A security framework for wireless body area network based smart healthcare system

Mobeen Khan, Muhammad Taha Jilani[1], Muhammad Khalid Khan, Maaz Bin Ahmed
Graduate School of Science & Engineering, PAF- Karachi Institute of Economics and Technology, Karachi, Pakistan
[1]e-mail: mtaha.jilani@gmail.com

***Abstract*—In recent years, there is enormous growth of smart systems that have been developed for range of applications. This development is focused on Internet-of-Things (IoT), which will eventually, transform IoT into system of systems. Such smart systems are widely utilized in healthcare; however, the wide scope of such systems is also vulnerable to security and privacy issues. This paper proposes a security framework for wireless body area network (WBAN) based smart healthcare system. The proposed framework implies the security mechanism by considering low power and low resources devices within the WBAN. This is not just reduces the complexity for resource constrained devices, but ensures the availability and data integrity in simple, yet effective manner.**

Keywords—Wireless body area network (WBAN) security; Internet-of-Things; smart healthcare; e-Health systems; ZigBee security framework; IoT architecture

I. INTRODUCTION

The recent advancements in the information and communication technologies enable the researchers and engineers to realize the smart systems for various applications. The realization of such systems will lead to develop the system of system, or also known as Internet-of-Things (IoT). The IoT is defined as various tiny physical objects, that are capable to sense from their surroundings, connected with each other by different networks and share their collected data to convey information [1]. These IoT based systems can be employed in industrial applications such as remote-sensing, manufacturing, transportation, smart-homes, smart-communities and healthcare. With the help of these small interconnected sensors or objects the automation of certain system can be achieved [2]. An important application is the smart healthcare system, where the doctors can monitor the symptoms of a patient remotely by Wireless Body Area Network in IoT environment [3]. However, for an IoT environment one of the most important aspect is the security and privacy, which is still questionable in many proposed IoT architectures. The architectures are not well defined, as they have not provided the information, like how data can be restricted and preserve its integrity. In conventional networks AES encryption technique can be used for information security [4]. But it cannot be applied to IoT based devices, that are small and limited resources, such as power and processing capabilities [5]. Therefore, an efficient security mechanism for these resource constrained devices is currently an important research area.

These days, multiple wireless networks are available around us, these wireless devices are interconnected over a traditional network like internet which can be used to connect the remote-users in a fast, reliable and cost effective manner. Nevertheless, the connected devices over conventional network then there will be need for a security mechanism that can restrict attacker access and control. However, conventional network has limited protection that is not suitable for an IoT network [5]. For instance, an endeavor can access and manipulate the IoT devices which may have an anonymous result. Therefore, there is a need for security framework that can be implemented to protect the IoT system that cannot be accessed from inside and outside of network, except authorized entities.

The wireless body area networks (WBANs), are one of the low power sensor network [6], which provides efficient and reliable infrastructure for healthcare system including implanted, non-implanted and wearable sensor devices for human body. These sensor devices are used to capture various symptoms of a patient like heartbeat, body temperature, blood pressure, respiration and ECG etc. and send these symptoms to a Body Network Controller (BNC). BNC is an essential part of a WBAN which is capable to capture sensor data and after processing forwards to the centralized e-Health server. The e-Health server in turn saves this real time data from various patients that can be monitored by his clinician.

As shown in *Figure 1*, a BNC collects and processes data from the devices and forward it to a server using a wireless access network. The Wireless access network which is used in this scenario is IEEE 802.11ah. This standard is especially designed for IoT devices. There can be use of WLAN 802.11a/b/n standards but IEEE 802.11ah has some additional feature (like long range with low power consumption).

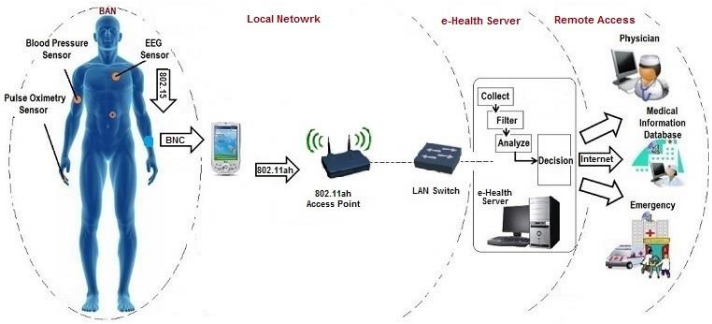

Figure 1. A typical WBAN in a smart healthcare system within the IoT network with its: things, network, and applications [7].

The comparison of various IEEE 802.11 standards is presented in Figure 2. In hospital vicinity, numerous 802.11ah WLAN access points are configured and installed. The e-Health server is connected via IEEE 802.3 Ethernet with these access points. As explained before, an e-Health server that stores real time data is connected to internet that enables doctors to access this information from remote-end. Likewise, conventional network here a vulnerability rises since the connection between BNCs and e-Health server may have insider threats and similarly, it may face outside attacks. Therefore, it is essential to implement a mechanism that ensure the security for a smart Hospital [3, 8].

Standard	Frequency Band	Bandwidth	Modulation Scheme	Channel Arch.	Maximum Data Rate	Range
802.11	2.4 GHz	20 MHz	BPSK to 256-QAM	DSSS, FHSS	2 Mbps	20 m
b	2.4 GHz	21 MHz	BPSK to 256-QAM	CCK, DSSS	11 Mbps	35 m
a	5 GHz	22 MHz	BPSK to 256-QAM	OFDM	54 Mbps	35 m
g	2.4 GHz	23 MHz	BPSK to 256-QAM	DSSS, OFDM	54 Mbps	70 m
n	2.4 GHz, 5 GHz	24 MHz and 40 MHz	BPSK to 256-QAM	OFDM	600 Mbps	70 m
ah	900 MHz	1, 2, 4, 8, and 16 MHz	BPSK to 256-QAM	SC, OFDM	40 Mbps	1 km

Figure 2. Comparison of variants of IEEE 802.11 WiFi standard

This research study focuses the three major goals, these are: (i) Access security of BNC and e-Health server (ii) Data confidentiality, and (iii) Availability of system. As mentioned earlier, traditional networks utilizes the state of the art encryption algorithm, such as 3DES, AES, IDEA etc. However, these algorithms cannot be implemented in small devices with limited resources (in term of power consumption and processing capabilities). This work implements the AES with CTR (Counter) mode in BNC for encryption [8]. The AES CTR keys are generated at server side and then sent to BNC via a shared (private) key. The generated key is shared and then configured at BNC while patient register themselves. The encryption that is performed by XOR operation with CTR keys, will exchange periodically while BNC is said to be in ideal mode. The logical operation of XOR, can be implemented easily and efficiently even for a small resource devices [9]. Thus, demonstrates that AES-CTR mode may have same security level as other modes.

At other side e-Health server also use the public key algorithm for secure communication with remote users (sucah as, Doctors). Each user has its own private key and they will communicate with server by using a session key (session key is exchanged with the help of public key). By implementing this method confidentiality and security access of BNC and e-Health server can be achieved. The availability of system can be ensured by tracking the heartbeat of a patient, whereas the unavailability activates the emergency.

The remaining paper is organized as, Section II overviews the different existing communication protocol and their vulnerabilities in terms of security, while the Section III represents our proposed framework and at last, Section IV concludes this study.

II. RELATED WORK

Wireless Personal Area Network (WPAN) falls in low power wireless technology category. WPAN is specified in IEEE 802.15 standard and released in 2005. For wireless connectivity IEEE defines PHY and MAC layer specifications for fixed, portable, and moving devices within a POS (personal operating space)[10]. POS is typically extends up to 10 m in all directions of an object, whether it is stationary or in motion. As shown in the Figure *3* there are different technologies that are defined within WPAN excluding IEEE 802.11ah:

- IEEE 802.11ah
- IEEE 802.15.1 is Bluetooth
- IEEE 802.15.4 ZigBee
- IEEE 802.15.6 WBAN

Wireless technology	Standard	Network topology	Transmission range	Frequency	Bit rate
ZigBee	802.15.4	star, cluster-tree, mesh	10 - 20 m	2.4 GHz	250 kb/s
Bluetooth	802.15.1	piconet, scatter net	10 - 30 m	13.56 MHz, 2.4 GHz	2.1 Mbit/s
Bluetooth low energy	802.15.1	star	≈ 50 m	2.4 - 2.5 GHz	1 Mbit/s
IEEE 802.15.6	802.15.6	star	< 100 m	NB, UWB, HBC	75.9 kb/s - 15.6 Mb/s
UWB	802.15.4a	piconet, peer-to-peer	10 m	3.1 - 10.6 GHz	480 Mb/s
WiFi	802.11	mesh	100 m	2.4 GHz	54 Mb/s
Low-power WiFi	802.11ah	single-hop	100 - 1000 m	780, 868, 915, 950 MHz	150 kb/s

Figure 3. Various technologies defined for wireless personal or body area networks (WPAN/WBAN)

The IEEE 802.11ah standard for the WLAN is developed in 2014, that operates in 900 MHz in contrast with other wireless LAN standards [11]. The main aim behind the development of this standard was to extend the range of IEEE 802.11ac standard, particularly for low power devices [12]. Utilization of

lower frequencies is not only helpful to extend the range but it has also lower consumption of power.

One of cheap technology that is also useful for a short distance is the Bluetooth. It is widely used, in various devices such as mouse, keyboard, headset and most popular for personal devices communication, for both data and voice[13]. The typical range is about 10m however it can be extend up to 100m (using amplifiers) [13]. The cipher algorithm used by Bluetooth uses stream cipher named E0, which required re-synchronization for every payload. The main parts of E0 stream cipher are (i) stream key-generator (ii) payload key-generator and the (iii) encrypt/decrypt parts [14]. There is variation in key size, that is 8 bits to 128 bits but it depends on both communicating devices. In spite of these security mechanisms, it is still vulnerable to different attacks, including Man in the middle, Blue-snarfing and Viruses [15].

The ZigBee is an extension of IEEE 802.15.4 WPAN standard developed by ZigBee Alliance. The protocol stack of ZigBee is built on the top of IEEE 802.15.4[16], as shown in *Figure 4*, which only define physical and MAC layer for low power personal area network[17]. In contrast with IEEE 802.11 WLAN it is much simpler protocol and supports multiple topologies. The main characteristic are low power, low throughput, and long battery life with secure networking (128 bit AES encryption)[18]. Its typical range is 10 to 100 meter LOS (Line Of Sight) normally depends on output power and environmental conditions. However data can be transmitted to longer distances with a mesh network.

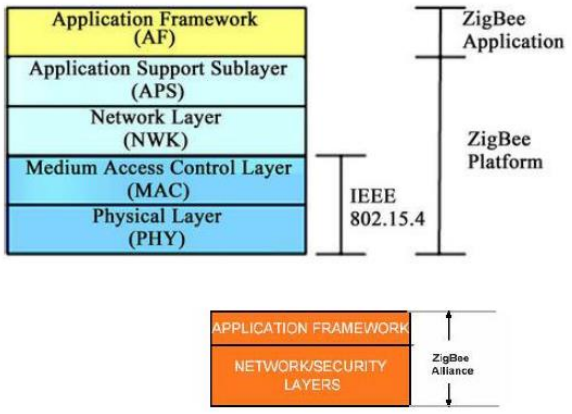

Figure 4. Layered architecture of ZigBee

The ZigBee network devices are included Coordinator, Router and End devices as shown in Figure 5. The core component of a ZigBee network is based on Coordinator, which installed initially and work as full-function device which establish and manages the whole ZigBee network. With a network there will only one Coordinator. Similarly, there will be another full function device called Router, and the major responsibility is to extend the network coverage by providing routing function. Unlike, Coordinator it is unable to establish a network by itself. The end devices, that are reduced function devices are neither similar to coordinator nor router, but they just sent their sensing data to network using Coordinator and Routers. Again, they are unable to establish ZigBee network and cannot serve or even assist in routing.

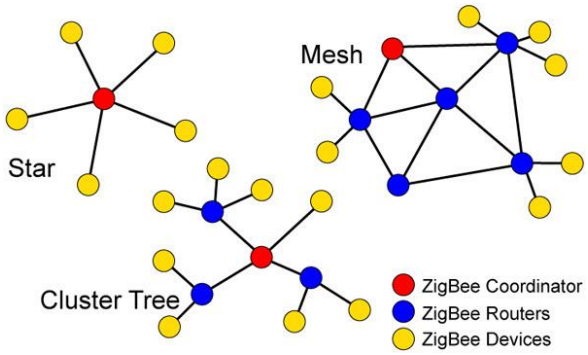

Figure 5. Topology of a ZigBee network

The Advance Encryption Standard algorithm is used in ZigBee that is based on AES-128 bit key and it provide security features on application and network layers [18]. Three different kinds of keys are used for this purpose, namely, link key, network key and Master key. The link key is utilized for data confidentiality between nodes, while, to exchange all information securely, each pair of node has a unique link key managed at application layer. The network key (which is 128 bit key) is generated by trust center that is shared among all the devices. The coordinator may become trust center or even any dedicated device. At last, the master key has prime function to secure the process of exchange the link keys between two nodes and it supposed to be preconfigured before deployment

In order to join ZigBee network each node must request current network key with the help of preconfigured master key (to avoid stealing of current network key). Network key is updated time to time by trust center and shared to all nodes by using current network key [19]. This whole security scenario works very well but it is inefficient for WBAN in term of resources (processing and power consumption). AES is a very complex encryption algorithm which requires high amount of processing and battery power (implementation of AES in small battery powered device) to encrypt the data. As mentioned in Abstract that it is infeasible to implement the conventional security mechanisms in very small resource constraint devices.

In various implementations of WBAN, AES is not used yet for security to the best of my knowledge. Because end devices of WBAN have very limited resources so it is infeasible to

implement complete AES algorithm even the CTR mode of block cipher. CTR mode is easiest to implement in contrast with other modes, but still not efficient for WBAN devices because to operate the CTR mode, still it have to perform whole AES process with certain values called Counter. Therefore, in this work, an implementation of AES counter (CTR) mode is proposed, which is feasible for resource constraint devices.

III. PROPOSED FRAMEWORK

In order to define my purposed idea it is important to get deep understanding of AES-CTR mode [20]. All modern block cipher operates in one of the five standard modes which are ECB, CBC, CFB, OFB and CTR. In CTR mode a variable called counter is initialized to IV (Initial Vector "some specified value") which is incremented linearly or randomly (with the help of some pseudo random sequence). This value is wrap around to initial value upon reaching to its maximum allowable limit. The size of the counter depends upon variant of encryption algorithm being used, like for AES-128 the size of counter is 128 bit.

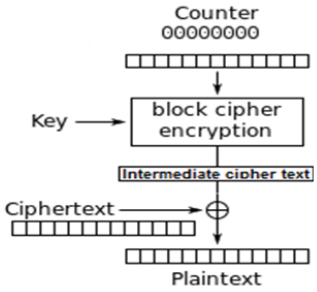

Figure 6. Basic building-block for counter mode encryption and decryption

The Figure *6* illustrates the counter mode, where the key that execute the AES process, must be shared with receiver. Initially, by using shared key it will encrypt the counter value with AES-128 encryption and produced the intermediate cipher text (this term will be used in remaining part of this article). For real time applications, if gateway router encrypts use other modes, such as CBC, so due to longer delays that will be not suitable. Additionally, the intermediate cipher texts can be computed prior to operation, or even along this process, since it depend upon counter values that can be determine earlier. The simplicity of XOR operation, provide fast logical operations that increase the efficiency of a hardware while comparing with other complex arithmetic operation [9]. Even, the proposed CTR mode uses XOR operation for real-time encryption, but it is able to achieved the security of well-established AES [20].

The thorough understanding of AES-CTR mode [20], help us to implement it. As shown in Figure *7*, e-Health server will registered a patient with a unique patient ID (PID), when he is being admitted in hospital. This information will store against that patient along with 128 bit intermediate cipher texts. Using this information, the BNC will be configured with PID and the previously generated cipher texts will now store at BNC. The additional protection through user login and password BNC will restrict any information modification or retrieval by an adversary that might reside in hospital vicinity. There will be a single BNC in WBAN for all sensors connected to a patient. It should be highlighted that noticeable that permanent memory of BNC can store up to 128 bit intermediate cipher texts. These texts will be used by BNC for data encryption thru XOR function with plain text data block. At this moment the whole BAN (comprising BNC and all sensors) will be ready for deployment.

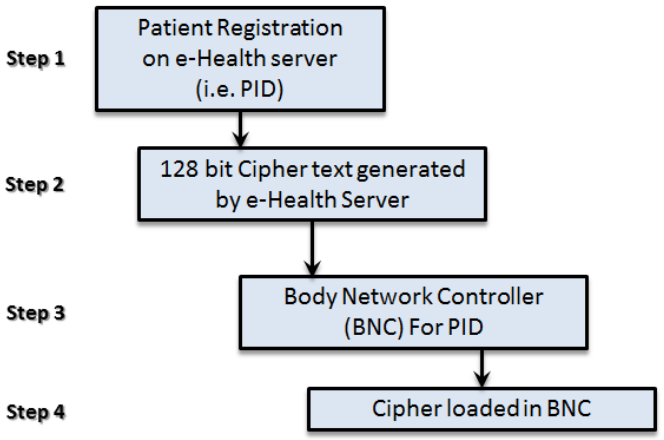

Figure 7. Flow-chart for the proposed security mechanism of a WBAN network

The symptoms of a patient will be sent by body sensors to the BNC, which in turn, aggregate the data and forwarded to the e-Health server. The BNC that is connected to e-Health server through IEEE 802.11ah access, can received data from various sensors that may capture different symptoms. Although, there will be range of sensors, but most common are the body temperature, heartbeat, respiration, blood pH and pressure etc. The Figure *8* depicts various characteristics of a patient's symptoms.

Physiological Signal	Parameter range	Data arrival time (sec)	Sample Size (bits)	Data rate (kbs)
Blood flow	1-300 ml/s	0.025	12	0.48
ECG signal	0.5-4 mV	0.002	12	6.0
Respiratory rate	2-50breaths/min	0.05	12	0.24
Blood Pressure	10-400 mm Hg	0.01	12	1.2
Blood pH	6.8-7.8 pH units	0.25	12	.048
Nerve Potentials	0.01-3 mV	5E-05	12	240
Body Temperature	32-40 ^{0}C	5	12	.0024

Figure 8. Various characteristics of a typical patient [21]

As mentioned earlier, the implementation of proposed security framework will provide confidentiality and data integrity to the communication between BNC and e-Health server. For encryption of data BNC will select an intermediate cipher text from its memory and will perform XOR operation with data as shown in Figure *9*.

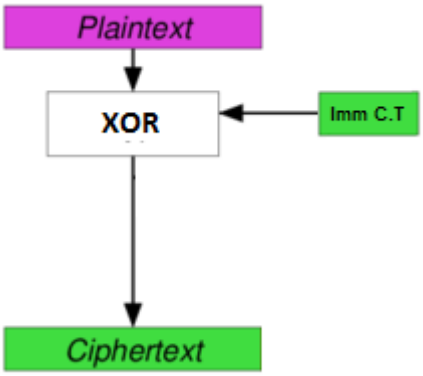

Figure 9. Data encryption through XOR operation

To provide confidentiality whole 128 bit block (10 bits for PID and remaining bits are symptoms) is encrypted with one of selected Intermediate cipher text from memory and its reference is also attached with payload. Now data block is ready to be transmitted towards server.

At this point it is briefly defined how data will be encrypted. A field named encryption ID will be attached with each PDU (Protocol Data Unit) to indicate particular intermediate cipher text which will be used to encrypt this PDU as shown in Figure 10.

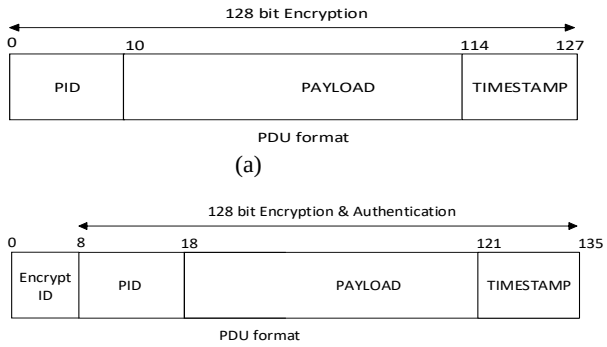

Figure 10. PDU Format (a) without ID Encryption (b) with Encrypt ID [21]

It can be seen that for selection of particular intermediate cipher text (to decrypt the PDU) the receiver will use this field. Once it will decrypted, PID at the start of payload will be checked by receiver and validate with stored PID for a corresponding BNC. This decryption will depend on successful validation otherwise it will be rejected. The receiver will be avoided from replay attack by enabling the timestamp within a PDU. Whereas, based on predefined time limit the received PDU is also validated on timestamp. It is worth to mention that before sending a packet to BNC, the server will carry-out the same procedure. To ensure availability, continuous monitoring for the arrival rate of packets of certain BNC can performed. If it does not receive packets of certain BNC within predefined limit, it will declare the emergency. The emergency indicates failure of one or more component within the network, which may include LAN switches, Access Points and BNC etc. Another important aspect is determining the failure of the sensors, it can be achieved by monitoring the status in each arriving payload. If the system do not receive any status in the payload in predefined limit (as defined in Figure *8*) it can assumed that the sensor is failed. Because when a sensor is failed it will not send data to BNC, and in turn, BNC will send all zero's bits in its associated payload slot in the subsequent packets.

IV. CONCLUSION

In this paper, different communication technologies for a smart hospital using IoT system are extensively reviewed, while the vulnerabilities for security and privacy are highlighted. The paper proposed a security framework for smart healthcare system based on wireless body area network (WBAN). It is found to be simple, more effective and low-cost implementation for the resource constrained devices, particularly in smart healthcare environment. The proposed work utilizes the well-established AES encryption algorithm in a decentralized manner, even for the resource-constraint devices. This

implementation not only fulfills the limitations of the resource constraint devices which includes less processing capability, limited battery, limited memory and hardware simplicity but also provides a well-defined security mechanism which is the prime requirement of today's networks. The proposed framework not just reduces the complexity for resource constrained devices, but ensures the availability and data integrity in simple, yet effective manner.

REFERENCES

[1] L. Atzori, A. Iera, 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, W. Qin, "Iot gateway: Bridging wireless sensor networks into internet of things," in *Embedded and Ubiquitous Computing (EUC), 2010 IEEE/IFIP 8th International Conference on*, pp. 347-352, 2010.

[3] H. Fotouhi, A. Cauevic, K. Lundqvist, "Communication and Security in Health Monitoring Systems--A Review," in *Computer Software and Applications Conference (COMPSAC), 2016 IEEE 40th Annual*, pp. 545-554, 2016.

[4] P. Hamalainen, T. Alho, M. Hannikainen, T. D. Hamalainen, "Design and implementation of low-area and low-power AES encryption hardware core," in *9th EUROMICRO Conference on Digital System Design (DSD'06)*, pp. 577-583, 2006.

[5] D. Boyle, T. Newe, "Security protocols for use with wireless sensor networks: A survey of security architectures," in *Wireless and Mobile Communications, 2007. ICWMC'07. Third International Conference on*, pp. 54-54, 2007.

[6] E. Jovanov, A. Milenkovic, C. Otto, P. De Groen, B. Johnson, S. Warren, G. Taibi, "A WBAN system for ambulatory monitoring of physical activity and health status: applications and challenges," in *2005 IEEE Engineering in Medicine and Biology 27th Annual Conference*, pp. 3810-3813, 2006.

[7] M. Ghamari, B. Janko, R. S. Sherratt, W. Harwin, R. Piechockic, and C. Soltanpur, "A survey on wireless body area networks for ehealthcare systems in residential environments," *Sensors*, vol. 16, p. 831, 2016.

[8] S. Saleem, S. Ullah, H. S. Yoo, "On the Security Issues in Wireless Body Area Networks," *JDCTA*, vol. 3, pp. 178-184, 2009.

[9] K. Tiri, I. Verbauwhede, "A logic level design methodology for a secure DPA resistant ASIC or FPGA implementation," in *Proceedings of the conference on Design, automation and test in Europe-Volume 1*, p. 10246, 2004.

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

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

[12] W. Sun, M. Choi, 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.

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

[14] C. T. Hager, S. F. MidKiff, "An analysis of Bluetooth security vulnerabilities," in *Wireless Communications and Networking, 2003. WCNC 2003. 2003 IEEE*, pp. 1825-1831, 2003.

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

[16] J.-S. Lee, Y.-W. Su, 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*, pp. 46-51, 2007.

[17] G. Mulligan, "The 6LoWPAN architecture," in *Proceedings of the 4th workshop on Embedded networked sensors*, pp. 78-82, 2007.

[18] P. Baronti, P. Pillai, V. W. Chook, S. Chessa, A. Gotta, 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.

[19] N. Vidgren, K. Haataja, J. L. Patino-Andres, J. J. Ramirez-Sanchis, 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*, pp. 5132-5138, 2013.

[20] H. Lipmaa, P. Rogaway, D. Wagner, "CTR-mode encryption," in *First NIST Workshop on Modes of Operation*, 2000.

[21] J. Y. Khan, M. R. Yuce, "Wireless body area network (WBAN) for medical applications," *New Developments in Biomedical Engineering. INTECH*, 2010.