ISSN (e): 2250 – 3005 || Volume, 07 || Issue, 12 || December – 2017 ||
International Journal of Computational Engineering Research (IJCER)

IoT implementation using secure communication protocols

KhurramNaim Shamsi[1], Dr.Mohammad Mazhar Afzal[2]
Department of Computer Science and Engineering, Glocal University Saharanpur, UP, India
Corresponding Author: KhurramNaim Shamsi

ABSTRACT
The Internet of Things (IoT) integrates a large number of physical objects that are uniquely identified, ubiquitously interconnected and accessible through the Internet. IoT aims to transform any object in the real-world into a computing device that has sensing, communication and control capabilities. There is a growing number of IoT devices and applications and this leads to an increase in the number and complexity of malicious attacks. It is important to protect IoT systems against malicious attacks, especially to prevent attackers from obtaining control over the devices. The common standard Internet security protocols are recognized as unsuitable in these type of networks, particularly due to some classes of IoT devices with constrained resources. This research discusses the applicability and limitations of existing IP-based Internet security protocols and other security protocols used in wireless sensor networks, which are potentially suitable in the context of IoT. The analysis of these protocols is discussed based on a classification focusing on the key distribution mechanism.

Keywords: Security, Scalability, Interoperability, Key management, Internet of Things, Wireless sensor network, Cryptographic primitives, Standard, Mobility, Integrity, Confidentiality, Availability.

Date of Submission: 19-12-2017 Date of acceptance: 09-01-2018

I. INTRODUCTION

The Internet of Things (IoT) is defined as a network of connected devices (things). In today’s perspective, the IoT includes various kinds of devices, e.g., sensors, actuators, RFID tags, smartphones or backend servers, which are very different in terms of size, capability and functionality. The key challenge is how to adapt such network functioning in the conventional Internet. Inspired by that motivation, recent research efforts focus on the design, application and adaptation of standard Internet protocols in the IoT.

The initiative of 6LoWPAN [1] working group allowed the small devices with limited processing capabilities to become part of the Internet by enabling the use of IPover these devices. Such great feature enables the connection of literally billions of devices to the Internet, in which very different things such as a humidity sensor or an RFID tag can communicate with each other, with a human carrying a smartphone, or with a remote backend server.

While the concept of IoT is easy to grasp, major research efforts still need to be made. Various aspects of IoT are currently being discussed, such as IoT applications and architectures. In addition, more and more research efforts are initiated in resolving challenges associated with security, privacy, and trust as IoT devices are increasingly deployed. According to Gartner’s forecast [2], the IoT, which excludes PCs, smartphones and tablets, will grow to more than 26 billion units installed in 2020. Allowing each single physical object to connect to the Internet and to share information, may create more threats than ever for our personal data and business secret information. Concerned objects cover our everyday friendly devices, such as, thermostats, fridges, ovens, washing machines, and TV sets. It is easy to imagine how bad it would be, if these devices were spying on us and revealing our personal information. As an example, a major cyber-attack campaign observed by Proof point’s researchers [3] in January 2014, proved that even a harmless fridge can be employed to launch security attacks. Their analysis shows that 25 percent of malicious emails from the cyber-attack between December 23, 2013 and January 2014 (over 750,000 messages), came from ‘‘smart’’ things, including home appliances (TVs, refrigerators...). It would be even worse if critical IoT applications, for instance, the control system in nuclear reactors, the vehicle safety system or the remote monitoring in healthcare, were compromised.

By means of IP protocols crafted for the IoT, an IoT device is able to directly interact with other Internet entities located far beyond its local network. In a typical WSN, devices should be properly authenticated in the network based on a set of credentials stored in a secure area. The security solutions generally deployed within the network are poorly defined to protect communications within the network premises and not between external entities. To provide end-to-end security, the potential adaptations of several standard security protocols have been studied in [4] such as IKE/IPsec, TLS, DTLS, and HIP-DEX, but certain issues continue to persist using these solutions. In particular, resource limitations and the large volume of IoT devices deployed in a network hamper the application of Internet standard solutions.

According to the authors in [5], several new issues brought by IoT need to be addressed, such as secure booting, firewalling and secure updating and patching. For example, we need to ensure that only authorized and authenticated software are loaded into the embedded device, for example, by verifying a digital signature attached to the software image. As stated in a recently HP security report [1], almost 60 percent of smart devices are not using encryption while downloading software updates. In order to deploy security solutions to this problem, devices are required not only to use cryptographic algorithms to perform encryption, but also to share the necessary keys required by these algorithms, which is an even worse issue considering the foreseen large deployment and the general resource limitations of these devices.

The main motivation of this research is to identify security issues associated with IoT, and to demonstrate the limitations of existing security solutions to fulfill these issues. The reviewed solutions are analyzed and compared.

II. RELATED SURVEYS AND POSITIONING

There have been several conducted studies and surveys that are relevant to the security in the IoT. For instance, Wang et al. [6] gave a very detailed survey of security issues in wireless sensor networks, which can be considered as a reference for the IoT. The authors identified the constraints and the requirements based on the existing attacks against the IoT at different layers. They also presented the key management systems in WSN according to the employed cryptographic primitives. Atzori et al. [7] focused on authentication, data integrity and privacy issues in the IoT, particularly in RFID systems and sensor networks. Kumar et al. [8] gave a general overview of security and privacy issues in IoT. They provided a description of different security threats and privacy concerns while processing, storing, and transmitting data. The main line of the existing surveys in relation with the IoT security is that they generally focus on identifying the challenges and the security threats present in the IoT. However, several security solutions and techniques have already been proposed since the advent of the IoT. For this reason, the present research takes a different direction by looking in depth into these security protocols and techniques. Indeed, we will not focus on specific security properties needed for the IoT. We will look closer at the security protocol itself, how it is constructed, which security properties are provided, and which cryptographic primitives are used. Moreover, the research proposes a new classification of key establishment mechanisms in the context of IoT that allows to better understand the proposed security approaches. In this way, strong and weak features of existing approaches can be identified with the objective to build secure protocols for the IoT.

The contributions of this document are threefold:

- Present an overview of the challenges and the requirements to build a secure IoT;
- Provide a classification of different security protocols proposed for WSN and IoT with respect to the employed key bootstrapping mechanism; and
- Finally, provide a review of ongoing research initiatives in the field of security in the IoT.

III. IOT SECURITY OVERVIEW

The IoT offers connectivity for both human-to-machine and machine-to-machine communications. In the near future, everything is likely to be equipped with small embedded devices which are able to connect to the Internet. Such ability is useful for various domains in our daily life: i.e. from building automation, smart city, and surveillance system to all wearable smart devices. However, the more the IoT devices are deployed, the greater our information system is at risk. Indeed, a non-negligible number of devices in IoT are vulnerable to security attacks, for example, denial of service and replay attacks, due to their constrained resources and the lack of protection methods. This kind of attacks lead to sensor battery depletion and results in poor performances of sensing applications. In more serious cases, information leak from such tiny devices can expose sensitive data to the outside. In this section, we summarize the challenges to be addressed in the IoT.

Scalability

There are billions of interconnected IoT devices that generate huge amount of data for processing and storage [9]. The IoT system that handles these devices should be scalable. The large amount of data generated by the current system is stored using the Big Data over Cloud.

Interoperability

There are several different manufacturers who provide different products, services and devices being used in the IoT systems. Unfortunately, they do not follow any standard protocols for the manufacturing and use of these devices. This becomes a major cause for the interoperability issues [10]. The existence of a large number of diverse devices and management of value added services are the key standardization issues at present.

Security

Several people continuously wear medical sensor-based devices to keep track of their medical statistics. In such scenarios, security becomes vital as any breach into it may prove to be critically life threatening [11]. Hence, the security of the information obtained by different sensors and devices in an IoT network becomes indispensable. Proper policies and technical security measures are essential to enable data sharing among authorized users and organisations [12]. Different characteristics such as confidentiality, Integrity and availability of people's personal data should be guaranteed in an IoT system. Along with these, efficient security of resources is another key requirement. The IoT based systems should be equipped with fool proof mechanisms that utilize minimum resources with maximum security performance.

Physical security

The devices used in the IoT system should have tampered resistant packaging [12]. It is possible that the attacker takes control of the device and alter it to obtain crucial data. Additionally, the routing algorithms used should be properly controlled in order to safeguard the transmitted data. The network nodes are always susceptible to attacks. Hence, there is a strong need for transmission of data by using secure routing protocols [13]. The IoT medical devices are equipped with procedures to access the cloud services [11]. The services should be properly monitored so that the patient's data can easily be tracked and controlled.

Mobility

It is a basic requirement for an IoT based system to permit mobility of devices so that the system is always functional, irrespective of the location. This feature makes it possible to connect heterogeneous environments [13].

Network Type

Sometimes, selection of a proper network becomes an issue. There are mainly three types of networks: data centric, service centric and user centric. The data centric network categorizes the IoT structure on the basis of captured data [14]. The service centric structure is based on the structures formed by assembly of services being provided by the system. The user centric structure is created by using the structure formed by the involvement of people in the system.

Classification of security protocols for the IoT

The life cycle of a ''thing'' is composed of three phases (as denoted in [4]): bootstrapping, operational and maintenance phases. The bootstrapping phase refers to any processing tasks required before the network can operate. Sarikaya et al. [15] also define that this process involves a number of settings to be transferred between nodes that shared no prior knowledge of each other. The bootstrapping step of a device is complete when all security parameters (e.g., secret keys) are securely transferred to the device. This study focuses on recent security solutions proposed for a secure bootstrapping process. The terms and definitions used throughout the rest of the document are presented in Table 1.

Abbreviations and notations.

Abbreviation	Definition
IoT	Internet of Things
WSN	Wireless Sensor Network
PKC	Public Key Cryptography
KDC	Key Distribution Center
6LBR	6LoWPAN Border Router
PKG	Private Key Generator
DH	Diffie–Hellman exchange
IBE	Identity-based Encryption
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie–Hellman exchange

Table 1

In this section, we first describe the reference model that illustrates the scenario in which the considered security protocols can be deployed. We then present, in Section 4.2, our classification of the security protocols based on the key bootstrapping mechanism.

Scenario under consideration

The security protocols analyzed in this document, as illustrated in Figure 1, involve two entities. At least one of them is a device with resource constraints, whereas the second entity can be seen as another constrained device or an external Internet server (i.e., with rich resources). The considered network of ‘‘things’’ consists of a number of tiny nodes communicating with each other and with an unconstrained resource border router (6LBR). The 6LBR is the bridge between the sensor node and the outside world. The 6LBR may take part in the communication between two entities in a passive (transparent to the communicating parties) or active (as a mediator in the communication process) manners.

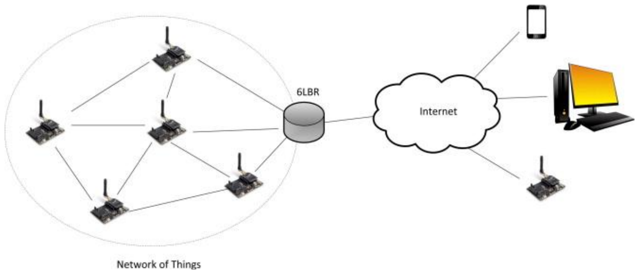

Figure 1: Network architecture of our scenario.

Classification

In this document, existing security solutions for IoT is categorized into two main types: solutions that rely on asymmetric key schemes and solutions that pre-distribute symmetric keys to bootstrap a secure communication. This section describes the first two levels of the proposed classification.

Asymmetric key schemes (AKSs)

The key schemes based on asymmetric cryptography, also known as Public-key cryptography (PKC) are considered as a very common approach to establish a secure communication between two (or more) parties. They employ asymmetric algorithms and are widely deployed in the conventional Internet. The applicability of AKSs in the IoT has one major inconvenience, which is the computation cost and energy consumption. Despite of expensive operations, a lot of researches still seek to apply AKSs in the context of IoT. The proposed approaches can be classified into two categories: *key transport based on public key encryption* and *key agreement* based on asymmetric techniques.
*Key transport based on public key encryption:*Similarly, to the traditional key transport mechanism, the first category requires from the public key to securely transport information. Various key establishment techniques have been proposed for IoT, ranging from raw public key usage to complex implementations in X.509 standard.

*Key agreement based on asymmetric techniques:*The second category is based on asymmetric primitives in which a shared secret is derived among two or more parties. In this category, we notice obviously the DH protocol [16] and its variants.

Symmetric key pre-distribution schemes

In addition to asymmetric approaches, researchers also propose multiple techniques using symmetric key establishment mechanisms to bootstrap secure communication in the IoT. Symmetric approaches often assume that nodes involved in the key establishment share common credentials. The pre-shared credentials might be a symmetric key or some random bytes flashed into the sensor before its deployment. This category can be divided into two main sub-categories:

Probabilistic key distribution: This sub-category concerns the mechanisms that distribute security credentials (keys, random bytes) chosen randomly from a key pool to constrained nodes. During their initial communication, each two nodes may discover a common key, with certain probability, to establish a secure communication.

Deterministic key distribution: In this sub-category, a deterministic design is applied to create the key pool and to distribute uniformly the keys such that each two nodes share a common key. Figure 2 summarizes our classification. Each class of the security solutions provides its own advantages and disadvantages.

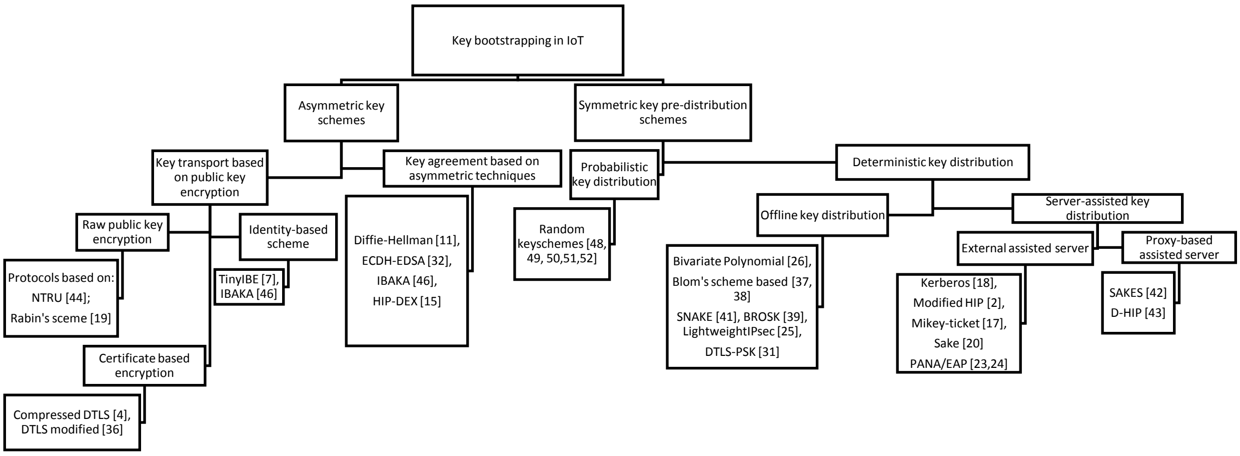
Key bootstrapping in IoT
Asymmetric key schemes
Symmetric key pre-distribution schemes
Key transport based on public key encryption
Key agreement based on asymmetric techniques
Probabilistic key distribution
Deterministic key distribution
Raw public key encryption
Identity-based scheme
Protocols based on: NTRU [44]; Rabin's sceme [19]
TinyIBE [7], IBAKA [46]
Certificate based encryption
Compressed DTLS [4], DTLS modified [36]
Diffie-Hellman [11], ECDH-EDSA [32], IBAKA [46], HIP-DEX [15]
Random keyschemes [48, 49, 50,51,52]
Offline key distribution
Server-assisted key distribution
External assisted server
Proxy-based assisted server
Bivariate Polynomial [26], Blom's scheme based [37, 38] SNAKE [41], BROSK [39], LightweightIPsec [25], DTLS-PSK [31]
Kerberos [18], Modified HIP [2], Mikey-ticket [17], Sake [20] PANA/EAP [23,24]
SAKES [42] D-HIP [43]

Figure 2: Classification of key bootstrapping mechanisms in IoT.

IV. RELATED WORK IN IOT SECURITY PROTOCOL CLASSIFICATION

Classification approaches have been proposed in several works [17,18,19,6]. In [17], the authors propose several ways to classify key establishment approaches, for instance based on the employed authentication method or the underlying cryptographic primitive. Camtepe and Yener [18] give a detailed classification of symmetric key distribution protocols for two different scenarios: distributed and hierarchical WSNs. In each scenario, the authors analyze diverse mechanisms to establish pair-wise and group-wise keys between sensor nodes. Similarly, Wang et al. [6] propose a classification of symmetric key management protocols in WSN, but based on the network structure and the probability of key sharing between a pair of sensor nodes. Their works at a very first level differentiate centralized and distributed key schemes. At a second level, they provide other differentiation based on the probabilistic and deterministic key establishment mechanisms. Roman et al. [19] give a high level classification based on the key management systems(KMS), namely: key pool framework, mathematical framework, negotiation framework and public key framework. They conclude that public key cryptography can be a viable solution for sensor nodes that run as client nodes (in the model client–server). For server nodes, mathematicalbased KMS, such as polynomial scheme, provide better performances. The aforementioned approaches do not sufficiently cover possible key distribution mechanisms (asymmetric and symmetric methods), for example, only symmetric approaches are studied in [18,6]. Besides, they provide heterogeneous classifications due to unrelated different criteria, as in [19,6].

By taking into account the classifications described above, especially in [17], our classification covers asymmetric key distribution mechanisms for IoT, in addition to symmetric approaches. The classification is marking out different protocols by the key establishment scheme used to establish a secret session key: asymmetric or symmetric techniques. As mentioned in Section 4.1, we do not consider protocols that establish group-wise keys between sensor nodes [18]. Only pair-wise key establishments are considered in this research paper. Our classification has a high classification degree leading to a more in depth protocol evaluation. For instance, in the asymmetric approach, we do not only discuss on the applicability of public key cryptography in the context of IoT, as described in [19], but we also differentiate different asymmetric key schemes based on the key delivery scheme (key transport or key agreement). In symmetric key pre-distribution schemes, we organize the existing securityprotocols into two categories: probabilistic and deterministic key distribution. These categories have also been mentioned in [18,6]. However, in the deterministic approach, we go further by distinguishing protocols that have server(s) participating in the key negotiation process from protocols that do not depend on any third party during key establishment phase.

V. OVERVIEW OF RECENT TRENDS IN IOT SECURITY PROTOCOLS

There are some new approaches being pushed by researchers. They always keep their interest in both asymmetric and symmetric approaches.Even if the symmetric paradigm is considered to be more energy efficient, the asymmetric solutions are still preferable because of their deployment facility, flexibility and scalability in terms of key management. Besides, the public key paradigm allows two entities without any prior-trust relationship with each other, establishing a secure channel, which is generally an important feature in real time scenarios.

The following points need to be highlighted before designing an efficient security protocol for constrained devices in IoT:

Optimizing asymmetric solutions

The asymmetric approaches are generally energy-consuming. The first ambition is to reduce the required computation time in order to save energy for sensor nodes. One can think about adapting directly NTRU to the standard protocols because it is currently the most energy-efficient primitive. However, this primitive requires more memory space for keying materials than other asymmetric primitives. Some researchers are working on optimizing mathematical mechanisms used in cryptographic algorithms, i.e. Marin et al. [20] discuss a solution to optimize the ECC primitives. They propose an optimization for the modular multiplication operation. The solution is evaluated in the widelyused microprocessor MSP430. The authors claimed that the optimization is presenting the lowest time and number of required operations for ECC multiplication. Another method to reduce the energy consumption on sensor nodes relies on pre-computation techniques. It helps diminishing the cost of modular exponentiations in several signature and key management schemes, such as ECDSA or Diffie–Hellman key exchange. The idea is to store a set of n Discrete Log pairs in the form (ai; gai mod q). Then, a ‘‘random’’ pair ðr; gr mod qÞ is generated from a subset of k pairs chosen randomly in the memory. The technique seems simple, but it requires the value of n to be sufficiently large in order to ensure the randomness of the generated pairs ðr; gr mod qÞ. Ateniese et al. [21] improve the pre-computation techniques above and apply it to ECDSA. They show that the almost 50% of energy is saved with ECDSA with pre-computation compared to the original signature scheme and also to the NTRUsign signature scheme (which is considered to be a natural candidate in low-power devices).

On the other hand, several researches adapt the properties of asymmetric primitives in an optimized manner to fit in the most constrained environment of IoT. Effectively, Moustaine and Laurent [22] propose an efficient authentication protocol for low-cost RFID systems based on an adaption of NTRU. This adaption first delegates the complex operations of NTRU (i.e. modular arithmetic, polynomial multiplication) to the server. Secondly, the tags require only additions and circular shifts to encrypt the challenges during the authentication phase. Besides, the protocol is resistant against classical attacks including replays, tracking and man in the middle attacks with very low requirements for computation.

As another asymmetric technique, Zero-knowledge proofs (ZKP) [23,24] is also a candidate for future proposals in IoT. ZKP are interactive proof systems involving two entities: a prover and a verifier. The prover demonstrates the knowledge of a secret to the verifier without revealing a single bit about the secret. ZKP relies on some hard mathematical problems, such as the factorization of integers, i.e. [23] or the discrete logarithm problem (DLP) [24]. This mechanism is commonly used in WSN for node authentication. For example, the authors in [24] provide an efficient authentication scheme based on DLP over elliptic curve groups. The scheme requires only three messages between the prover and verifier. ZKP has advantages in terms of the amount of messages being sent and the memory usage on nodes as also mentioned in [23,24]. One can benefit ZKP to propose an efficient key bootstrapping protocol in IoT with the node authentication provided by ZKP.

Tailoring the existing standard protocols to IoT

Standard security protocols can be adapted to work in constrained and heterogeneous environments of IoT. As described in this research, many attempts have been done to adapt and apply standard protocols in the context of IoT, for example, DTLS [25,26], IPsec [27], IKEv2 [28], HIPDEX [29,30,31]. As another example, Kivinen [32] propose a minimum implementation of standard IKE [33] by removing the requirement for certificates. This minimum variant defines only two message exchanges for key negotiation and provides entity authentications using pre-shared key approach. On the other hand, Migault et al. [34] suppose that the security associations between entities are established using existing mechanism like IKEv2. They are interested in the security of packet transmissions by proposing Diet-ESP – an adaptation of ESP (Encapsulation Security Protocol) to IoT in order to compress and reduce the ESP overhead. The authors define mechanisms to remove or reduce some ‘‘unnecessary’’ or ‘‘larger than required’’ ESP fields for the specific needs or applications of IoT devices. However, the deployment of Diet-ESP has to keep the trade-off between the security requirements and the battery life time of constrained devices. Indeed, as depicted by the authors, small SPI (Security Parameters Index) size, small size of ICV (Integrity Check Value) and removing SN (Sequence Number) expose the devices to respectively Denial of Service, spoofing and replay attacks.

Using hybrid approaches

Another trend consists of combining the advantages of both symmetric and asymmetric solutions. Meca et al. [29] choose HIP-DEX (an asymmetric technique) [30] to provide access to a local sensor network. A mobile node is authenticated with help of a central server. If the authentication is successful, the server sends securely the necessary parameters for the mobile node by encrypting the data with the session key generated after the DH exchanges. These parameters are actually a bivariate polynomial used to bootstrap secure communications with a local node (a symmetric technique). The pairwise key generated by the shared polynomial is employed as a master key to generate multiple session keys for specific purposes.

The presence of a third party in such hybrid approach becomes essential in the IoT. Firstly, the rich-resource server is expected to support almost all heavyweight computations. As such, the sensor nodes with limited energy and capabilities are no longer involved in this expensive process as described in [35,36]. The constrained node can establish a communication with external hosts without implementing the full asymmetric process. Additionally, the assisted servers are capable to provide fine-grained access control such that only authorized actions are executed on sensor nodes.

VI. CONCLUSION

This paper considered several secure, lightweight and attack-resistant solutions for WSNs and IoT based on identified security requirements and challenges. We also provided a novel classification of existing protocols relying on their key bootstrapping approach to establish a secure communication channel. These protocols and techniques are analyzed according to different criteria in order to identify the advantages and drawbacks of each protocol.

Using this methodology, we noted that symmetric approaches are not anymore the default choice for IoT. Public key cryptography is likely to be more recommended in the IoT context, provided that the associated asymmetric techniques are properly optimized. A trusted third party will also certainly take a more active role to secure the IoT and to adapt to its heterogeneous nature. Additionally, security protocols should take into account the resource-constrained feature of things. Heavyweight cryptographic operations i.e. based on RSA and Diffie–Hellman agreement protocols should be replaced by lightweight operations, i.e. using symmetric cryptography or applying more lightweight asymmetric primitives such as ECC and NTRU. Besides, lightweight security protocols are also needed to reduce the communication complexity. Aside from performance concerns, the proposed security solutions will offer perspectives on new applications that increasingly expand the coverage of capabilities and features offered by IoT devices making them more and more intelligent.

REFERENCES

[1]. HP report on Internet ofThings Research Study, 2014 <http://fortifyprotect.com/HP_IoT_Research_Study.pdf>.

[2]. Gartner Inc., Forecast: The Internet of Things, Worldwide, 2013.

[3]. Proofpoint, Article Proofpoint Uncovers Internet of Things (IoT) Cyberattack. <http://www.proofpoint.com/about-us/press-releases/01162014.php> (accessed September 2014).

[4]. O. Garcia-Morchon, S. Kumar, Security Consideration in the IP-based Internet of Things, CoRE, Internet-draft, 2013.

[5]. W. River, White Paper, Security in the Internet of Things, 2014. <http://www.windriver.com/whitepapers/security-in-the-internetof-things/wr_security-in-the-internet-of-things.pdf>.

[6]. Y. Wang, G. Attebury, B. Ramamurthy, A survey of security issues in wireless sensor networks, IEEE Commun. Surv. Tutorials 8 (2)(2006).

[7]. L. Atzori, A. Iera, G. Morabito, The Internet of things: a survey, Comput. Netw. 54 (15) (2010) 2787–2805.

[8]. J.S. Kumar, D.R. Patel, A survey on Internet of things: security and privacy issues, Int. J. Comput. Appl. 90 (11) (2014) 20–26.

[9]. DATTA, S. K., BONNET, C., GYRARD, A., COSTA, R. P. F. D. & BOUDAOUD, K. 2015. Applying Internet of Things for personalized healthcare in smart homes. 24th Wireless and Optical Communication Conference (WOCC). Taipei, Taiwan: IEEE.

[10]. SIVAGAMI, S., REVATHY, D. & NITHYABHARATHI, L. 2016. Smart Health Care System Implemented Using IoT. International Journal of Contemporary Research in Computer Science and Technology 2.

[11]. SAMUEL, R. E. & CONNOLLY, D. 2015. Internet of things-based health monitoring and management domain-specific architecture pattern. Issues in Information Systems, 16, 58-63.

[12]. RAHMANI, A.-M., THANIGAIVELAN, N. K., GIA, T. N., GRANADOS, J., NEGAS, B., LILJEBERG, P. & TENHUNEN, H. 2015. Smart e-Health Gateway: Bringing intelligence to Internet-of-Things based ubiquitous healthcare systems. 12th Annual IEEE Consumer Communications and Networking Conference (CCNC). NV, USA: IEEE

[13]. AGRAWAL, S. & VIEIRA, D. 2013. A survey on Internet of Things. Abakós, Belo Horizonte, 1, 78 – 95.

[14]. RIGGINS, F. J. & WAMBA, S. F. 2015. Research Directions on the Adoption, Usage, and Impact of the Internet of Things through the Use of Big Data Analytics. 48th Hawaii International Conference on System Sciences. HI, USA.

[15]. B. Sarikaya, Y. Ohba, et al., Security Bootstrapping Solutions for Resource-Constrained Devices, Internet-draft, 2012.

[16]. E. Rescorla, Diffie–Hellman Key Agreement Method, IETF, RFC 2631, 1999.

[17]. Thesis:CollaborativeSecurityfortheInternet ofThings, YosraBenSaied. <http://www.theses.fr/2013TELE0013> (accessed November 2013).

[18]. S. A. Camtepe, B. Yener, Key Distribution Mechanisms for Wireless Sensor Networks: A Survey, Technical Report TR-05-07, Rensselaer Polytechnic Institute, 2005.

[19]. R. Roman, C. Alcaraz, et al., Key management systems for sensor networks in the context of the Internet of things, Int. J. Comput. Electr. Eng. (2011) 147–159.

[20]. L. Marin, A. Jara, et al., Shifting primes: optimizing elliptic curve cryptography for smart things, in: 6th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), 2012.

[21]. G. Ateniese, G. Bianchi, et al., Low-cost Standard Signature in Wireless Sensor Networks: A Case for Reviving Pre-Computation Techniques, Usenix Network and Distributed System Security Symposium (NDSS), 2013.

[22]. E. Moustaine, M. Laurent, A lattice based authentication for low-cost RFID, in: IEEE International Conference on RFID-Technologies and Applications (RFID-TA), 2012.

[23]. I. Chatzigiannakis, A. Pyrgelis, et al., Elliptic curve based zero knowledge proofs and their applicability on resource constrained devices, in: 8th IEEE Conference on Mobile Ad-Hoc and Sensor Systems, 2011.

[24]. U. Feige, A. Fiat, A. Shamir, Zero-knowledge proofs of identity, J. Cryptogr. 1 (2) (1988).

[25]. S. Raza, H. Shafagh, et al., Lithe: lightweight secure CoAPs for the Internet of things, IEEE Sens. J. 13 (10) (2013).

[26]. R. Hummen, Jan H. Ziegeldorf, et al., Towards viable certificate-based authentication for the Internet of things, in: Proceedings of the 2nd ACM Workshop on Hot Topics on Wireless Network Security and Privacy (HotWiSec'13), 2013.

[27]. S. Raza, S. Duquennoy, T. Chung, et al., Securing communication in 6LoWPAN with compressed IPsec, in: International Conference on Distributed Computing in Sensor Systems and Workshop, 2011.

[28]. S. Ray, G.P. Biswas, Establishment of ECC-based initial secrecy usable for IKE implementation, in: Proc. of World Congress on Expert Systems (WCE), 2012.

[29]. F. Meca, J. Ziegeldorf, et al., HIP security architecture for the IP-based Internet of thing, in: 27th International Conference on Advanced InformationNetworkingandApplicationsWorkshops (WAINA),2013.

[30]. R. Moskowitz, HIP Diet EXchange (DEX), IETF, draft-moskowitz-hiprg-dex-06, 2012.

[31]. R. Moskowitz, P. Jokela, et al., Host Identity Protocol version 2 (HIPv2), Draft-Internet, 2013.

[32]. T. Kivinen, Minimal IKEv2, Draft-Internet, 2011.

[33]. C. Kaufman, Internet Key Exchange (IKEv2) Protocol, IETF, RFC 4306, 2005.

[34]. D. Migault, T. Guggemos, D. Palomares, Diet-ESP: A Flexible and Compressed Format for IPsec/ESP, Draft-Internet, January 2014.

[35]. H.R. Hussen, G.A. Tizazu, et al., SAKES: secure authentication and key establishment scheme for M2M communication in the IP-based wireless sensor network (6LoWPAN), in: 5th International Conference on Ubiquitous and Future Networks (ICUFN), 2013.

[36]. Y.B. Saied, A. Olivereau, D-HIP: a distributed key exchange scheme for HIP-based Internet of things, in: First IEEE WoWMoM Workshop on the Internet of Things: Smart Objects and Services (IoT-SoS), 2012.

International Journal of Computational Engineering Research (IJCER) is UGC approved Journal with Sl. No. 4627, Journal no. 47631.

KhurramNaim Shamsi "IoT implementation using secure communication protocols." IInternational Journal of Computational Engineering Research (IJCER), vol. 7, no. 12, 2017, pp. 36-43.