International Journal of Advanced Research in Engineering and Technology (IJARET)
Volume 11, Issue 12, December 2020, pp. 621-627, Article ID: IJARET_11_12_065
Available online at http://www.iaeme.com/ijaret/issues.asp?JType=IJARET&VType=11&IType=12
ISSN Print: 0976-6480 and ISSN Online: 0976-6499
DOI: 10.34218/IJARET.11.12.2020.065

ANALYSIS OF LIGHT WEIGHT SMART AUTHENTICATION PROTOCOL SCHEMES FOR EFFECTIVE COMMUNICATION IN SMART ENVIRONMENT

T. Charan Singh
Assistant Professor, KMIT, Hyderabad, Telangana, India

S. Naveen Kumar
Assistant Professor, KMIT, Hyderabad, Telangana, India

Dr. P. Pavankumar
Assistant Professor, KMIT, Hyderabad, Telangana, India

ABSTRACT

Smart home IoT networks have been recognized as one of the common and part of daily life in coming 5G era. Internet of Things (IoT) sensors are used in daily routine by the users to control the home services through remote access anywhere anytime. Without being protected, network management can cause smart home networks to be vulnerable to various security threats. It is so important to protect data traffic transmitted between user mobile devices and their in-home IoT appliances because they include users' sensitive and critical privacy information. To overcome this problem a new method is proposed known as Lightweight and Robust mutual-authentication scheme (LRMA) for protecting distributed smart environments from unauthorized abuses.

In smart environment between smart devices uses implicit certificates and enables mutual authentication and key agreement. Computation and communication complexities are reduced to obtain efficiency and various attacks are resists to LRMA. Moreover, both security analysis and performance evaluation prove the effectiveness of LRMA as compared to the state of the art schemes.

Keywords: Security, Authentication, IoT, Elliptic Curve Qu-Vanstone (ECQV), implicit certificate.

Cite this Article: T. Charan Singh, S. Naveen Kumar and P. Pavankumar, Analysis of Light Weight Smart Authentication Protocol Schemes for Effective Communication in Smart Environment. *International Journal of Advanced Research in Engineering and Technology*, 11(12), 2020, pp. 621-627.
http://www.iaeme.com/IJARET/issues.asp?JType=IJARET&VType=11&IType=12

1. INTRODUCTION

A smart environment is one of the emerging trends that allow people and objects to stay connected via the information and communication technologies. Smart environments (also known as Internet of Things (IoT)) include smart homes [1], smart healthcare [2], Smart car and cities [3] and many more. Note that smart environments/objects and IoT applications/objects are interchanged throughout the paper. In a recent research report, it is estimated that the "things" in connected smart environments to grow tremendously and is anticipated to reach up to billions of devices by 2025 [4].

In smart environment, IoT objects are computationally constraint devices, such as sensors, that can sense, compute, and extend connectivity between the last miles systems and users via the Internet in a ubiquitous manner. Fig. 1 shows a typical network of distributed smart environments, where several heterogeneous objects/nodes are installed to control and monitor the applications through the IoT cloud. All the sensors, objects or nodes collect data within their respective environments and send it to the cloud via the networking technologies, e.g., Zwave, ZigBee, and other IoT protocols. The collected data can be used for many purposes which depend on an application of interest e.g., health monitoring, data analytics for smart homes and cities [5], faults reporting in a flight system, leakage alarm of chemical in a factory etc.

As data from IoT objects is precious, inadequate security measures in IoT devices may invite various security threats to the applications. An unauthorized data access may cause harm to an application where the end-users are directly involved. An attacker may exploit vulnerabilities in IoT devices to collect data through eavesdropping, and may gain financial profit by selling collected data. Moreover, recently security researchers have pointed out several vulnerabilities in smart cities technologies, few of them are attributed to authentication flaws, thus leaving IoT applications unse- cured [6].

Various vulnerabilities including lack of sufficient authentication is pointed out in the smart home technologies, and have claimed that these vulnerabilities may pose many risks to the individuals [7]. Home routers can be accessed by an attacker are identified through some researchers by exploiting a list of default login credentials on the IoT devices almost 2,000 devices [8]. Stellios et al. have shown verified cyberattacks on various IoT enabled domains, e.g., smart grid, intelligent transport network, industrial control system, medical IoT, and smart homes, etc. [9].

The authors have also claimed that the vulnerabilities (e.g., design flaws in authentication mechanism) in a smart light may lead to many threats in a smart home. Moreover, a dynamic attack is carried out by the IoT Botnet named 'Mirai' which has seriously affected many of IoT devices as claimed in [10]. Nevertheless, such lack of sufficient authentication and/or design flaws in authentication mechanisms in IoT devices leads to sensitive information or data breach which may be misused. Resultant, security has been one of the main challenges in the success of distributed smart environments and applications.

Lightweight and secure against security attacks. However, the threat model designed in this paper does not include many popular attacks, such as impersonation, man-in-the-middle (MITM), etc. As a consequence, their scheme may be incompetent to protect against impersonation and MITM attacks [11]. In addition, to execute the scheme (e.g., mutual authentication phase), the system incurs high time complexities. Therefore, this scheme may not be practical for resource-constrained devices.

A new technique is introduced a pair-wise key establishment scheme for wireless sensor net- works (WSNs) [12]. The scheme uses ECC based implicit certificates for pair-wise key establishment. The authors first performed the bootstrapping followed by establishment of

pair-wise key between nodes. However, physical capturing of a node may lead to disclosure of authentication key, which may emanate high security risks to other non-compromised IoT applications.

Figure 1 IoT based smart home security

An authentication and access control protocol is described for IoT [13]. The scheme has used ECC based mutual authentication (EMA) and capability based access control (CBAC) for operation. Elliptic Curve Discrete Logarithm Problem (ECDLP) and ECDH are used for generating and sharing the common secret keys for authentication. In order to do this, the protocol utilized a plethora of cryptosystem operations which make it compute expensive.

An authentication technique is proposed which is based on hardware and software co-verification for IoT. The authors have pointed out that since inception of IoT, targeting devices through cloning of hardware has become easy. To address cloning issue, they have proposed a physical unclonable function (PUF) based security protocol [14]. The proof-of-concept is implemented on Contiki operating system. This method is claimed to be very first attempt to prevent the IoT devices from cloning and reprogramming attacks.

2. SYMMETRIC KEY BASED SCHEMES

A lightweight session key establishment protocol is proposed for smart home environments [15]. A session key is produced using a short authentication token, which uses the silicon chip-identity. The authors claimed their scheme is efficient in terms of computation and communication costs and capable of protecting against attacks e.g., DoS, eavesdropping, masquerade, message forgery. In addition, their scheme satisfies the property of mutual authentication, session key establishment, confidentiality, integrity, and freshness. However, the scheme may not resist time synchronisation attacks. For instance, if clock loses synchronisation, then the scheme is vulnerable to replay attack. Moreover, anonymity and unlink ability issues are not addressed in the scheme [16].

Here elaborated that IoT networks have become a honeypot for attackers, thereby turning the privacy of the individuals under threat. The session key in their protocol is continuously renewed to prevent replay attacks. However, the authors have introduced several cryptosystem operations which made it bulky e.g. eight times hashing operations [17].

New technique is proposed on vulnerability of IoT devices at public places but also realized a need of robust IoT device authentication strategy. The authors proposed an authentication model using PUF to make IoT devices invulnerable to physical and cloning attacks [19]. Authors claimed that their scheme is resilient to impersonation, achieves un-traceability and also exhibit security properties e.g., mutual authentication, protection against physical attacks etc. However, their scheme may incur high computation requirements due to massive use of hash operations and high communication complexities. Thus, the scheme may not pertinent for the resource constrained and sensitive applications of IoT.

2.1. Contribution of Paper

- Here proposed a Lightweight and Robust Mutual Authentication Scheme (LRMA) for the distributed smart environments.
- To achieve the efficiency and light weight ness at resource constrained nodes, elliptic curve cryptography (ECC), implicit certificates, and symmetric encryption are used.
- The proposed scheme exhibits several security properties, such as mutual authentication, session key agreement, message freshness and anonymity and/or untraceability. Besides security properties, security analysis also shows that the proposed scheme is secure against many security attacks, e.g., replay, message modification, node compromise, key compromise, impersonation, known key, denial of service (DoS), and man-in-the-middle (MITM).
- Performance evaluation (including energy efficiency) and comparison demonstrates its high computational and communicational efficiency as compared to the state-of-the-art schemes.

3. SYSTEM MODEL (PROPOSED MODEL)

Fig. 2 depicts a high level system model in distributed smart environment. The system model mainly consists of following entities, such as IoT nodes, bi-directional communication channel, certification authority, etc. (e.g., humidity, light, etc.) from their respective environments and send the data wirelessly to the sink node via utilizing low-powered technologies, e.g., ZigBee. More precisely, sensors data is easily available from anywhere in an ad-hoc manner. From the security perspective, the IoT nodes request security credentials from the certificate authority. These security credentials are later utilized to perform the mutual authentication.

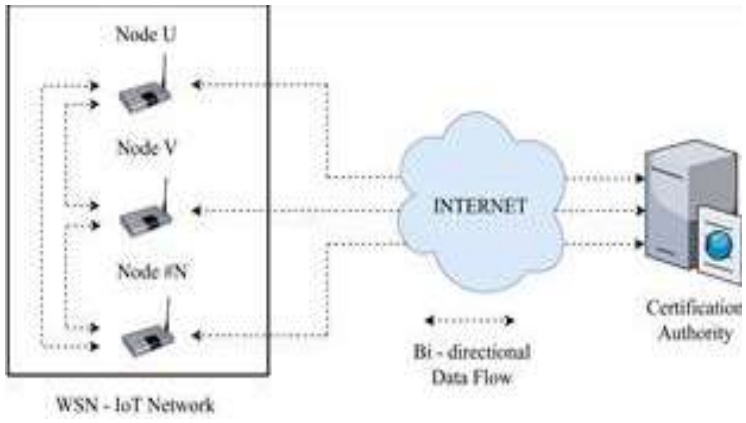

Figure 2: System model for authentication of IoT devices in smart homes.

Certificate Authority (CA): The CA is a trusted entity, and is responsible for generating and distributing implicit certificates to the entities. Moreover, it is con- sidered to be a tamper proof entity.

Communication Link: In the distributed IoT applications, IoT-nodes communicate with each other through bi-directional wireless technologies, such as Zigbee, Bluetooth, etc. In addition, the IoT nodes can communicate to CA either directly through GPRS/WiFi functionality or via gateway and cloud.

4. PROPOSED SCHEME

Assume a distributed smart environment, for instance a smart home (also known as a home area network (HAN)), which consists of several WSN-IoT nodes. Within a smart home and forward it to the IoT cloud and to the user. In order to provide security in such application, this section proposes a robust and lightweight authentication scheme. Note that in order to run the proposed scheme (i) all the entities are assumed to have identical cryptographic sys- tems including encryption and hashing algorithms, (ii) each certificate has its lifetime, e.g., a year. The proposed scheme consists of three phases: system set-up phase, registration phase, and authentication and key exchange phase.

4.1. System Set-Up Phase

In this phase, the CA off-line initializes the cryptographic mechanisms (such as, EC, n, point generator, hash function, symmetric encryption algorithm). Table 1 shows the nota- tions and descriptions which are used throughout the paper. Note that the background on ECC is omitted intentionally due to the space limit [19]. The CA generates own public key (Q_{CA}) and private key (d_{CA}). In addition, it generates a key pool of secret keys (e.g., $KS1, KS2, \ldots KSn$) for the HANs ($HAN\,1, HAN\,2, \ldots HANn$). It then publishes EC, n, point generator, Q_{CA}.

4.2. IoT-Node Registration Phase

In each home area network (HANi), an IoT node (e.g., node U) needs to be registered to the CA and obtains security creden- tials including a certificate and a key. The flow of registration phase is depicted in Fig. 3 and described as follows:

- *Initially, the node U generates a random number rU and computes RU = rU G. It then computes H 1 = H (RU || U) and M 1 = EQCA [rU, U]. Finally, the node U sends a cert-request message {M 1, H 1} to the CA.*
- *Upon receiving cert-request, the CA decrypts M 1 using dCA and obtains rU, U, and computes RU = rU G and H 10 and verifies H 10 == H 1. It then generates a random number rCA and implicit certificate CertU = RU + rCAG, computes e = H (CertU), s = erCA + dCA (mod n), H 2 = H (CertU , s, LT , KS1, RU , U , IDCA), Key = (rU ⊕ U ⊕ IDCA) and M 2 = EKey[CertU , s, LT , KS1, RU , U , IDCA]. Here, LT is the certificate lifetime of node U. Finally, the CA sends cert-response message {M 2, H 2} to the node U.*
- *The Node U derives Key0 = (rU ⊕ U ⊕ IDCA) decrypts M 2 using Key0 and obtains CertU , s, LT , KS1, RU , U , IDCA and stores them. Now it computes H 20 and verifies H 20 == H 2. Upon successful verification, the node U computes own public and privacy keys from the received implicit certificate, as follows:*
- *dU = erU + s(mod n)*
- *QU = dU G*

- $= (erU + s(mod\ n))G$
- $= (erU + erCA\ (mod\ n) + dCA\ (mod\ n)\ (mod\ n))\ G$
- $= (erU + erCA\ (mod\ n) + dCA\ (mod\ n))\ G$
- $= e(rU + rCA)G + dCAG$
- $= e\ (rU\ G + rCAG) + QCA$
- $= e(RU + rCAG) + QCA$
- $QU = eCertU + QCA$

5. CONCLUSION

Here proposed a Lightweight and Robust Mutual-Authentication (LRMA) scheme for the distributed smart environments. LRMA utilized implicit-certificate to achieve its simplicity and efficiency. The accomplishment of the security goals (i.e., secrecy, authentication, and message freshness) of the proposed scheme has been proven through formal (AVISPA) and informal analysis. We have demon- strated, through the performance evaluation, that LRMA is robust against attacks, consumes less computation and communication energy costs. All these properties make the LRMA suitable for the next generation smart home area networks. As future work, the authors plan to extend the proposed model to support authentication between users and devices in Machine Learning.

REFERENCES

[1] Geneiatakis, Dimitris, et al. "Security and privacy issues for an IoT based smart home." 2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO). IEEE, 2017.

[2] Elhoseny, Mohamed, et al. "Secure medical data transmission model for IoT-based healthcare systems." Ieee Access 6 (2018): 20596-20608.

[3] Arena, Fabio, Giovanni Pau, and Alessandro Severino. "An Overview on the Current Status and Future Perspectives of Smart Cars." Infrastructures 5.7 (2020): 53.

[4] Poongothai, M., P. Muthu Subramanian, and A. Rajeswari. "Design and implementation of IoT based smart laboratory." 2018 5th International Conference on Industrial Engineering and Applications (ICIEA). IEEE, 2018.

[5] Rathore, M. Mazhar, et al. "Urban planning and building smart cities based on the internet of things using big data analytics." Computer Networks 101 (2016): 63-80.

[6] Alqahtani, Abdulaziz, et al. "Identifying Vulnerable Critical Infrastructure Zones in Smart Cities." 2020 16th International Conference on the Design of Reliable Communication Networks DRCN 2020. IEEE, 2020.

[7] Moraci, Francesca, et al. "Making less vulnerable cities: resilience as a new paradigm of smart planning." Sustainability 10.3 (2018): 755.

[8] Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, “Electron spectroscopy studies on magneto-optical media and plastic substrate interfaces (Translation Journals style),” IEEE Transl. J. Magn.Jpn., vol. 2, Aug. 2002, pp. 740–741 [Dig. 9th Annu. Conf. Magnetics Japan, 1982, p. 301].

[9] M. Young, The Techincal Writers Handbook. Mill Valley, CA: University Science, 2013.

[10] J. U. Duncombe, “Infrared navigation—Part I: An assessment of feasibility (Periodical style),” IEEE Trans. Electron Devices, vol. ED-11, pp. 34–39, Jan. 2017.

[11] Conti, Mauro, Nicola Dragoni, and Viktor Lesyk. "A survey of man in the middle attacks." IEEE Communications Surveys & Tutorials 18.3 (2016): 2027-2051.

[12] R. W. Lucky, “Automatic equalization for digital communication,” Bell Syst. Tech. J., vol. 44, no. 4, pp. 547–588, Apr. 2019.

[13] G. R. Faulhaber, “Design of service systems with priority reservation,” in Conf. Rec. 2012 IEEE Int. Conf. Communications, pp. 3–8.

[14] W. D. Doyle, “Magnetization reversal in films with biaxial anisotropy,” in 2014 Proc. INTERMAG Conf., pp. 2.2-1

[15] J. P. Wilkinson, “Nonlinear resonant circuit devices (Patent style),” U.S. Patent 3 624 12, July 16, 2000.

[16] IEEE Criteria for Class IE Electric Systems (Standards style), IEEE Standard 308, 2012.

[17] Letter Symbols for Quantities, ANSI Standard Y10.5-2000.

[18] R. E. Haskell and C. T. Case, “Transient signal propagation in lossless isotropic plasmas (Report style),” USAF Cambridge Res. Lab., Cambridge, MA Rep. ARCRL-66-234 (II), 2012, vol. 2.

[19] Gope, Prosanta, and Biplab Sikdar. "Lightweight and privacy-preserving two-factor authentication scheme for IoT devices." IEEE Internet of Things Journal 6.1 (2018): 580-589.