz, Javier Lopez, Nicolas Sklavos, Key management systems for sensor networks in the context of the Internet of Things, Computers & Electrical Engineering, Volume 37, Issue 2, Modern Trends in Applied Security: Architectures, Implementations and Applications, March 2011, Pages 147-159, ISSN 0045-7906, DOI: 10.1016/j.compeleceng.2011.01.009.

11. Jara, A. J.; Zamora, M.A.; Skarmeta, A.F.G.; “An internet of things–based personal device for diabetes therapy management in ambient assisted living (AAL)”, to be published in: Personal and Ubiquitous Computing, DOI: 10.1007/s00779-010-0353-1, “in press”, 2011.
12. Papadimitriou, D.; Tschofenig, H.; Rosas, A.; Zahariadis, S.; et al; “Fundamental Limitations of Current Internet and the path to Future Internet, European Commission”, FIArch Group, Ver. 1.9, 2010.
13. Zorzi, M.; Gluhak, A.; Lange, S.; Bassi, A.; "From today's INTRAnet of things to a future INTERnet of things: a wireless- and mobility-related view", Wireless Communications, IEEE , vol.17, no.6, pp.44-51, 2010.
14. Personal Networks: Wireless Networking for Personal Devices Martin Jacobsson, Ignas Niemegeers, Sonia Heemstra de Groot ISBN: 978-0-470-68173-2 June 2010, Wiley