Challenges in Wireless Body Area Network

Muhammad Asam[1], Tauseef Jamal[2], Aleena Ajaz[6]
PIEAS University, Islamabad, Pakistan

Muhammad Adeel[3], Areeb Hassan[4]
Superior University
Lahore, Pakistan

Shariq Aziz Butt[5]
The University of Lahore, Pakistan

Maryam Gulzar[7]
The University of Lahore,
Software Engineering Dept., Pakistan

***Abstract*—Wireless Body Area Network (WBAN) refers to a short-range, wireless communications in the vicinity of, or inside a human body. WBAN is emerging solution to cater the needs of local and remote health care related facility. Medical and non-medical applications have been revolutionarily under consideration for providing a healthy and gratify service to humanity. Being very critical in communication of the data from body, it faces many challenges, which are to be tackled for the safety of life and benefit of the user. There is variety of challenges faced by WBAN. WBAN is favorite playground for attackers due to its usability in various applications. This article provides systematic overview of challenges in WBAN in communication and security perspectives.**

Keywords*—WBAN (Wireless Body Area Network); denial of service attacks; resource management; cooperation; security

I. Introduction

Wireless communication brought numerous benefits to our society. Technology up gradation has made this communication possible by the help of 4G, LTE-A, 5G and so on. Recently, Machine to Machine (M2M) communication has been a favorite area of research in past few decades. Communication between machines and the human was next destination. T.G. Zimmerman proposed Personal Area Network (PAN) [1]. Low power, lightweight and miniature physiological sensors has made it possible to connect them to form a Body Area Network (BAN). This connection is supplemented by the wireless technology and the WBAN is formed. This network represent the natural union between connectivity and miniaturization [2].

WBAN comprises multiple sensors. These sensors sample, process and communicate vital sign like heart beat rate, vascular blood pressure and or blood oxygen saturation. Same can be done by the sensors for environmental parameters like location, temperature, humidity and light. These sensors as an attachment with the body and sometime within the clothes. Implants inside the body are getting more attention [3].

Communication network in WBAN can be divided into two major parts or tiers, one is the communication between the sensors and the second is the distribution network as shown in the Fig. 1 [4]. Three-tier architecture is mostly agreed upon by inserting another layer of communication between WBAN coordinator and WBAN gateway or sink node.

In the remaining section describe the architecture of WBAN, while Section 2 details its applications. In Section 3, explain major challenges faced by WBAN. Section 4 discusses the open research issues and our findings in this area.

WBAN communication commonly comprises of three tiers communications as shown in Fig. 2 [5].

- First tier of WBAN architecture is realized by body sensor units which are placed outside or inside of human body. These sensors are responsible for detecting the physiological data signals, converting the signals to digital form and then transmitting through wireless media it get from human body. Then sends it wirelessly to the next tier. This communication is also referred as intra-BAN communication.
- Second tier is comprised of personal server units. These units get data from sensors and process it. This tier formats the processed results to convey to the upper, third tier if necessary. Communication with both the first and third tier is done wirelessly. This communication is also known as inter-BAN communication.
- Third tier comprises of user machines, where end users are data experts who can take some decision, or can conclude some results from this data. This inference may be about someone's health in hospital or at home. It may be sending some caretaker or ambulance to the patient. It may be about taking some specific diet for sportsman. It may be about some artillery movement command from the army head quarter.

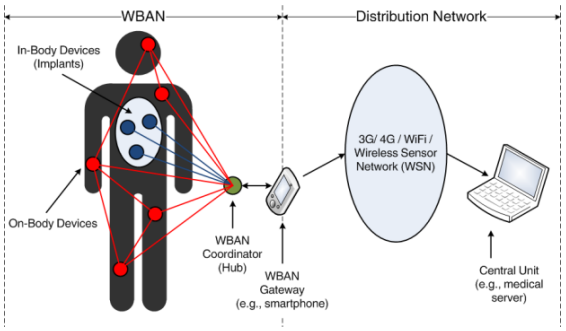


Fig. 1. Two Tier Architecture for WBAN [4].

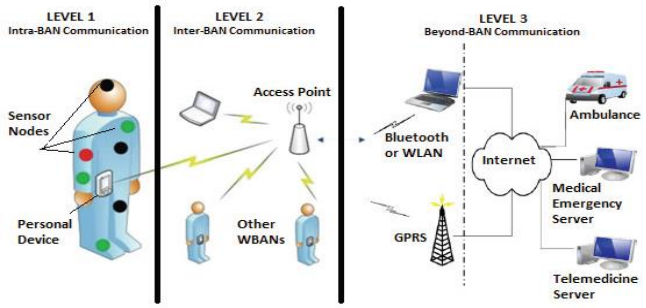


Fig. 2. Three Tier Architecture for WBAN [5].

Despite of the two-tier and three-tier architecture, can be distinguish WBAN entities into two major categories, sensor node and sink or gateway node. Former entity is responsible for data collection from the human body through sensors while the later entity sends it to other servers and communication networks. These communication networks can be mobile network, WLAN, hospital, military's base station or sports training center, etc.

IEEE 802.15.6 on the other hand is an international standard for WBAN, specifies the wireless communications near body or inside the body. It provides low power, short range, and extremely reliable wireless communication within the surrounding area of the body. Different applications can enjoy a vast range of data rates. This standard specifies the wireless communications in the vicinity of body or inside the body. This standard is not limited to humans only but could support any living or non-living thing. It defines the Physical (PHY) and Medium Access Control (MAC) using the frequency bands which are approved by regulatory authorities. This standard considers effects on portable antennas due to the presence of a person (varying with male, female, skinny, heavy, etc.), radiation pattern shaping to minimize the Specific Absorption Rate (SAR) into the body, and changes in characteristics as a result of the user motions. In the next section explained detailed some of its applications.

II. Applications

There are many useful and innovative applications of WBAN. As the WBAN is closely attached to acquire the body parameters so its most favorite applications are in medical field. We classify these applications into two broad categories, i.e. Medical and Non-Medical applications (c.f. Fig. 3).

A. Medical Applications

- A number of sensors are attached to the body like ECG, pulse oxi meter and heart beat sensor on the patient's body. These sensors used to immediately inform the corresponding medical staff about the irregularities and heart rate in advance.
- Cancer can be detected by the help of nitric oxide. Sensor is attached to the affected area, which has the ability to detect nitric oxide emitted from cancer cells.
- WBAN helps to monitor and track the patient's movement which is necessary in home based rehabilitation scheme.
- Allergic sensors used to automatically detect the allergic agents in the air and will immediately report it to the patient or his physician.
- Implanting a bio-sensor in the patient's body to monitor the glucose level and inject insulin automatically when the glucose level is at a certain threshold.
- The solution to all these problems is placing the ambient sensors at home to measure the physiological data of the patient. This data is stored or transmitted to a control unit/healthcare center in regular intervals. This helps the patients to stay at home and get continuous healthcare support without visiting the hospital. Moreover, these sensors, placed on the patient's body, will raise an alarm or urgent notification to the nearby healthcare center in case of any emergency.
- Telemedicine helps remote diagnosis and treatment of patients using telecommunication technologies. WBAN technology can used in telemedicine sector by online consultation of patients with their doctors, transmission of the patient's medical reports and remote medical diagnosis (c.f. Fig. 4).

B. Non-Medical Applications

- Heart rate sensors along with some additional sensors can be used to provide information like speed, body temperature, heart rate, oxygen level, timer and location.
- WBAN can be used to safeguarding the personnel like soldiers, policemen and firefighters. Sensors can be placed on their uniforms in order for them to attain facilities. The WBAN sensors can monitor the level of toxics in the air and warn the firefighters or soldiers if a life-threatening level is detected. WBAN sensors can also monitor health of the uniformed personnel especially soldiers who need medical assistance during war.

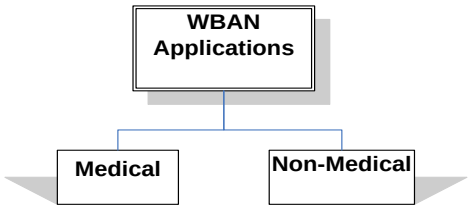


Fig. 3. WBAN Applications.

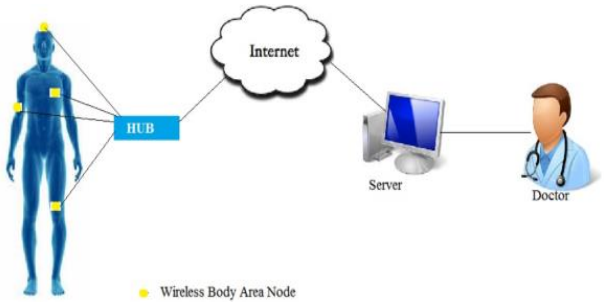


Fig. 4. Application of WBAN in Telemedicine.

III. Challenges in WBAN

Effectiveness of the WBAN is important from both patients and healthcare perspective. As the time passes, challenges to the emerging technologies increases along with the advancements. There is variety of challenges faced by WBAN as explain below. These challenges are classified in six major classes such as energy, mobility, security and communications (i.e., networking, QoS and cooperation), as shown in taxonomy provided in Fig 5. Security is the major issue need to be tackle in parallel with any of other issues.

A. Energy Requirements

Since, most of the devices in WBAN are using the wireless medium, therefore they are portable. Such devices are small in size and carry power source too. Hence, the power is always limited. Wireless natures made them roam free, meaning the devices are free to move. So the power to the device of the network is provided with the help of batteries. Things are not simplified by allowing the power from battery but is encompasses some more challenges of power management of the battery supplies especially in case of implants. Since the sensors that are implanted in the body are so small that the battery cannot sustain more than a month [6]. Removing the implants and re-installation require even more management of the complications generated. Different parameters that alter the power consumption include communication bandwidth and processing power. So there is need to have better scheduling algorithm along with better power management schemes.

Different equipments and sensors for monitoring the body parameters are called body nodes. Each body node has different power consumption profile. To entertain all the body nodes, a reasonable power source is required to work effectively. As a rough estimate, weight of the battery is directly proportional to the power of it. So we may not increase the weight to increase the power as it is to be carried out by the human body and the case is more severe if it is to be implanted inside.

Energy harvesting technique is one solution to the power issue [7]. Energy present in the vicinity of the nodes is converted into electrical energy by the help of specific devices or techniques. The energy harvesting can eliminate the batteries charging either full or partial, based on technique. Such solutions are more clean and green. Vibration, electrostatic, electromagnetic, solar, thermoelectric, pyro and kinetic energy are candidates for harvesting.

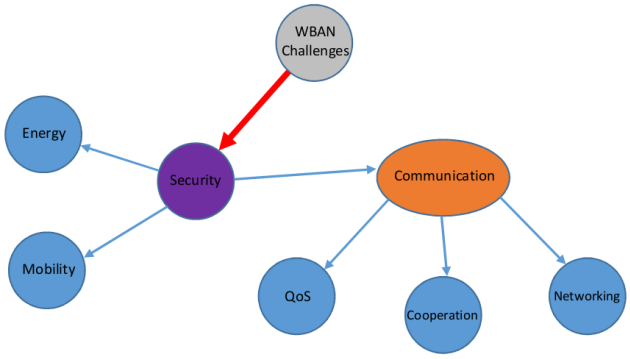


Fig. 5. WBAN main Challenges.

B. WBAN Security

In any network, communication data is of worth importance. In case of WBAN, it becomes more critical as it has been connected to the Physical system. These communication channels are very much visible to the attacker and if not securely implemented it could any of the attack including eavesdropping on traffic between the nodes, message injection, message replay, spoofing and off course compromise the integrity of physical devices. Upon successful attack, such actions not only invade privacy but may lead to catastrophic situation [8, 11]. As reported in Healthcare IT news in February, 2014, hackers accessed a server from a Texas healthcare system, compromising the protected health information of some 405,000 individuals, which was one of the biggest HIPAA security breaches. Even worse, it was demonstrated that implantable cardiac devices can be wirelessly compromised [5]. Security measures are necessary to protect the users from potential risks. Security architecture for WBAN is more challenging than other networks. Efficiency, scalability and usability are performance requirements for the security architecture for WBAN. Regardless of the architecture of the WBAN can coarsely divide the communication into two parts, internal communication between WBAN and external communication between WBAN and external users.

1) Security requirement in internal communication

It includes the following:

- Data authenticity means that data is coming from the claimed source. An attacker may inject bogus data into the WBAN. Public key cryptography schemes are used for data authenticity
- Data confidentiality leads to information disclosure to unauthorized entities. Encryption is also done to achieve this.
- Data integrity is achieved through Message Authentication Code (MAC) or by the help of hashed MAC. Integrity is made sure by doing the reverse process of generating the authentication codes.
- Data availability is the most pervasive security requirement for WBAN. Due to its criticality of the physical system in WBAN, availability of data is made sure. Denial of Service (DoS) attack is the favorite place for the attackers over here.

Along with completing the security requirement, WBAN protocols must be efficient enough to fulfill its desired mandate. In [9, 10], the authors suggested secure and reliable routing framework for WBAN. They demonstrated that it can significantly counter the data injection attacks.

2) Security requirements in external communication: Utility of WBAN in healthcare system may include the self-monitoring patients, network service provider for data transmission, application support and local/remote personnel who offer medical services. Considering the privacy and significance of patient-related data and medical messages, WBAN may suffer threats such as message modification and

unauthorized access. It is desirable that proper security mechanism should be considered for securing the communication between WBAN and external users, where each user must prove their authenticity and then access the data according to their privileges.

WBAN is suitable and useful for different applications and solution. So it is found favorite playground for attackers. One of the classifications of attack is four part communication implementation stack namely PHY layer, MAC layer, network layer and transport layer attacks.

- Being the radio frequency based, PHY is more prone to attacks like tempering and jamming. In jamming attack, attacker transmits radio signal of random frequency. This signal interferes with the other sensor signals. Eventually, node in the range of the attacker cannot communicate message and become isolated. In tampering attack, the cryptographic keys and even program code can be tampered.
- MAC is dealing with the frame detection, multiplexing and channel accesses. Collision attack at this layer may cause in exponential rise in back-off packet in certain protocols. MAC schemes can be interrupted at this layer to cause unfairness attack. Continuous transmission of corrupted packets may result in DoS.
- In WBAN, routing is carried through the coordination of nodes. A compromised node in a network can spoof, alter or replay the routing facts for the network. Sometime the attacker node may selectively route the packets in the network causing selective forwarding attack. A malicious node may attract all the traffic in the network to itself by claiming it to be the best coordinator in the network. It can do alteration with the data received once it is recognized as best data exchange. A single node may pose to have multiple network identities. This results in Sybil attack. An attacker may send a hello message powerful enough to be selected by the nodes to route their messages. This arise the hello flood attack as shown in Fig. 6.
- End to end connection between the nodes are managed at transport layer. An attacker may send a lot of requests to establish the connection to use its all resources. This results in restricting making legitimate connections of the nodes. This is known as flooding attack. An attacker in de-synchronization attack sends fake control flags or sequence number to both nodes in an active connection.

C. Mobility Support

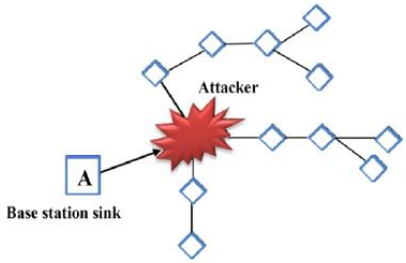
WBAN provides two major advantages, i.e., portable monitoring and location independence. Regardless of the application, these are the key factors due to which WBAN is potential candidate in many venues. But these two advantages put some special limitations i.e., mobility. Mobility can pose serious problem in some application like E-Health care even posture do effect the communication [12].

The mobility is defined between the user and the WBAN as a seamless link. One of the major issues is to reach to sink, which may be single or multi hop. Collier et al. in [13] show that may not stick to single strategy and can find which one is better for the particular case. The same may be applied to optimize the hop count. M. Shanmukhi et al. in [14] proposed a TDMA technique for MAC protocol. Message is flooded to all nodes to reach sink node and the path with minimum delay is selected. Reliable multipath routing is another solution proposed by Birgani et al. in [15]. A path list is maintained depending upon different factors of the routing and the link is established accordingly. Braem et al. in [16] proposed Loose association Implicit reservation Protocol for Mobile WBAN. It works on one hop communication model and has less delay.

D. Quality of Service

Quality of Service (QoS) is the requirements fulfilled by system as requested by the users. For more life critical system, timeliness may be the parameter for the quality. System, that cannot fulfill the said requirement, falls short of providing the QoS. Same is true for other factors like bandwidth, latency, jitter, robustness, trustworthiness, adaptability [17]. Similarly, seamless roaming and end to end wireless connection between the body nodes and the sink nodes is another QoS factor [18].

It is of worth mentioning that system may not be able to fully provide the requested services but the goal of the quality of service may be categorized to Soft QoS, Hard QoS and even no QoS [19]. Challenges to QoS centric WBAN system may be categorized as shown in the



Hello Flood, A Network Layer Attack.

[20, 21].

E. Cooperation between Nodes

When the intermediate nodes help source destination pair in communication, the cooperation occurs. The intermediate nodes may refer as helper or relay as shown in Fig. 7 [22]. Cooperation offers a good solution for many of the limitations in WBAN such as distance, mobility, coverage and channel impairments.

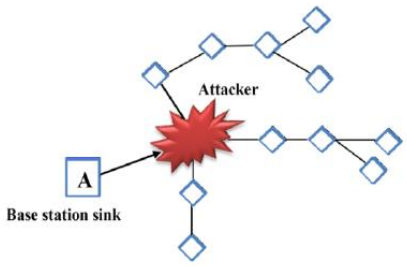


Fig. 6. Hello Flood, A Network Layer Attack.

TABLE. I. QOS PARAMETERS

Parameters for QoS
Limited resources and Capabilities
Scalability
Multi-source multi-sink systems
Node deployment
Dynamic network topology
Various types of applications
Various traffic types
Wireless link unreliability
Real-time system
Data redundancy

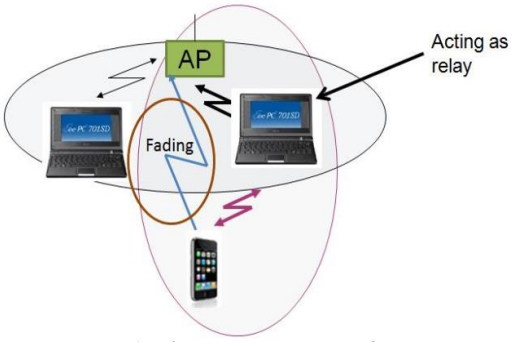


Fig. 7. Cooperative Networking System.

However, introduction to cooperation may leads to additional blockage and overhead. Which limit its benefits and affects the resource management [23].

Communication via relay can add additional interference as well. Therefore, cooperation communication protocols must be devised in way to incur less overhead and interference.

Another issue with cooperation is relay selection. Normally relays are pre-selected, which is based on historic information [24]. Therefore, such relays are not suitable for mobile scenarios. Also, selecting malicious node as relay can make it is easy to launch any attack.

F. Networking Issues

As the size of network grows, it mainly affects the routing protocols performance and throughput of the network. Bandwidth utilization also suffers from links sharing in each connected node; this is one of major cause of slow routing in homogenous channelization.

- Self organization of Mobile nodes in Ad-hoc networks is one of challenging research problem in the context of efficient routing protocols. Multi hop routing is also a promising solution when source and destination are not directly connected to each other. The challenges due to routing protocols are dynamic topology, re-configuration and management, monitoring free, no centralized control, and scalability.
- Multicast routing is a promising solution in ad hoc networks due to frequent attachment and detachment of mobile nodes. Multicast routing is getting special attention in ad hoc networks due to its suitability for link efficiency and central broadcast. Challenges faced by multicasting are lack of QoS, low scalability, frequent updates, delay tolerant multicasting etc.
- The major limitations in WBAN come from limited resource devices and shared medium [25].

MAC layer is very important since it communicate with next hop and access the medium. Therefore, collisions, contention and resource blockage could be handled in case of efficient MAC layer schemes. Hence, backoff algorithms, Carrier Sence Multiple Access (CSMA), contention windows and handshaking need attention while devising MAC protocol for WBAN specially when there is ad-hoc connectivity.

IV. Discussion

This article discussed how different factors affect the performance of the WBAN, its related work and its challenges.

Since health is top priority for all of us. Making the health systems efficient and affective can benefit the human society. Compromising a node could even result in loss of lives (humans or animals). Therefore, security is the utmost challenge for such systems. As a summary, security is needed to be addressed at every level.

The security mechanism must be light weight, since have limited resources. There are various kinds of attacks that can be launched in e-health systems. This could be passive i.e. regarding patients' data confidentiality etc., or active i.e., DoS etc. Issues related to DoS attack is explained below:

A. Denial of Services

Whenever the requested resource is not granted within due time, it can say DoS attack is occurred. DoS attack can active or passive. In former case the attacker launches the attack, while in later case there is depletion of resources. Therefore, DoS attack is very critical to WBAN systems. It can avoid active attacks but better intelligence is required for mitigating the passive attacks such as lazy node behavior etc. There is need to improve the performance of overall network in order to avoid such passive DoS attacks. That's why it can be very easy for adversary to launch DoS attack, as well as it can be launch by itself from inside the network. Therefore, it is very important to design better solutions for handling DoS. This is an open research area within e-health systems.

Most of the attacks we discussed in this paper are kind of active DoS attacks, as shown in Fig. 8.

As discussed earlier, MAC layer is important in term of resource managements. Therefore, depletion of resources leads to DoS attack. One of the solutions in this regard is cooperation, as explained below.

B. Cooperation

As explained earlier, cooperation offers good solution for many problems rises in wireless networks. One of the main advantages is always-connected situation. With the cooperation it can be ensure that patient is always connected even in case of disaster or loss of infrastructure.

Multiple relays assisting source-destination pair could allow higher diversity gain, which could increase the reliability. This way it can achieve performance gain equal to Multiple Input and Multiple Output (MIMO) using single antenna devices without any additional hardware. Cooperation

can also mitigate effects of mobility such that in case of handover or ping pong movement. However, sending data frames via intermediate nodes are not always secure. The relay node may be malicious or its unavailability may lead to DoS itself. Hence, cooperation might itself become security risk.

In our opinion, there is need of good cooperative networking protocol at MAC layer to enable cooperation in case of link failure. Such protocol must be light weight and based on current channel information. Such cooperation can be used instead of layer 3 path re-computation (c.f. Fig 9).

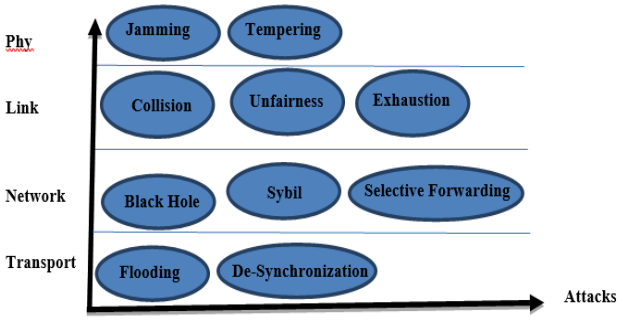


Fig. 8. DoS Attacks on WBAN.

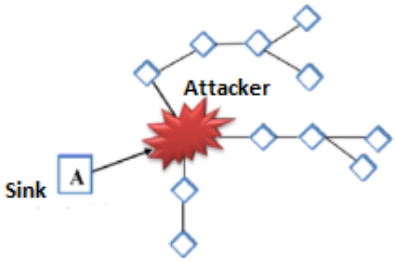


Fig. 9. Attack Mitigation via Cooperation.

V. Conclusions and Future Work

WBAN provides monitoring of human health systems weather inside or outside. However, this is new technology and research is needed to address the conflicting challenges. In this paper we discussed various issues and proposed some taxonomies. However, these issues are categorized into two types: (i) Cooperation and (ii) Security issues.

Security issues need to be tackle at every layer and scenarios of eHealth systems. Similarly, all the networks related issues such as mobility, QoS, energy, routing, and distance could be resolved via cooperation. Cooperation on the other hand adds additional interference, blockage and overhead.

Therefore, in future work we will propose cooperative relaying solution for WBAN to address most of the inherit issues [26]; similarly, as a part of effective security mechanism on various kind of DoS attack's detection and mitigations.

References

[1] T. G. Zimmerman, "Personal AreaNetworks: Near-fieldintrabodycommunication," IBM SYSTEMS JOURNAL, vol. 35, 1996.

[2] M. A Kavitha and S. A Sendhilnathan, "Body area network with mobile anchor based localization," Cluster Computing, pp. 1-10, 2017.

[3] SA Butt, and T. Jamal, "Study of Black Hole Attack in AODV", in Proc. of International Journal of Future Generation Communication and Networking, Vol. 10, No.9, pp. 37-48, 2017.

[4] M. A.-u. Deena M. Barakah, "A Survey of Challenges and Applications of Wireless Body Area Network (WBAN) and Role of A Virtual Doctor Server in Existing Architecture," 2012.

[5] H. S. Sangha and H. Sohal, "Power Challenges in Wireless Body Area Network for Mobile Health Powered by Human Energy Harvesting," vol. 9, December 2016.

[6] A. D and K. K. Venkatasubramanian, "Biomedical devices and systems security,," USA, September 2011.

[7] X. L. X. Liang, Q. Shen, "Exploiting prediction to enable secure and reliable routing in wireless body area networks," 2012.

[8] X. L. M. Barua, R. Lu et al., "Peace: an efficient and secure patient-centric access control scheme for ehealth care system," in Proceedings of the Computer Communications Workshops (INFOCOM WKSHPS), IEEE Conference, 2011, pp. 970-975.

[9] N. Z. C. Hu, H. Li, X. Cheng, and X. Liao, "Body area network security: a fuzzy attribute-based signcryption scheme," IEEE Journal on Selected Areas in Communications, vol. 31, pp. 37-46, 2013.

[10] M. G. Nabi, MCW. Basten, AA., "MoBAN: A Configurable Mobility Model for Wireless Body Area Networks," March 2011.

[11] T. Jamal and Z. Haider, "Denial of Service Attack in Cooperative Networks", in Proc. of ArXiv, arXiv: CoRR Vol. arXiv:1810.11070 [cs.NI], Oct. 2018.

[12] C. J. M. Shanmukhi, "A Review on Mobility Feature in Wireless Body Area Networks," vol. 6, June 2017.

[13] Y. Birgani, N. Javan, and M. Tourani, "Mobility enhancement of patients body monitoring based on," Indonesia, May 2014.

[14] B. Braem and C. Blondia, "Supporting mobility in wireless body area networks: An analysis," Ghent, Belgium, November 2011.

[15] Butt, S. A., Diaz-Martinez, J. L., Jamal, T., Ali, A., De-La-Hoz-Franco, E., & Shoaib, M. (2019, July). IoT Smart Health Security Threats. In 2019 19th International Conference on Computational Science and Its Applications (ICCSA) (pp. 26-31). IEEE.

[16] A. C. W. W. Okundu Omeni, Alison J. Burdett, and Christofer Toumazou, "Energy Efficient Medium Access Protocol for Wireless Medical Body Area Sensor Networks," IEEE Transactions on Biomedical Circuits and Systems, vol. 2, 2008.

[17] M. Asam and Z. Haider, "Novel Relay Selection Protocol for Cooperative Networks", in proc. of ArXiv, arXiv:1911.07764 [cs.NI], November 2019.

[18] N. U. Shah Murtaza Rashid Al Masud, P.O. Box 1988 and S. A. Najran, "QoS Taxonomy towards Wireless Body Area Network Solutions," International Journal of Application and Innovation in Engineering Management vol. 2, April 2013.

[19] T. Jamal, and SA Butt, "Malicious Node Analysis in MANETS", in Proc. of International Journal of Information Technology, PP. 1-9, Springer Publisher, Apr. 2018.

[20] T. Jamal, P. Mendes, and A. Zúquete, "Relay-Based Cooperative MAC Protocol," in MAP TELE Porto, Portugal, June, 2013.

[21] T. Jamal, P. Mendes, and A. Zúquete, "Analysis of Hybrid Relaying in Cooperative WLAN," in IEEE/IFIP WirelessDays, Nov. 2013.

[22] T. Jamal, P. Mendes, and A. Zúquete, "Relayspot: A Framework for Opportunistic Cooperative Relaying," in IARIA ACCESS, Luxembourg, June, 2011.

[23] T. Jamal, P. Amaral, and A. Khan, "Denial of Service Attack in Wireless LAN," in ICDS, Rome, Italy, 2018.

[24] T. Jamal and M. Alam, "Detection and Prevention Against RTS Attacks in Wireless LAN," 2018.

[25] Z. Haider and K. Ullah, "DoS Attacks at Cooperative MAC", in Proc. of ArXiv, arXiv:1812.04935 [cs.NI], Dec. 2018.

[26] Butt, S. A., Jamal, T., Azad, M. A., Ali, A., & Safa, N. S. (2019). A multivariant secure framework for smart mobile health application. Transactions on Emerging Telecommunications Technologies, e3684.