Enhanced Security Mechanism for Emerging Home Area Networks

Mobin Khan[1], Muhammad Taha Jilani[2], Safdar Rizvi[3], Asif Aziz [4]
[1,2]PAF Karachi Institute of Ecnomics and Technology, Karachi, Pakistan
[3]Bahria university, Karachi Campus, Pakistan
[4]Sir Syed University of Engineering and Technology, Karachi, Pakistan
[2]mtaha.jilani@gmail.com

Abstract **- The recent advancement in internetworking technologies has provided the connectivity not only between humans, but between things too. For these things, it introduces the "internet of things" (IoT) that is now widely using in various domains. Under the IoT umbrella, particularly for homes, a relatively new type of network, i.e. home area network (HAN) has gained much interest these days. However, for such networks the security is the biggest concern for the users. This paper provides an overview of HAN that can be used for smart homes using range of multiple wireless access techniques. Further, a thorough discussion on security vulnerability is presented while an enhanced security mechanism is also proposed for the future HANs. For this purpose, a state of the art encryption algorithm Elliptic Curve Cryptography (ECC) which provides high level security with small key size is proposed. The proposed ECC has considered all the aspects of information security such as data confidentiality, access control, authentication, availability, data integrity and non-repudiation. Moreover, it also reduces the processing overhead and battery consumption of battery operated devices in typical HAN.**

Keywords - Internet-of-things, IoT, home area network, network security, ZigBEE.

I. INTRODUCTION

The evolution of internet at DARPA in late 70's enabled people to share information in more efficient manner. In 2012, the further progress in evolution of Internet envisioned a new concept IoT (Internet of Things). The term IOT is combination of two terms. The "Things" refers to the devices while "Internet" defines their interconnectivity. So IoT comprise of small interconnected objects which interact, coordinates and share information to obtain a specific goal [1]. The objects can be interconnected via various communication technologies such as ZigBee, UWB, Blue tooth and 802.11 WLAN etc. They can also be interconnected through Internet via gateways.

The Smart Home is most inspiring application of IoT now a day[2]. It aims at developing technologies for making home automated and intelligent. Many tasks are automated in Smart Home such as lightning, temperature control, ventilation, entertainment and door opening etc. In door opening service, a resident can enter in home by authenticating its identity to the system. Lights and various other devices such as Air conditioner will be automatically switched on according to resident's preferences. Same as when the resident leaves the home, the system will automatically switch off the lights and other devices to conserve energy. The door will be locked to provide protection against the unauthorized physical entry. The home automation system enables its resident to remotely control home appliance through smart phones at any place any time. Moreover alerts can be sent to resident regarding various events happening in home in his absence.

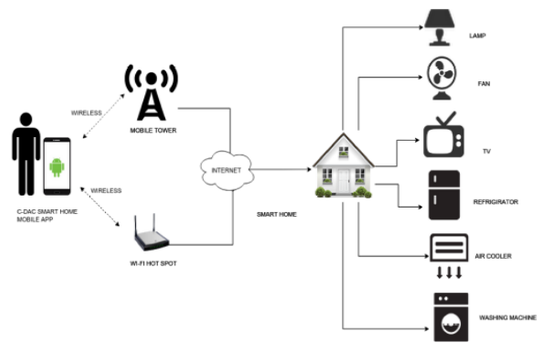

Figure 1 Typical Smart Home

The devices in Smart Home are connected to Home Automation server via HAN (Home Area Network). Different technologies can be used for HAN such as ZigBee, Bluetooth and 802.11 WLAN series. The Home Automation Server collects, analyzes the data received from the devices and provides various services to its residents. To provide services to its resident remotely, a gateway is used to connect Home Automation system to Internet. However inside the home, the resident will use HAN to get services.

The security of home is not limited only to physical security but also to security of HAN. Since devices are connected via wireless network, any adversary can access and manipulate HAN [3]. The devices used in Smart Homes are heterogeneous and have diverse features. Some have less computational resources and limited battery so they cannot afford security mechanisms, while other devices have adequate computational resources to accommodate the traditional security mechanisms. Moreover any remote access to the system also requires authentication to prevent misuse of the system. This approach has also presented in few industrial applications, those has been reported before [4].

Many proposed solutions of Smart Home have vulnerability in term of security. Beside the security issues low power, efficient and reliable connectivity is also a weak spots in these solutions. In this research paper, a comprehensive implementation for a secure smart home system is provided. The implementation resolves different issues in the existing solution such as

(i) Providing reliable, low power and efficient HAN connectivity
(ii) Prevention of HAN from unauthorized access
(iii) Providing secure mechanism for accessing the smart home system remotely by resident

Copyright held by the author(s).

CEUR-WS.org/Vol-2145/p23.pdf

The rest of paper is organized in following sequence. The Section II overviewed different existing solutions and their vulnerabilities. Different communication technologies that can be used for smart home network are also reviewed in this section. The Section III discuses my proposed design and Section IV concludes the research paper.

II. RELATED WORK

This Section is divided in two parts. First part reviews existing smart home implementations. The second part provides a brief overview of candidate communication technologies for implementing smart home.

A: - Existing Smart Home Implementations

Extensive research work is in progress to build efficient Home Automation System. Although the idea of Smart Home is uncommon in developing countries such as Pakistan. But in developed countries, the smart home is now a reality. Many studies are carried out in near past in the area of Smart Home.

The [5] proposed a Home Automation system to control home appliances. The proposed system has ability to prevent tempering. It enables the user to interact with system through SMS.

Another Home Automation System is proposed by [6] which is Microcontroller based and provides security through password. The user can control and monitor different activities such as lightening, ventilation and cooling etc.

The [7] presented an architecture which analyzes the data received from various sensors to extract contextual information. This contextual information enables the system to provide context aware services to its user. The author also has discussed various mechanisms for acquiring and analyzing the data received from the sensors that are deployed at home.

The [8] suggested the use of IoT for conservation of energy in Smart Home. His implementation made use of camera images for recognition of human activities with the aid of image processing algorithms.

The [9] identified different requirements of Smart Home. He discussed various issues which can be faced in deploying IoT in smart home. He also presented some possible solutions to overcome these issues.

B:- Candidate Communication Technologies

In 2005, IEEE finalized specifications for WPAN (Wireless Personal Area Network) and announced it in IEEE 802.15 standard. This IEEE 802.15 standard provides specifications for wireless connectivity up to two layers (Physical and MAC Layer). The WPAN standard focuses on provision of wireless connectivity in POS (Personal Operating Space). The POS is area up to 10 meters in all around of a person or any object[10]. The IEEE 802.15 standard's specifications (Physical and MAC Layer) are used by many communication technologies such as

(i) IEEE 802.15.1 is Bluetooth
(ii) IEEE 802.15.3 UWB
(iii) IEEE 802.15.4 ZigBee

Bluetooth was developed in 1990 to interconnect the personnel devices around the body of soldier. The major goals of Bluetooth development project were to develop a low energy and self-healing network having ability to provide on the fly communication[11]. Bluetooth is mostly used for wireless personal devices now a day such as headphone and keyboard etc. Its range is normally 10 meters but extendable (up to 100 m) by using Amplifier. The cryptographic system named E0 (a stream cipher) is used in Bluetooth to provide confidentiality. The key size in this cipher algorithm is not fixed. It can be in the range from 8 to 128 bits (mutually selected by both sender and receiver). Despite of sufficient long key size, the E0 stream cipher is vulnerable to various attacks which include Man-in-Middle, Blue-Snarfing and viruses[12].

UWB (Ultra Wideband) make use of large band of frequencies to provide low power communication with high data rate[13]. UWB is NLOS (Non Line of Sight) based communication technology. One of its distinguishable features which make it superior from other is that it can efficiently penetrate through doors, walls and any obstacle which is non-conductor. As aforementioned, it sends data over a large band of frequencies in the form of narrow pulses. To send pulses efficiently and time precisely manner, pulses are modulated with a carrier. The data rate provided by UWB is 40 Mbps to 60 Mbps which is suitable for many applications (in this case it is Home Automation System). However UWB is not suitable for this implementation due two reasons. First, the high level of radiation over large frequency band is dangerous to human body. Second is that UWB requires high level of coordination between sender and receiver to transfer data (as aforementioned) which is infeasible for small device to achieve it[14].

ZigBee is protocol stack developed by ZigBee Alliance. All specifications of ZigBee are defined in IEEE 802.15.4 which is extension of IEEE 802.15 WPAN[14]. As aforementioned, the IEEE 802.15 standard has just defined specification for first two layers[14]. The specifications for rest of the layers are defined by ZigBee Alliance as shown in figure 2

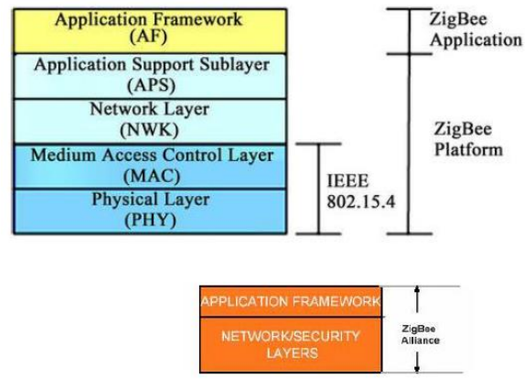

Figure 2 ZigBee Protocol Stack

ZigBee is low power and simple protocol which provide efficient communication at the cost of low data rate. A dominating feature of ZigBee is robust security mechanism AES-128 (Advance Encryption Standard with 128 bit key) whose cryptanalysis is not reported till yet[15]. Maximum range of communication which it can provides is 100 meter (can be reduced due to environmental conditions) based on LOS (Line of Sight). To extend the range, it supports various topologies such as Mesh, tree, star or their combination.

ZigBee network consist of three devices which are Coordinator, Router and End Device. The coordinator is full

function device and always installed first before other types of devices. It is responsible for establishing ZigBee network. It allocates PAN ID for identification of each device that is going to join the network. Another type of device is also a full function device named Router. It assists in extending the range of network. It performs relaying operation in network. The last type is reduced function device called End device. It can be an ordinary device or sensor which sends data to coordinator as shown in figure

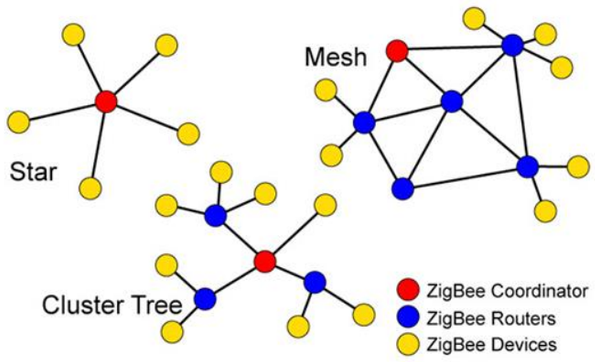

Figure 3 ZigBee Devices

As aforementioned, ZigBee uses AES-128 (Advance Encryption Standard with 128 bit key) for data encryption. For secure key management at run time, three types of keys are used by ZigBee. First one is Master key which is preconfigured in devices to provide secure communication with other devices while joining the network. The Link key is used to provide secure communication between each pair of devices. Third is Network key which should be shared among all the devices. This key is 128 bit long and is used for secure communication among all the devices in the network at current time. This key is changed time to time to enhance security[16]. ZigBee is not suitable for this implementation due to two reasons. First, the AES-128 is very resource extensive algorithm which make it infeasible for small devices having low resources (such computational capability and limited battery power). Second it works in Ad-hoc mode which has inherited drawbacks such as complex routing protocol and increased latency etc.

IEEE 802.11ah is developed by IEEE in 2014 to be operated in 900 MHZ frequency band[17]. This is a WLAN standard and has long range in contrast with other contemporary WLAN standards because it operates in lower frequency band[18]. Moreover having capability to uniquely identify large number of devices, it is supposed best for IoT applications. This standard has simple and small frame size along with efficient MAC protocol which enables the devices to reduce their power consumption during data transmission and reception.

Infect the security of communication is not just encryption of data but risk jamming is also its important aspect. To counter jamming, two modulation techniques are used which are FHSS (Frequency hopping spread spectrum) and DSSS (Direct sequence spread spectrum). The IEEE 802.11ah uses DSSS as modulation technique which make it suitable for establishing jamming resistant Home Area Network in my implementation.

We have proposed a secure, efficient and reliable implementation for Home Automation System. My proposed scheme uses Elliptic Curve Cryptography (ECC) for encrypting data. ECC is considered very efficient for resource constraint devices and provides same level of security as other state of the art cryptographic algorithms provides.

III. PROPOSED WORK

For better understanding this section is divided in two parts. Part one describes HAN and its interface with traditional network. This part also addresses various aspects of remote access to HAN by resident. The Part two covers various security aspects of Smart Home system such as data confidentiality, authentication, data integrity, access control and non-repudiation.

A. Home Area Network

A typical Smart Home contains many small smart sensors, devices and actuators. The sensors or devices are attached to home appliances for making them controllable by Smart Home System. These devices or sensors are heterogeneous and having diverse features. The diversity of features makes the design of overall system difficult. As aforementioned, IEEE 802.11ah is considered best technology for IoT application due to its long range with low power consumption. Moreover its capability of identifying large devices uniquely also attracts the IoT application designers. To interconnect the devices in HAN, an IEEE 802.11ah AP (Access Point) is installed in home. All devices in the home are connected to each other and to Smart Home system via this AP. The AP provides communication in infrastructure mode for simplicity (Ad-hoc mode has more complex communication protocol). The AP is responsible for allotment of Device ID to each device for identification purpose. This AP is connected to Smart Home system via IEEE 802.3 Ethernet. It is noticeable that one AP can efficiently interconnect all the devices in the home but second AP is installed to make the HAN fault tolerant. The layout of HAN is shown in figure 4

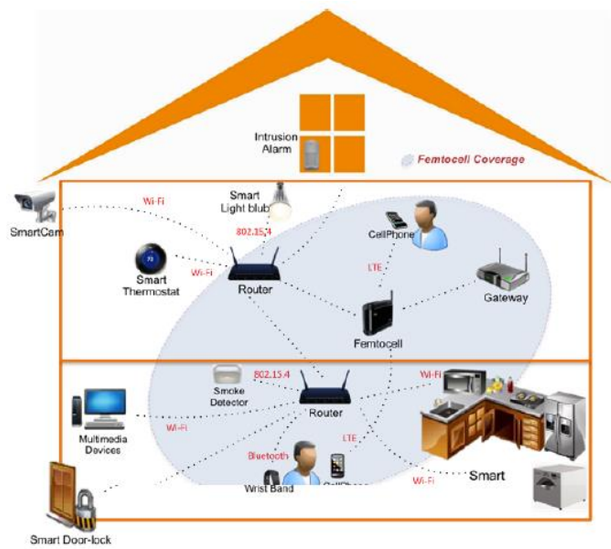

Figure 4 Home Area Network

As shown in figure, HAN is connected to a gateway. The gateway connects the Smart Home System to internet. This enables the resident to interact with the Smart Home System through application installed on his smart phone. For high speed and reliability, DSL is used in my proposed scheme to connect the Smart Home system to internet.

To interconnect the resident with system in the home vicinity, an IEEE 802.11b/g/n AP is installed. This AP is

further connected to Smart Home System via Ethernet. The reason for installing this AP is that traditional smart phone's Wi-Fi supports a/b/g/n variants of 802.11 standards. So IEEE 802,11ah AP cannot be used to connect the user with system. At the places other than home vicinity, user uses the 3G/4G to interact with Smart Home System. More emerging technologies that reported elsewhere [19], can also become the part home area network.

B. Security of Home Area Network

In the modern era, a computer system or network is useless if it is not secured [20]. The security of computer or network is not just limited to access control but there other aspects security also. The other aspects are availability, data confidentiality and data integrity etc. For efficient and secure Home Automation System, a good design must address all these aspects of security. To provide security of the whole HAN which is based on IEEE 802.11ah, my proposed scheme makes use of Elliptic Curve Cryptography (ECC). It is noticeable that other WLAN standards such as IEEE 802.11b/g/n has its own comprehensive security mechanism such as WPA2 (Wireless Protected Access 2) which employees state of the art encryption algorithm AES (Advance Encryption Standard). Although encryption reduce the throughput but at the other hand security of data is obtained which is prime requirement of modern era. The use of encryption algorithm is inevitable in proposed scheme because IEEE 802.11ah has no built-in security mechanism. It is worth to mentioned that the AES encryption algorithm has been proposed earlier [21], for the resource-constraint devices using decentralized approach.

There ECC has some good features due to which it is chosen for security implementation in my proposed scheme. The prime feature is that it provides same level of security with smaller key size which makes it distinguishable from other contemporary asymmetric cryptographic algorithms such as RSA [22].

As aforementioned, network security is not limited to just encryption of data or access control. There are other aspects of network security also. All aspects of network security are discussed under mentioned and their implication in proposed idea is also explained.

(i) Data Confidentiality

Data confidentiality means prevention of data from unauthorized disclosure. In easy words, the data should be disclosed to only authorized entities involved in communication. To provide confidentiality, proposed scheme make use of ECC as aforementioned. Each network entity or device will be allotted a public/private key pair. Public keys of all the devices will be shared among all the devices. If a device "A" want to send data securely to device "B", it will encrypt its data with public key of device "B". When device "B" receives data, it will decrypt the data with its private key. It is noticeable that asymmetric or public key cryptographic algorithms are different from symmetric key cryptographic algorithm because they encrypt data with one key and decrypt with other key. In symmetric cryptographic algorithms data is encrypted and decrypted with same key. The public/private key pair for each device will be generated by Home Automation System and will be configured in device before deployment. If a new device joins the HAN, its public key will be broadcasted to all the entities in HAN so they can securely communicate with this device. Similarly a remote user is also allotted with a public/private key pair so it can securely communicate with Home Automation System over traditional network (internet).

(ii) Data Integrity

Data integrity mean that received data is same as sent by sender. In other words received data is intact and is not altered during transient. There are many algorithms such MD-5, SHA-1 and SHA-2 etc. for checking integrity of data. My proposed scheme employs SHA-1 for integrity check because it is faster than MD-5 and has small hash code size than SHA-2 with adequate security level. The SHA (Secure Hash Algorithm) is basically a one way hash function invented in 1990 by NIST (Nation Institute of Standards and Technology) USA. In 1995 its improved version is introduced named SHA-1. This version produce message digest or hash code of 160 bits. To provide data integrity check, sender will compute hash code of data based on SHA-1 before encryption and hash code will be attached to data. After attaching the hash code data will be encrypted and will be sent. The receiver will decrypt the data with its private key and will compute SHA-1 hash code of received data. If the computed hash code of data is similar with received hash code, the integrity of received data is preserved and data will be accepted. If both hash code found dissimilar the data will be rejected. It is noticeable that two or more messages may have same hash code (which is called collision in hashing concept) but it is almost impossible to compute message from hash code. The collision often happens because hashing maps unlimited arbitrary length message to a limited fixed length code so there may be one or more hash code which is being mapped by many messages.

(iii) Availability

Availability means system is available all the time to its user for providing services. If the system is not available to its user (due to any reason such as network down) then it is useless. System should be available all the time for usage. There are many reasons that effect availability which includes network down, network equipment or hardware failure (such as LAN switch or AP became down) and power failure etc. To tackle the problem of failure of network equipment (AP), the proposed scheme includes two AP in its HAN design to provide redundancy. Both AP provides same functionality and also backup each other if one AP becomes fail. UPS (Uninterrupted power supply) will provide electric power to Home Automation System's Server, network equipment and all the devices in case of primary AC power fails. However network unavailability (both in term of physical unavailability of network or due to DoS (denial of service) attack) is a difficult problem to tackle. This problem can only be solved by providing multiple internet connection (of different ISPs) to this Home Automation system for redundancy.

(iv) Access Control

Access control refers to prevention of resources from unauthorized usage. It means that only authorized entity can access and use a system resource. In order to ensure access control to resources based on only IP address is not sufficient

because IP address can be easily spoofed. Each data sending device in HAN will attach its device ID with data before encryption. This Device ID will enable the receiving device to ensure the identity of sender so that access to resources of this device could be granted. To avoid replay attack, time stamp will also be attached to data.

(v) Authentication

Authentication refers to verifying that communicating entity is the legitimate entity. In easy words to verify that the entity who is communicating with the system is disclosing its real identity (IP address and user ID etc.). For providing authentication checking facility, sender will encrypt the message hash code with its private key. The receiver will decrypt the message hash with the public key of sender. If hash code of message is successfully decrypted then data is authenticated (sent by legitimate sender) and will be accepted. Because only sender know its private key and no one other than sender can form a message such that it can be decrypted with the public key of sender without knowing sender's private key. The encryption of data by sender with its private key is called Digital Signature

(vi) Non-repudiation

Non-repudiation means that entities involved in communication should not be able to deny the messages they have sent. It means that if "A" send a message to "B" than there should be a mechanism such that "B" can prove that message is really sent by "A" in case of dispute ("A" denied sending of such message). For providing non-repudiation mechanism among the all entities of Smart Home Automation System (users, devices and network equipment) digital signature is an efficient solution (explained aforementioned).

IV. CONCLUSION

The integration of internetworking technologies and the computation has emerged the IoT. The application of IoT in homes introduces the home area network (HAN). For such networks, security is the biggest challenge and concern for the users. This work has presented a design of a reliable, simple but secure Smart Home Automation System. It has two important features which make it distinguishable from other Smart Home implementations. First is that it made use of Elliptic Curve Cryptography which provides same level of security with small key size (in contrast with other contemporary cryptographic algorithms such as RSA).Due to small key size processing overhead and battery consumption is reduced. The second feature is that all the aspects of information security such as data confidentiality, access control, authentication, availability, data integrity and non-repudiation is considered and implemented.

REFERENCES

[1] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," *Computer networks,* vol. 54, pp. 2787-2805, 2010.

[2] Q. Zhu, R. Wang, Q. Chen, Y. Liu, and W. Qin, "Iot gateway: Bridgingwireless sensor networks into internet of things," in *Embedded and Ubiquitous Computing (EUC), 2010 IEEE/IFIP 8th International Conference on*, 2010, pp. 347-352.

[3] T. Zia and A. Zomaya, "Security issues in wireless sensor networks," in *Systems and Networks Communications, 2006. ICSNC'06. International Conference on*, 2006, pp. 40-40.

[4] M. T. Jilani, M. Z. U. Rehman, A. M. Khan, O. Chughtai, M. A. Abbas, and M. T. Khan, "An implementation of IoT-based microwave sensing system for the evaluation of tissues moisture," *Microelectronics Journal,* 2018/03/26/ 2018.

[5] M. S. H. Khiyal, A. Khan, and E. Shehzadi, "SMS based wireless home appliance control system (HACS) for automating appliances and security," *in Informing Science and Information Technology,* vol. 6, pp. 887-894, 2009.

[6] I. Kaur, "Microcontroller based home automation system with security," *International journal of advanced computer science and applications,* vol. 1, pp. 60-65, 2010.

[7] B. Kang, S. Park, T. Lee, and S. Park, "IoT-based monitoring system using tri-level context making model for smart home services," in *Consumer Electronics (ICCE), 2015 IEEE International Conference on*, 2015, pp. 198-199.

[8] J. JeyaPadmini and K. Kashwan, "Effective power utilization and conservation in smart homes using IoT," in *Computation of Power, Energy Information and Commuincation (ICCPEIC), 2015 International Conference on*, 2015, pp. 0195-0199.

[9] P. P. Gaikwad, J. P. Gabhane, and S. S. Golait, "A survey based on smart homes system using Internet-of-things," in *Computation of Power, Energy Information and Commuincation (ICCPEIC), 2015 International Conference on*, 2015, pp. 0330-0335.

[10] K. S. Sze-Toh and K. C. Yow, "Usage of mobile agent in configuring WPANs," in *Control, Automation, Robotics and Vision, 2002. ICARCV 2002. 7th International Conference on*, 2002, pp. 938-943.

[11] P. McDermott-Wells, "What is bluetooth?," *IEEE potentials,* vol. 23, pp. 33-35, 2004.

[12] T. Panse and V. Kapoor, "A review on security mechanism of Bluetooth communication," *International Journal of Computer Science and Information Technologies,* vol. 3, pp. 3419-3422, 2012.

[13] M. Santhanam, "UWB technology and its application," ed, 2012.

[14] J.-S. Lee, Y.-W. Su, and C.-C. Shen, "A comparative study of wireless protocols: Bluetooth, UWB, ZigBee, and Wi-Fi," in *Industrial Electronics Society, 2007. IECON 2007. 33rd Annual Conference of the IEEE*, 2007, pp. 46-51.

[15] P. Baronti, P. Pillai, V. W. Chook, S. Chessa, A. Gotta, and Y. F. Hu, "Wireless sensor networks: A survey on the state of the art and the 802.15. 4 and ZigBee standards," *Computer communications,* vol. 30, pp. 1655-1695, 2007.

[16] N. Vidgren, K. Haataja, J. L. Patino-Andres, J. J. Ramirez-Sanchis, and P. Toivanen, "Security threats in ZigBee-enabled systems: vulnerability evaluation, practical experiments, countermeasures, and lessons learned," in *System Sciences (HICSS), 2013 46th Hawaii International Conference on*, 2013, pp. 5132-5138.

[17] S. Aust, R. V. Prasad, and I. G. Niemegeers, "IEEE 802.11 ah: Advantages in standards and further challenges for sub 1 GHz Wi-Fi," in *Communications (ICC), 2012 IEEE International Conference on*, 2012, pp. 6885-6889.

[18] W. Sun, M. Choi, and S. Choi, "IEEE 802.11 ah: A long range 802.11 WLAN at sub 1 GHz," *Journal of ICT Standardization,* vol. 1, pp. 83-108, 2013.

[19] A. Abbas, M. T. Jilani, and M. K. Khan, "Comparative Analysis of Wireless Technologies for Internet-of-Things Based Smart Farm," *Science International,* vol. 29, pp. 373-378, 2017.

[20] C. Lee, L. Zappaterra, K. Choi, and H.-A. Choi, "Securing smart home: Technologies, security challenges, and security requirements," in *Communications and Network Security (CNS), 2014 IEEE Conference on*, 2014, pp. 67-72.

[21] M. Khan, M. T. Jilani, M. K. Khan, and M. B. Ahmed, "A Security Framework for Wireless Body Area Network Based Smart Healthcare System," in *International Conference for Young Researchers in Informatics, Mathematics and Engineering, (ICYRIME), Kaunas, Lithuania*, 2017, pp. 80-85.

[22] N. Alimi, Y. Lahbib, M. Machhout, and R. Tourki, "On Elliptic Curve Cryptography implementations and evaluation," in *Advanced Technologies for Signal and Image Processing (ATSIP), 2016 2nd International Conference on*, 2016, pp. 35-40.