Malware Detection and Challenges in WBAN

Authors: Musadiq Umair (Uni Derby)

musadiqumair889@gmail.com

Federal Institute de Jeneiro.

Abstract---- The popularity of smartphones has led to an increasing demand for health apps. As a result, the healthcare industry is embracing mobile technology and the security of mHealth is essential in protecting patient's user data and WBAN in a clinical setting. Breaches of security can potentially be life-threatening as someone with malicious intentions could misuse mHealth devices and user information.

1. Introduction:

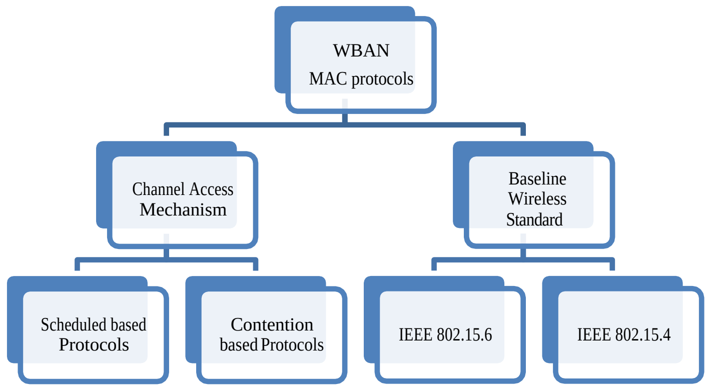
WBANs are of the promising technologies, applied in the e-healthcare systems, for extracting and transferring critical medical data from patient body. In WBANs, the privacy and integrity of the patient's private medical data are very important, as a result, the WBANs communications and even communication with other E-Healthcare components should be authenticated and secured. This paper provides a complete survey and analysis of the various authentication schemes proposed in the literature to improve the WBANs security. Besides, it classifies the proposed authentication schemes based on the applied techniques for authentication and illustrates each scheme in detail. Furthermore, it highlights the advantages and limitations of the authentication schemes and presents a comprehensive comparison of their capabilities and features.

Scheduled Based Protocols: In these protocols, one of the nodes is categorized as the coordinator, which ensures that all the nodes get an equal access to the wireless channel. In this way the nodes do not have to compete for the channel access as all them get a specified time resulting in time synchronization. Due to this, collision and overhearing problems are avoided.

Contention Based Protocols: In these protocols, the nodes access the wireless channel without being pre-coordinated i.e. Nodes are not given a predefined time for the channel access. They check whether the channel is idle or not for the transmission. In these protocols, packet collisions are very common due to the absence of time synchronization.

The latest WBAN standard is defined in IEEE 802.15.6, including the physical and MAC layer. This standard defines the access mechanisms: Random Access Mechanism, which includes Slotted Aloha and

CSMA/CA Access Mechanisms, Scheduled and Scheduled Polling Access Mechanism and Improvised Access Mechanism.



1.1.1 ***Fig.1.1 Classification of MAC Protocols***

2. Channel Access Mechanism

2.1.

2.2. Scheduled Based Protocols:

- **H-MAC:** Heartbeat MAC is scheduled based protocol. It is an energy efficient protocol which synchronizes the time by using heartbeat rhythm information. One of the features of this protocol is that it decreases the extra energy which is required for synchronization. It is best for one hop topologies as it considers the time slot for this topology. [1]

- **Body-MAC:** It is a scheduled based protocol which is a TDMA based protocol. It reduces the collision, idle listening and overhearing by using a technique in which it divides the MAC frame. It divides the frame into three parts known as Beacon, Downlink and Uplink. The Beacon frame is used for synchronization. The Downlink frame is used for transmission from the gateway to the nodes. The Uplink frame is further categorized into **CFP** (Contention Free Period) and **CAP** (Contention Access Period). CAP competes for the control of transmission of data packets and CFP allocates the time slots to nodes. In this protocol the energy is saved by the nodes using sleep mode when no data is being transmitted. [2]

- **Med-MAC:** It is a TDMA based protocol which handles the network traffic by adjusting time slots and Quality of Service requirements. It provides schemes such as synchronization which provides channel access on various channels [1]. This protocol provides flexibility along with low energy consumption and it also handles emergency traffic. [2]

- **U-MAC:** Urgency MAC is also a scheduled based protocol but it is priority based protocol used in medical applications. It basically divides the collected data into sublevels so that the important medical data can be transmitted before. In this protocol the access mechanism used is Slotted Aloha in which the sensor node competes for the channel at the starting of the time slot in a MAC frame.

- **AR-MAC:** It is called adaptive reliable MAC protocol which is TDMA based. In this protocol, each node is given GTS (Guaranteed Time Slots) for the communication in this way the collision and overhearing is avoided which results in decreasing the energy consumption of the nodes.
- **A-MAC:** It is called the adaptive MAC which is a TDMA based protocol. It is just like AR-MAC protocol. It reduces the energy consumption by limiting the channel access. It uses adaptive time slot allocation for allocating the time slots to the nodes.

2.3. Contention Based Protocols:

In these protocols, there is no time synchronization i.e. nodes are not given a pre-defined time for channel access. Nodes have to compete for the channel access.

- **CSMA/CA:** Carrier Sense Multiple Access with Collision Avoidance is a protocol in which the nodes listen to the shared medium to check whether or not the channel is idle. If the channel is idle, the nodes start the transmission of data packets. In this way the collision is avoided as the nodes check the medium before transmission.

- **S-MAC:** Sensor MAC is a contention based protocol which listens to the medium to check whether it is idle or not. If the medium is idle, a node sends a **SYNC** (Synchronization) packet along with a schedule containing information about listen and sleep periods. The nodes listening to the sending node, adopt this schedule. All nodes keep the schedule of their neighbors in a table. During the listening periods, the sending node transmits a **RTS** (Request to Send) frame and the receiver will acknowledge it with a **CTS** (Clear to Send) frame. The nodes not participating in this communication will go in the sleep mode. Due to the sleeping feature, the energy consumption is decreased which proves the protocol to be very useful in WBAN.

- **B-MAC:** Berkeley MAC is also a contention based protocol which reduces idle listening which is one of the major causes for energy consumption in protocols. In this protocol the nodes wait in a back-off time to send a packet. The nodes basically checks whether the channel is idle or not after waiting in a back-off time. If the channel is idle, the nodes transmit packets. If it is not idle, the node waits in a second back-off time. The nodes periodically check the channel using LPL (low power listening). If the channel is clear but the node do not have any data to send then the node goes back to sleep. This protocol does not use control frames like RTS, CTS or ACK and it has no synchronization.

- **PW-MAC:** Predictive Wakeup MAC is a contention based protocol which avoids idle listening and overhearing by using pseudo random scheduling. When a node wakes up it sends a small beacon to alert other nodes that it has woken up. Basically the sender predicts wakeup time of the receiver on the basis of pseudo random wakeup schedule generator. In this way the energy consumption of the sender is reduced due to the prediction made by the sender and it goes to sleep till the receiver wakes up. [3]

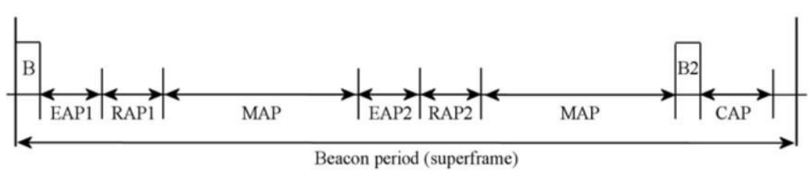
2.4. WBAN MAC Standards:

2.3.1. IEEE 802.15.6:

This is a standard of WBAN, which defines the physical and MAC layer. Following are the communication modes of the standard IEEE 802.15.6.

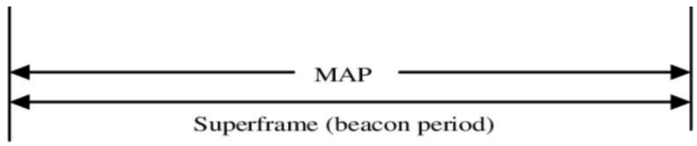
Beacon Mode with Super-frame Boundaries: The superframe structure consists of beacon frames, exclusive access phases (EAP1 and EAP2), random acess phases (RAP1 and RAP2), managed access phase (MAP), contention access phase (CAP) and B2 frames as shown in figure. The EAPs are used for the transfer of high priority emergency traffic. The RAPs and CAP are used for regular traffic. The MAP period is used for scheudled and unscheuled access. B2 frame is used to provide non zero length CAP [4].

In this communication mode, beacon frames are transmitted by the hub in active superframes to communicate superframe boundaries. There may be many continuous inactive superframes after active superframes in which the hub doesn't send any beacons.



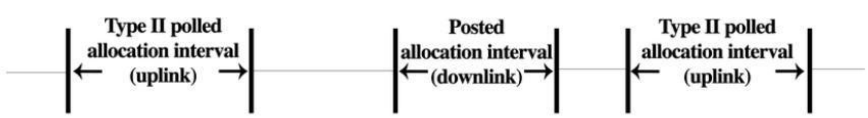
1.1.2 ***Fig 2.1 Beacon Mode with Super-frame Boundaries*** *[5]*

Non Beacon Mode with Super-frame Boundaries: In this communication mode, the hub uses managed access phase (MAP) without using beacons. [6]



1.1.3 ***Fig 2.2 Non-Beacon Mode with Super-frame Boundaries*** *[7]*

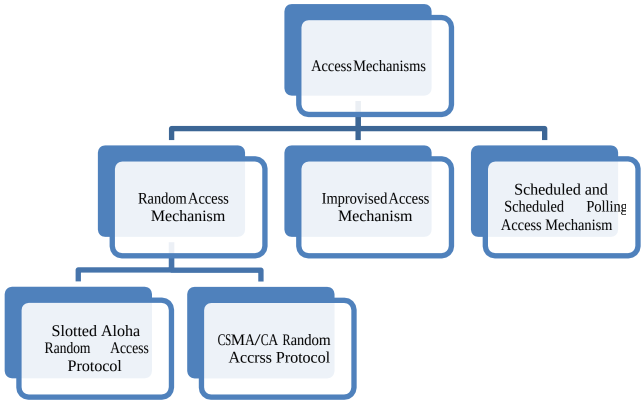
Non Beacon Mode without Super-frame Boundaries: In this communication mode, there are no beacons, super-frames or allocated slots. The hub may provide polled or posted allocations. The poll frames are control frames that allow nodes to start frame transmission by giving polled allocations. Whereas the post frames are the data frames that allow the hub to start frame transmission.



1.1.4 ***Fig 2.3 Non-Bean Mode without Super-frame Boundaries*** *[8]*

2.3.1.1. Access Mechanisms:

This standard supports following access mechanism:



1.1.5 ***Fig 2.4 Classification of Access Mechanisms in IEEE 802.15.6***

Random Access Mechanism:

In this access mechanism there are two further access mechanisms:

TABLE 1: Bounds for slotted-ALOHA and CSMA/CA protocols.

User Priorities	Slotted-ALOHA		CSMA/CA	
	CP_{max}	CP_{min}	CW_{min}	CW_{max}
0	0.125	0.0625	16	64
1	0.125	0.0937	16	32
2	0.25	0.0937	8	32
3	0.25	0.125	8	16
4	0.375	0.125	4	16
5	0.375	0.1875	4	8
6	0.5	0.1875	2	8
7	1	0.25	1	4

Fig 2.5 [9]

Slotted Aloha Random Access Protocol: In this access mechanism, the nodes can access the channels by using User Priorities (UPs) as shown in the above table. UPs are used to classify the high or low priority traffic. The Contention Probability (CP) is selected from User Priorities (UPs) i.e. from the interval [0-7]. In case of a successful transmission, CP is set equal to CP_{max}. It remains unchanged in the case of transmission failure i.e. odd number of failures. And CP is halved in the case of even number of failures. [9]

CSMA/CA Random Access Protocol: In this protocol, the nodes have three variables i.e. Contention Window (CW), Back off Counter (BC) and number of back off times (NB). The CW lies between the interval of [CWmin, CWmax] where CWmin and CWmax are determined by User Priorities. First the channel is checked whether it is idle or not. If the channel is idle for Inter-Frame Space (IFS) then BC is initialized to a random variable lying between the intervals [1, CW]. And for each attempt NB is increased by 1. In case where the channel is idle, BC is decremented by 1.

If the channel is idle and BC is equal to zero then a packet can be sent. If the channel is not idle, the nodes block their BC until the channel becomes idle. In case of a transmission failure, CW is doubled but by maintaining a limit such that CW is not greater than CWmax for even NB. While CW remains same for odd NB. [10]

Improvised Access Mechanism: In this access method, the hub uses poll and post frames in beacon and non-beacon modes with superframe boundaries. The hub uses poll frames to give access to nodes to start frame transmission whereas it uses post frames to send information about the network.

Scheduled and Scheduled Polling Access Mechanism: In scheduled access method, the nodes get scheduled time intervals to transmit frames. In scheduled polling access method, the poll and post allocations are used with the allocations being one periodic and m-periodic. In one periodic allocation, the nodes get time intervals in every superframe whereas in m-periodic allocation, the nodes get time intervals in every

mth superframe.

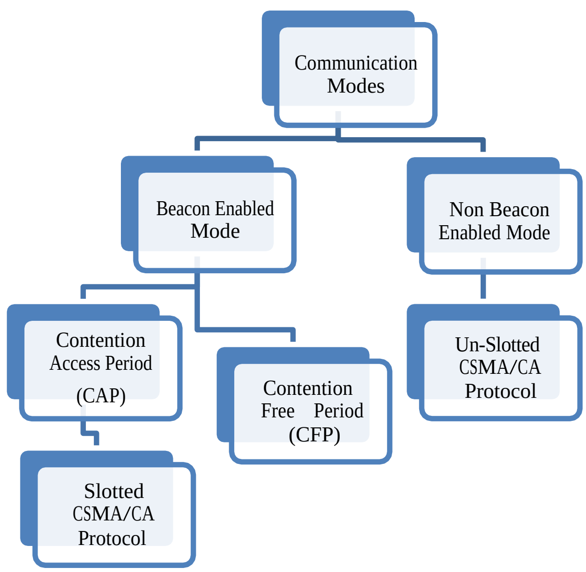
2.3.2. IEEE 802.15.4:

This standard was designed for Low Rate Wireless Personal Network (LR-WPN). It supports MAC and Physical Layer ofLR-WPN.

It supports two communication modes i.e. Beacon Enabled Mode and Non Beacon Enabled Mode.

Beacon Enabled Mode: In this mode, for the synchronization of nodes with the coordinator a beacon is used. The coordinator saves energy by having active and inactive periods which are called the Superframe structure. The active part has up to 16 time slots which are further classified into CAP (Contention Access Period) and CFP (Contention free period) [1]. During CAP, Slotted Access Mechanism is used. [11]

Non Beacon Enabled Mode: In this mode the channel is accessed when it is necessary. The data is sent only when the channel is idle otherwise the node has to wait for a period of time defined by the standard [1]. In this mode, Un-slotted CSMA/CA Access Mechanism is used.



1.1.6 ***Fig 2.6 Classification of Communication Modes of IEEE 802.15.4***

2.3.3. Access Mechanism:

Un-Slotted CSMA/CA Protocol: When there is no super-frame structure, this protocol is used [12]. This protocol is used in Non-Beacon Enabled Mode for channel access. For the transmission of frames, the nodes use Clear Channel Assessment (CCA) to check whether the channel is idle or not. If the channel is not idle, the node will wait for a random back off time and after that time, it will try again [12].

Slotted CSMA/CA Protocol: This protocol allocates specific time slots to the nodes thus ensuring a high rate of data delivery. In CAP (Contention Access Period), all of the nodes access the medium by Slotted CSMA/CA access mechanism [11]. For the transmission of frames, the nodes use Clear Channel Assessment (CCA) to check whether the channel is idle or not. If the channel is not idle, the node will wait for a random back off time and after that time, it will try again [12].

3. Comparisons of MAC Protocols:

After studying different types of MAC protocols, this section will discuss which MAC protocols are better than others by discussing their advantages and disadvantages.

MAC protocols	**Advantages**	**Disadvantages**
H-MAC	• It reduces energy consumption by avoiding use of external clock for synchronization. • It avoids collision by giving each node a Guaranteed time slot (GTS).	• It is not traffic adaptive. • It provides low bandwidth efficien
U-MAC	• It takes priority consideration in which the urgent traffic is given the priority.	• It does not take context and traffic awareness into consideration.
Med-MAC	• It reduces energy consumption • It provides flexibility • It handles traffic emergencies	• It does not take any priority consideration, context and traffic awareness into account.
Body-MAC	• It reduces idle listening and overhearing • It limits collision	• It does not take any priority consideration, context and traffic awareness into account
AR-MAC	• It saves energy by avoiding collision and overhearing.	• It does not take priority considerati account.

A-MAC	• It limits the channel access of nodes thus resulting in less energy consumption	• It does take context awareness into account in which the protocol is adapted according to channel and traffic conditions.
S-MAC	• Overheads are avoided as the nodes not participating in transmission go to sleep. [13]	• It provides low throughput.
B-MAC	• It reduces energy consumption by reducing idle listening.	• It does not provide synchronizatio
PW-MAC	• It avoids idle hearing and overhearing by using pseudo random scheduling. • It also reduces energy consumption	• Its disadvantage is that it includes overhearing and idle listening. [14]

4. Issues in MAC

Listed below are some general issues of MAC:

4.1. Synchronization:

Synchronization is very important for the network to be effective. It represents the continuous acceptance of data packets in such a way that energy is not largely consumed and it doesn't affect the throughput of the network [1].

Also for bandwidth reservation, synchronization is very important. One of the major issues in wireless networks is making the synchronization fixed to expand the time slots between exchanging nodes. For this, the control packets are exchanged and they carry the carrier signals between the sender, receiver and other intermediate nodes in the network.

As the carrier signals provide knowledge about progress so the specific amount of time slot is used for exchanging the packets and the network services might be lost.

Therefore, when designing the MAC protocol, it should be kept in mind that exchanging packets won't consume much time slot. [18]

4.2. Security:

One of the biggest issues of MAC WBAN is security as in MAC there are many attacks which can occur like: Spoofing, Unfairness, Collision, Sybil and Eavesdrop. To protect the network from these attacks we need to design the MAC protocol in such a way that it guarantees security against these attacks. [1]

4.3. Quality of Service:

Quality of service refers to providing better service to the network traffic. This is one of the major issues in MAC WBAN. The issues of QoS like reliability, energy efficiency and throughput can be solved by using an adaptive channel coding, time slot division and power scaling. [1]

4.4. Power Utilization:

In a wireless body area network, the sensors have limited battery power and during transmission, over-emitting, collision, idle listening, control packets overhead and overhearing much of this battery is lost. In order to solve this issue the MAC protocols should be designed in a way that the energy is utilized and the battery power of the nodes can be optimized. [1]

4.5. Delay Control:

Another major issue is propagation delay and transmission delay. These delays refer to the delay time in which the receiver receives the data. If this time is enough for a node to send data and it starts sending, but on the other side, transmission is taking place from the other nodes and the data has not reached to the receiver, then delay in the transmission can occur [15]. To decrease such delays, keeping the control on the flow of data rates should be done. [1]

4.6. Error Prone:

WBAN is prone to errors as in this network the data gets lost or it gets corrupted due to many reasons. To overcome these errors there must be a channel or a network coding scheme which can control these errors from occurring and increase the performance of the network. [1]

4.7. Dynamic Channel Assignment:

In WBAN, to overcome the issues like low throughput, data delay and data loss there should be a solution where the nodes are scheduled in way that distributes the bandwidth among the nodes [1]. Also there is not a centralized coordinator that is responsible for distributing the bandwidth among nodes. Thus, the MAC protocols should be developed in a distributed way. [17]

4.8. Over-hearing:

MAC layer in WBAN consists of over-hearing problem. This issue is a primary source of energy wastage.

It occurs when the sensor nodes receive the packets that are meant for other nodes, however, it can increase the energy wastage when the traffic load or node density increases. [1]

Over-emitting:

MAC Layer incurs a problem of over-emitting. It occurs when a transmitting node transmits the message but the receiver node is not prepared to receive it. This problem results in poor performance and energy wastage. Moreover, it causes congestion at transmitter and receiver side and can also make the channel unnecessarily busy. [1]

Idle-listening:

Idle-listening is also a primary source of energy wastage in MAC layer. It occurs when a sensor node is listening to the channel but no data packets are sent, leaving the channel idle. Idle-listening thus causes the node to stay in idle state for a long duration of time. [1]

5. Analysis and Discussions

Quality of service refers to providing better service to the network traffic. This is one of the major issues in MAC WBAN. QoS ensures that the issues like reliability, energy efficiency and throughput are overcome. By ensuring better QoS the general throughput of the network can be maximized.

5.1. QoS

Qos is one of the important features of WBAN whose efficiency can be increased by using the PEH-QoS scheme [2]. PEH-QoS is a Power-QoS control Scheme. The scheme focuses on using the energy collected by human movements which reduces the difficulty of charging the batteries of nodes with the help of the external nodes in WBAN. The PEH-QoS Scheme not only increases the efficiency but helps to improve storage capability as well. It comprises of three sub-modules, these modules interact with each other to reduce the energy wastage and enhance the QoS [3]. The main advantage of using this scheme is that only those data sequences are transmitted that are useful. This advantage is achieved by deducting those data packets that have lost their clinical validity.

The functionalities of QoS can be increased by using models co-related to the traffic model. The model uses the ON/OFF process and results in the effective handling of long distance traffic patterns and operational self-behavior. The proposed model encompasses the use of G/M/I queuing method.This queuing method along with the method of low latency queuing helps to enhance the QoS functionalities like that of delaying the packet losses. [2]

QoS can be maintained even when the sensors are declining gradually. This can be done by using two techniques. The first one involves the use of Gur Game [2]. The Gur Game is a control algorithm. The Adaptive Periodic Gur Game is used in this technique to maximize the performance as it increases the stability [4]. The APGur reduces the time to reach stability and can handle large amount of active sensors. By combining the Gur Game with the QoS feedback provided to each sensor, the QoS can be then maintained more effectively. The second technique would be to distribute this feedback to the sensors individually.

We can provide QoS by using a QoS aware routing protocol for WBAN.

One way is by using a Data-Centric Multi-objective QoS (DMQoS) aware routing protocol. This protocol addresses the issues like delay, energy requirement and reliability and ensures QoS for each traffic. It implements hop by hop routing by observing the QoS performance of the neighboring nodes.

And the other way by using a different QoS aware routing protocol which uses geographical routing to ensure the energy requirements. It divides the data traffic into different categories depending on the QoS metric and then it attempts to maintain the QoS by using the best candidate for routing.
In a cross layered designed QoS aware routing protocol, the route is selected by using a user defined QoS metrics, packet priority level and channel status. Furthermore it provides a service of feedback to user applications for the adjustment of medical application service level. [5]

5.2. Overhearing:

MAC layer in WBAN consists of over-hearing problem. This issue is a primary source of energy wastage.
It occurs when the sensor nodes receive the packets that are meant for other nodes, however, it can increase the energy wastage when the traffic load or node density increases. [1]

One of the solutions to the overhearing problem in MAC is by using a Traffic Adaptive MAC (TaMAC) protocol. This protocol provides energy efficiency by utilizing the node's traffic information to provide communication at a low power. This protocol, based on the type of traffic, uses two channel access mechanisms called the traffic based wakeup mechanism and wakeup radio mechanism. . It uses a traffic based wakeup mechanism for normal traffic and uses a wakeup radio mechanism for emergency or on demand traffic.

In traffic based wakeup mechanism, every operation performed by a node is based on a pattern called the traffic pattern. These patterns are initially defined by the coordinator and all of the traffic patterns of each node are kept in a table called traffic based wakeup table. This table is maintained by the coordinator and it stores the ID's of all nodes and their respective traffic patterns. All of the unnecessary power wastage caused by the overhearing or idle listening is avoided due to this mechanism as the nodes are given a predefined traffic pattern according to which they wake up when they have to send or receive data. Otherwise the nodes are in the sleep mode.

In wakeup radio mechanism, the wakeup radio signals are sent by either the nodes of the emergency traffic or the coordinator of the on demand traffic. [6].

6. Conclusions and Future Work

This paper presented the most important features of the IEEE 802.15.6 standard. A deep explanation of MAC, PHY, and security specifications of the standard was presented. Different communication modes and access mechanisms were explained. The NB, HBC, and UWB PHY specifications were reviewed in terms of frame structure, modulation, and other key parameters. In addition, the security services, including key generation and message security, were discussed. We believe that this paper could be used to quickly understand the key features of the standard and to analyse its potential for different applications.

References

1. M. Naeem, Jorge Diaz-Martinez, Shariq Aziz Butt and Nicolo Montesano, “Trends and Future Perspective Challenges in Big Data”, in Proc. Of The Sixth Euro-China Conference on Intelligent Data Analysis and Applications (ECC2019) Arad-Romania, March 2020.
2. Z. Haider and M. Saleem,"Analysis of Interference in Wireless", in Proc. of ArXiv, arXiv:1810.13164 [cs.NI], Oct. 2018.
3. A Khalid, SA Butt, and S Gochhait, “Agile Scrum Issues at Large-Scale Distributed Projects: Scrum Project Development At Large”, in International Journal of Software Innovation (IJSI), Vol 8, Issue 2, Pages: 85-94, IGI Global 2020.
4. S Gochhait, SA Butt, and A Ali, “Cloud Enhances Agile Software Development” Book Chapter in Cloud Computing Applications and Techniques for E -Commerce, Pages: 28-49, IGI Global, 2020.
5. M Alam, and MM Umair, "Detection and Prevention Against RTS Attacks in Wireless LANs", in Proc. of IEEE C-CODE, Islamabad Pakistan, Mar. 2017.
6. 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.
7. S. A. Butt, and M. Shoaib, "IoT Smart Health Security Threats," in proc. of 19th International Conference on Computational Science and Its Applications (ICCSA), Saint Petersburg, Russia, 2019, pp. 26- 31. doi: 10.1109/ICCSA.2019.000-8.

8. M. Asam and Z. Haider, "Security Issues in WBANs", in proc. of Arxiv, Volume arXiv:1911.04330 [cs.NI], November 2019.
9. M. Asam and Z. Haider, "Novel Relay Selection Protocol for Cooperative Networks", in proc. of Arxiv, Volume arXiv: 1911.07764 [cs.NI], November 2019.
10. Zeeshan Haider, Muhammad Asam, Shariq Butt and Aleena Ajaz, "Mitigation of Wireless Body Area Networks Challenges using Cooperation", International Journal of Security and Its Applications (IJSIA), ISSN: 1738-9976(Print); 2207-9629(Online), NADIA, (2020), Vol. 14, No. 1, pp. 15-30.
11. SA Butt and M. Ajmal Azad, "A multivariant secure framework for smart mobile health application", in Transactions on Emerging Telecommunications Technologies, Aug. 2019.
12. M. Asam and A. Ajaz, "Challenges in Wireless Body Area Network", in Proc. of International Journal of Advanced Computer Science and Applications, Volume 10, No. 11, Nov. 2019.
13. SA Butt and A. Ali, "Predictive Variables for Agile Development Merging Cloud Computing Services", in Proc. of IEEE Access, Volume 7, 2019. DOI: 10.1109/ACCESS.2019.2929169.
14. P. Mendes, "Analysis of Hybrid Relaying in Cooperative WLAN", In Proc. of IEEE IFIP Wireless Days (WD), Valencia, Spain, November 2013.
15. P. Mendes, and A. Zúquete, "Relayspot: A Framework for Opportunistic Cooperative Relaying", in Proc. of IARIA ACCESS, Luxembourg, June 2011.
16. SA Butt, "Cooperative Cloudlet for Pervasive Networks", in Proc. of Asia Pacific Journal of Multidisciplinary Research, Vol. 5, No. 3, PP. 42-26, Aug 2017.
17. SA Butt, and T. Jamal, "Frequent Change Request from User to Handle Cost on Project in Agile Model", in Proc. of Asia Pacific Journal of Multidisciplinary Research 5 (2), 26-42, 2017.
18. P. Amaral, "Flow Table Congestion in Software Defined Networks", in Proc. of IARIA 12th ICDS, Rome Italy, Mar. 2018.
19. P. Mendes, and A. Zúquete, "Wireless Cooperative Relaying Based on Opportunistic Relay Selection", in Proc. of International Journal on Advances in Networks and Services, Vol. 5, No. 2, PP. 116-127, Jun. 2012.
20. 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.
21. SA Butt, "Low-Energy Adaptive Clustering Hierarchy (LEACH) Enhancement for Military Security Operations", In Proc. Of Journal of Basic and Applied Scientific Research, ISSN 2090-4304, 2017.
22. Z. Haider, "Denial of Service Attack in Cooperative Networks", in Proc. of ArXiv, arXiv: CoRR Vol. arXiv:1810.11070 [cs.NI], Oct. 2018.
23. T. Jamal and P. Mendes, "Relay Selection Approaches for Wireless Cooperative Networks", in Proc. of IEEE WiMob, Niagara Falls, Canada, Oct. 2010.
24. T. Jamal and P. Mendes, "Cooperative relaying in user-centric networking under interference conditions", in Proc. of IEEE Communications Magazine, vol. 52, no. 12, pp. 18–24, Dec 2014.

25. Fawad, U., et al. "Proton, UV, and X-ray Induced Luminescence in [Tb.sup.3+] Doped Lu[Gd.sub.2][Ga.sub.2][Al.sub.3][O.sub.12] Phosphors." Crystals, vol. 10, no. 9, 2020.
26. Fawad, U.; Kim, H. J.; Gul, Ibrahim; Khan, Matiullah; Tahir, Sajjad; Muhammad, Wazir. 2020. "Proton, UV, and X-ray Induced Luminescence in Tb3+ Doped LuGd2Ga2Al3O12 Phosphors" *Crystals* 10, no. 9: 844.
27. T. Jama, and A. Zúquete, "Opportunistic Relay Selection for Wireless Cooperative Network", in Proc. of IEEE IFIP NTMS, Istanbul Turkey, May 2012.
28. P. Mendes, W. Moreira and Huiling Zhu, "Cooperative Networking in User-Centric Wireless Networks", In: Aldini A., Bogliolo A. (eds) User-Centric Networking. Lecture Notes in Social Networks. Springer, Cham, ISBN 978-3-319- 05217-5, May 2014.
29. T. Jamal, and P. Mendes, "COOPERATIVE RELAYING FOR DYNAMIC NETWORKS", EU PATENT, (EP13182366.8), Aug. 2013.
30. T. Jamal, and P. Mendes, "802.11 Medium Access Control In MiXiM", in Proc. of Tech Rep. SITILabs-TR-13-02, University Lusófona, Lisbon Portugal, Mar. 2013.
31. L. Lopes, T. Jamal, and P. Mendes, "Towards Implementing Cooperative Relaying", In Proc. of Technical Report COPE-TR-13-06, CopeLabs University Lusofona Portugal, Jan 2013.
32. P. Mendes, and A. Zúquete, "Interference-Aware Opportunistic Relay Selection", In Proc. of ACM CoNEXT student workshop, Tokyo, Japan, Dec. 2011.
33. T. Jamal, "Cooperative MAC for Wireless Network", In Proc. of 1st MAP Tele Workshop, Porto, Portugal, 2010.
34. T. Jamal, and P. Mendes, "Cooperative Relaying for Wireless Local Area Networks", In: Ganchev I., Curado M., Kassler A. (eds) Wireless Networking for Moving Objects. Lecture Notes in Computer Science, vol 8611. Springer, Cham, (WiNeMo), Aug. 2014.
35. R. Sofia, P. Mendes, W. Moreira, A. Ribeiro, S. Queiroz, A. Junior, T. Jamal, N. Chama, and L. Carvalho, "Upns: User Provided Networks, technical report: Living-Examples, Challenges, Advantages", Tech. Rep. SITI-TR-11- 03, Research Unit in Informatics Systems and Technologies (SITI), University Lusofona, Lisbon Portugal, Mar. 2011.

36. P. Mendes, “Cooperative Relaying in Wireless User-Centric Networks”, Book Chapter In: Aldini, A., Bogliolo, A. (eds.) User Centric Networking. Lecture Notes in Social Networks, Springer, Cham, pp. 171–195, 2014.
37. T. Jamal, P. Mendes, and A. Zúquete, “Design and Performance of Wireless Cooperative Relaying”, PhD Thesis MAP-Tele, University of Aveiro, Oct. 2013.
38. T. Jamal, P. Mendes, and A. Zuquete, “RelaySpot: Cooperative Wireless Relaying”, in Proc. of MAP-Tele Workshop, Aveiro, Portugal, May 2011.
39. T. Jamal, and P. Mendes, “Cooperative Wireless Relaying, Key Factors for Relay Selection”, in Proc. of MAP-Tele Workshop, Porto, Portugal, Dec. 2009.
40. T. Jamal, and P. Mendes, “RelaySpot, OMNET++ Module”, Software Simulator Extension In Proc. of COPE-SW-13-05, 2013.
41. P Amaral, A Khan, SAB, Kiramat, "Denial of Service Attack in Wireless LAN", in Proc of 12th ICDS 2018, Rome Italy.
42. M. Asam, K. Ghmman and Z. Haider, "Ubiquity of Healthcare System", in Proc of e-LIS [Preprint], Dec 2019, http://eprints.rclis.org/39303/
43. Khan A, Zameer A, Raza A (2018b) Deep belief networks based feature generation and regression for predicting wind power. Preprint arXiv:1807.11682
44. Muhammad Imran, Farrukh Khan, and Muhammad Durad, "Analysis of Detection Features for Wormhole Attacks in MANETs", International Workshop on Cyber Security and Digital Investigation (CSDI 2015).
45. Asam, M., “IoT Malware Detection Architecture using a Novel Channel Boosted and Squeezed CNN”, arXiv preprint , arXiv:2202.04121 [cs.CR], Feb 2022.
46. Aleena Ajaz et al., “Small Object Detection using Deep Learning”, arXiv preprint, arXiv:2201.03243 [cs.CV], Jan 2022.
47. Asam, M., Khan, S. H., Jamal, T., Zahoora, U., & Khan, A. 2021, “Malware Classification Using Deep Boosted Learning", arXiv preprint arXiv:2107.04008.
48. Asam, Muhammad, et al. "Detection of Exceptional Malware Variants Using Deep Boosted Feature Spaces and Machine Learning." Applied Sciences 11.21 (2021): 10464.