International Journal of Security and Its Applications
Vol. 14, No. 1 (2020), pp.15-30
http://dx.doi.org/10.33832/ijsia.2020.14.1.02

MITIGATION OF WIRELESS BODY AREA NETWORKS CHALLENGES USING COOPERATION

Zeeshan Haider[1], Tauseef Jamal[2], Muhammad Asam[3], Shariq Butt[4*] and Aleena Ajaz[5]

[1]*UIIT, PMAS-Arid Agriculture University, Rawalpindi, Pakistan*
[2,3,5]*DCIS, PIEAS University, Islamabad, Pakistan*
[4]*Univeristiy of Lahore, Pakistan*
[1]scholarxeeshan@gmail.com, [2]jamal@pieas.edu.pk, [3]asim2k994@gmail.com,
[4*]shariq2315@gmail.com, [5]aleena.ajazsh@gmail.com

***Abstract*— The degradation of an adequate medical facilities for safety and healthy human atmosphere motivated researchers to think more generously to provide a smart solution in medical applications. Wireless body area network (WBAN) is one of the potential platform to cope up to the needs of prevailing medical demands and challenges. In the literature, WBAN is a femto-network (ranges up to few meters) formation around a human body for sensing, transmission and reception functionality. These functionalities are executed using various modes by placement of sensors node on human posture or by injecting inside of the human body. This mode of communication have various challenges when deployed in medical applications. Due to the critical nature of human physiological sensed data which demands a reliable and secure transmission, reception between sensors, intermediate and master node. This article outcomes are two fold, first is the state of art challenges of WBAN and the need of the ultimate smart solution for safe and reliable communication in Wireless body area Networks. Secondly, using Cooperation techniques for mitigation of WBAN issues, proposed cooperative model is presented for reliable data transmission using an efficient network resource utilization mechanism.**

***Keywords*— WBAN (Wireless Body Area Network), Denial of Service Attacks, Resource Management, Cooperation, Security**

1. 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) in 1996 [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.

Received: September 13, 2019
Reviewed: March 19, 2020
Accepted: March 24, 2020
* Corresponding Author

ISSN: 2207-9629 IJSIA

Same can be done by the sensors for environmental parameters like location, temperature, humidity and light. We place 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 of this section, we describe the architecture of WBAN, while Section 2 details its applications and challenges. In Section 3, we explain how cooperation techniques overcome the issues faced by WBANs. Section 4 discusses proposed solution with used cases. Sections 5 concludes the discussion on our findings and future work.

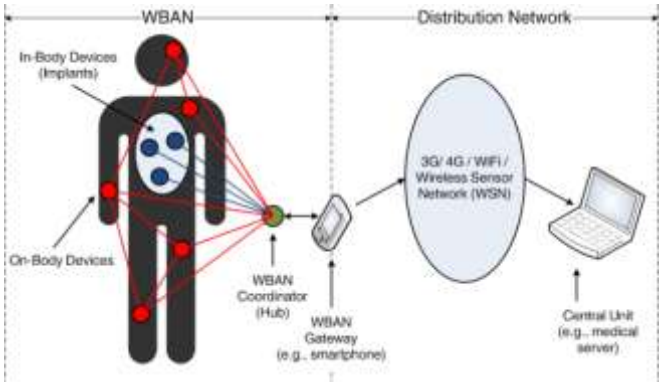


Fig. 1 Two Tier Architecture for WBAN [4]

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.

Despite of the two-tier and three-tier architecture, we can 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*.

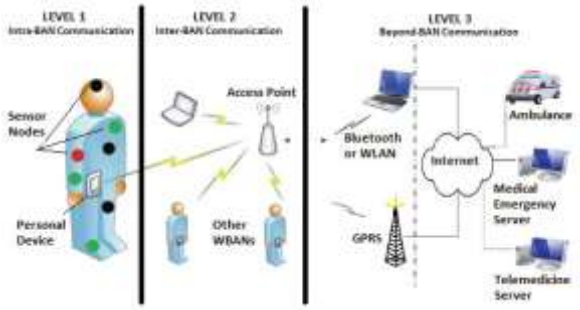


Fig. 2 Three Tier Architecture for WBAN [5]

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, we detailed some of its applications.

2. APPLICATION AND CHALLENGES

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.

2.1. APPLICATIONS

We classify these applications into two broad categories, *i.e.*, Medical and Non-Medical applications (c.f. Fig. 3).

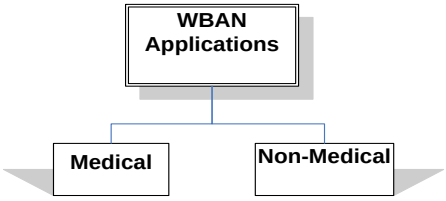


Fig. 3 WBAN Applications

2.1.1 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.).

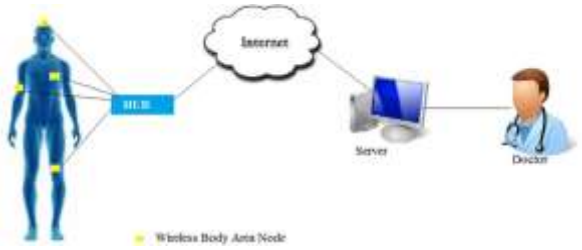


Fig. 4 Application of WBAN in Telemedicine

2.1.2 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 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.

2.2 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. We have classified these challenges 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.

Fig. 5 WBAN main Challenges

2.2.1 ENERGY REQUIREMENTS

Since, most of the devices in WBANs 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 we 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.

2.2.2 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]. 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, we can coarsely divide the communication into two parts, internal communication between WBAN and external communication between WBAN and external users. Security requirement in internal communication 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], the authors suggested secure and reliable routing framework for WBAN. They demonstrated that it can significantly counter the data injection attacks.

Security Requirements in external communication includes the Utility of WBAN in healthcare system that handles 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. .

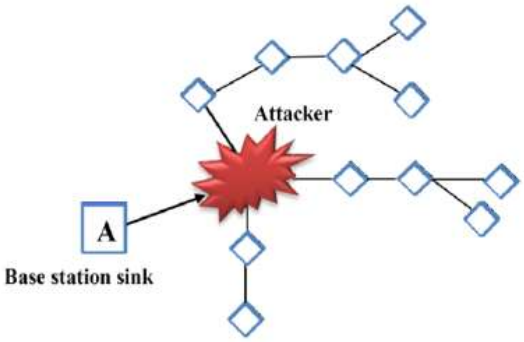


Fig. 6 Hello Flood, a Network Layer Attack

- 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.

2.2.3 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 we 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 WBANs. It works on one hop communication model and has less delay.

2.2.4 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 Table I [20, 21].

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

2.2.5 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 WBANs specially when there is ad-hoc connectivity.

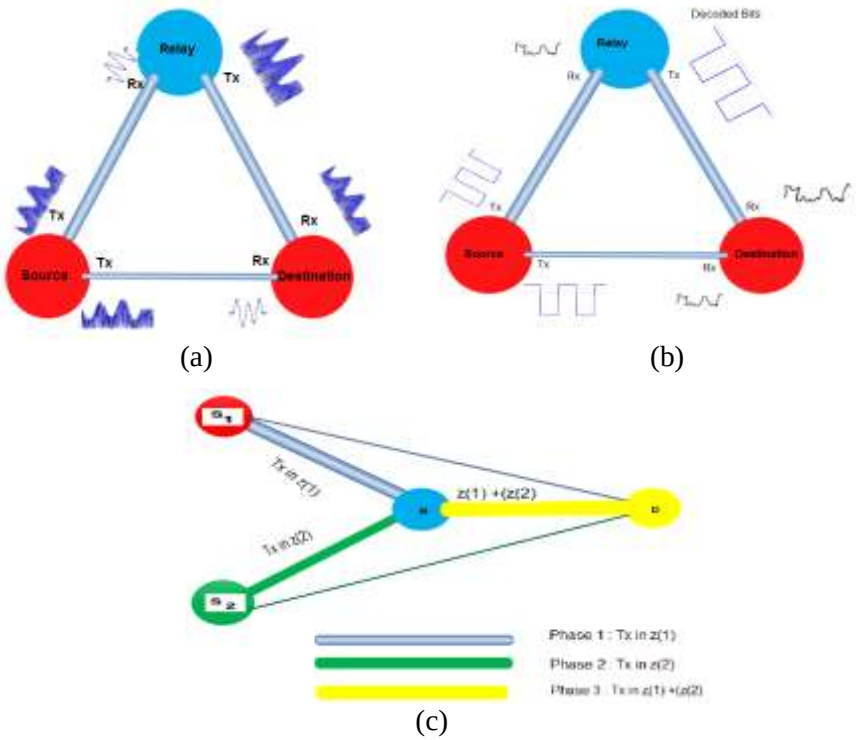
3. COOPERATION IN WBAN

In high pervasive and ubiquitous WBAN networking, one of the emerging technologies of cooperative networks [22] brought many opportunities to enhance performance and reliability among wireless nodes. The cooperative relaying provides the self-organization [23] role in the network and can adjust the transmission parameters dynamically using opportunistic relays. In wireless networks the use of cooperative networks use the overhearing approach called relays , the use of relaying in networking at different location assist the source nodes to send multiple copies of same packet/frame helps in achieving same packet from more than one sources. The high capacity links have

more accurate and reliable information therefore, relaying bring a high throughput, coverage and longer network lifetime.

First type, the reactive relaying (opportunistic relays) are having less overhead. However, to find the optimal relay selection is a complex task [24]. The second type of relaying called proactive relaying which is also called broadcasted relaying. Broadcasted relaying keep neighbors map for relay selection but a considerable overhead make undesirable where high performance and reliability are prime objectives. A hybrid approach is therefore deeming important, that will ensure an optimal level of performance and reliability. There are three main cooperative techniques used in relaying *i.e.*, (1) Amplify and Forward, (2) Decode and Forward and (3) Coded Cooperation [24].

The first approach of amplify and forward technique is very effective in achieving high diversity gain, however along with information signal the noise signal also get modified which is not required and cause degradation of Quality of service. Fig 7(a) is elaborated amplify and forward approach. The second approach is decode and forward approach, the major drawback faced by amplify and forward approach overcome by decode operation. Where original signal is decoded and then again modulated to new transmission scheme. This method increases the reliability assurance. However, due to decoding of original signal at relaying node the sufficient delay factor added which decrease the performance of the source to destination communication. Fig 7(b) shows the decoded and forward operation. The third strategy is coded cooperation is another powerful technique. In this approach, each node transmits code-word information on independent fading channel. Subsequently, the multiple sources data sent over the channel for final destination. In Fig 7(c), a coded cooperation-relaying model is shown.



(a) (b)

(c)

Fig. 7 (a) Amplify and Forward technique (b) Decode and Forward technique, (c) Coded Cooperation technique

The exploiting of cooperation for high performance and reliable communication bring the promising benefits for achieving high QoS, in term efficient of flow control mechanism. The optimal flow control increases the probability of the efficient

transmission and retransmission mechanism that ultimately assure the high packet success rate (good put). The second performance dependent metric of self-organization and scalability is also being addressed in the solution. For that reason, a hybrid approach will be designed to address the limitation of ad-hoc networks performance (explained in next section), fault tolerance and reliable communication. The cooperation networks have a various benefits but their independent techniques are not suitable for high performance and reliability. Therefore, a hybrid (proactive and reactive relaying) is considered for reliability and optimal relay selection. In Fig 8 the ad-hoc cooperation model is shown where four nodes are deployed in a network. It can be seen that direct communication channels are shown with thinner pipeline and high diversity links are shown with thicker pipeline that shows high capacity and throughput channels. The concept of cooperation will not only provide the better performance but better resource utilization as well. The cooperation node depicted in diagram as Cooperative node will be hybrid relay for data transmission from source to destination. The ad-hoc cooperation model will help in achieving in high diversity gains through optimal flow control. Secondly, enhanced self-organization of nodes can help in achieving high network lifetime. Thirdly, and scalability of the ad-hoc network will be achieved using optimal self-organization functionality.

The system modeling will be carried using two system modeling approaches. Firstly, the analytical model approach of Markov chains can be used. Secondly the simulation topology will be designed; furthermore, the evaluation and comparison will be carried out. Subsequently, the comparison with cooperative and non-cooperative model/protocol will be prepared.

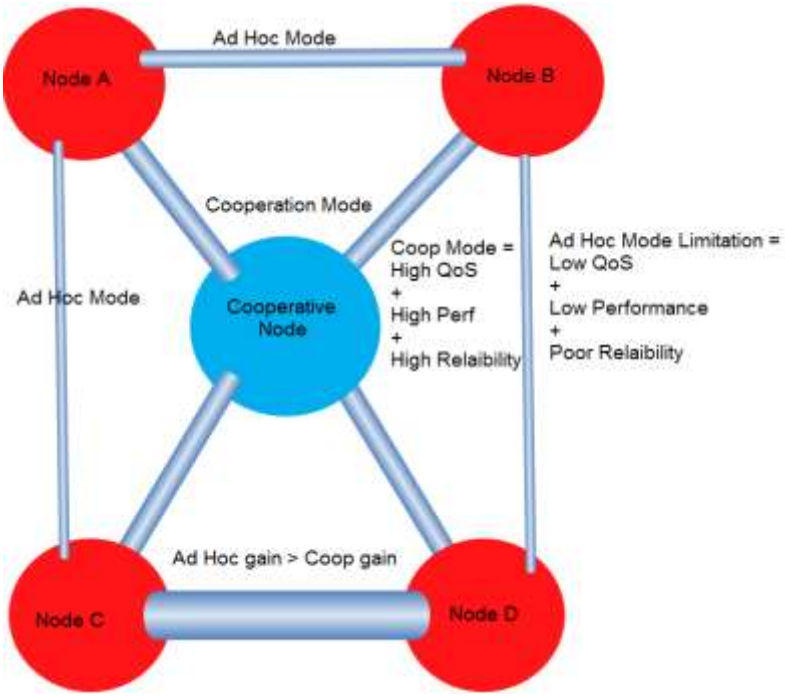


Fig. 8 Ad-hoc Cooperation Performance and Reliability model

3.1. WBAN PROBLEM SPACE

The wireless body area networks are facing High performance and reliability issues which cause degradation in Quality of Service, self-organization and scalability [21]. Firstly, The Quality of Service degradation is increased due to link layer packet impairments, which is caused by inefficient flow control mechanism that increases the delay, packet delivery ratio and reduce channel utilization. Secondly, the self-

organization of nodes poses another research challenge that needs a reliable communication mechanism for better good put. Thirdly, the scalability issue increases the collision and contention of wireless resources that cause failure of network functionality.

3.2. WBAN COOPERATION OBJECTIVES

The proposed WBAN cooperation model has following research objectives.

1. To introduce an optimal flow control approach that can handle packet re-transmission, collision and contention to build a reliable network.
2. To develop a Hybrid Cooperative Protocol to integrate the self-organization that will address the scalable networking.
3. To design simulation environment for performance analysis and evaluation of the results.

3.3 PROPOSED WBAN COOPERATION MODEL

The high performance and reliable ad-hoc communication using hybrid cooperative approach is main goal of our cooperative framework. A cross layer cooperative protocol is proposed to cater the challenges of QoS degradation using optimal flow control and high diversity gain of hybrid cooperative approach to address the ad-hoc node self-organization and scalability. First phase, the hybrid cooperative technique for ad-hoc performance and reliability are to be designed. In second phase, the optimal flow control model is designed for improving QoS and achieving desired objective. The third phase will deal with the self-organization, which will enhance handover using hybrid-relaying mechanism. The third phase will also deal with the nodes scalability problem using ad-hoc cooperation. The flow activity of the proposed model component is shown in Figure 9.

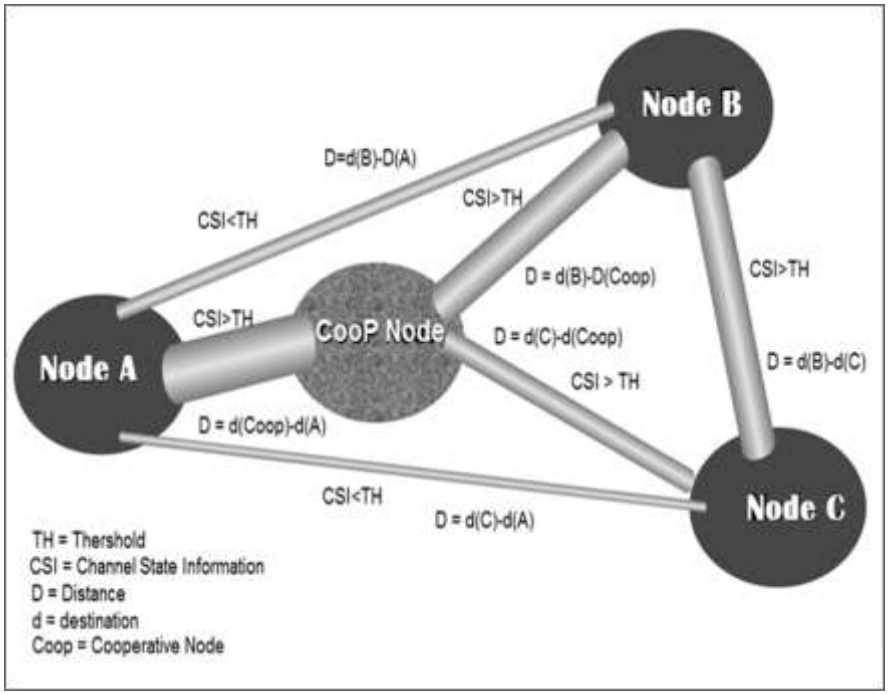


Fig. 9 WBAN Cooperation Model for High Performance and Reliability

The WBAN cooperation model is shown in Figure 10. The nodes are interlinked with direct link as well as cooperative relay node. It has been observed through diagram that

the channel capacity using cooperation is increased and thicker pipe shows high bandwidth and thorough put that is possible using diversity gain. Secondly, the optimal placement of cooperative node and efficient relay selection will help to achieve the reliability feature for WBAN cooperation. The channel state information using cooperative node is better than direct link. However, if nodes are close and their distance is less than threshold value then direct communication will be carried out.

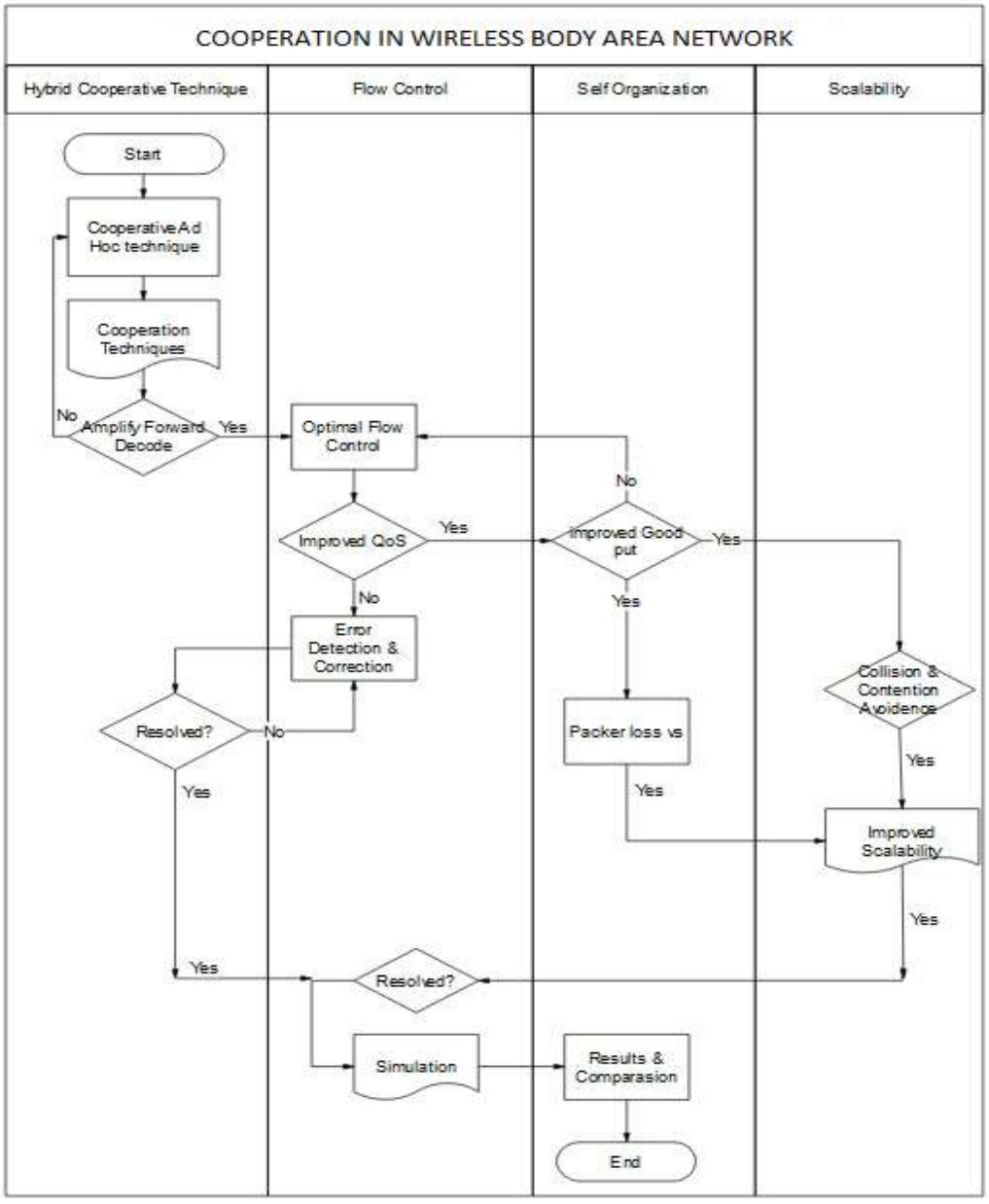


Fig. 10 Proposed Cooperative WBAN Model Flow Diagram

4. PROPOSED SOLUTIONS

The proposed solution of WBAN using Cooperation techniques are hereby presented. The hybrid cooperation technique can be a viable solution to achieve below use cases implementation. It is hybrid since, it is combination of proactive and reactive protocols. The proposed solution is preventing single point of failure (reactive) in existing WBAN architecture where coordinator or master node collapse results in whole communication

network failure in WBAN, in that the alternative routing and selection of coordinator carried out to utilize the network resources efficiently this can be one of the best approach. The WBAN sensor nodes are inexpensive nodes but fully functional devices are expensive due to intelligent and more resourceful than the reduced function devices. The proactive solution deals with resource management and to help the master node when needed.

4.1. REACTIVE PROTOCOL

WBAN devices form a topology where three types of nodes are deployed *i.e.*; Coordinator or Master Node (MN), fully functional devices or intermediate routers and third is the sensors which have limited functionality are also called reduced function devices. The typical architecture is WBAN is shown in Fig. 11. Where sensors send data to intermediate routers which then send this data to the master node. The sensor nodes can directly send to coordinator as well if they are at the close proximity with respect to each other, they can send directly to master nodes. The cross line in coordinator shows the master node failure.

To overcome this important research issue in WBAN, a redundant data sink method is proposed that not only avoids single point of failure. The tree priority mechanism is proposed for maximum availability of network for sensors nodes. In the shown in figure, there are three cases when master nodes failure effect on the part of WBAN communication.

- Master Node Failure
- Master Node Link Failure
- Direct Link to Master node failure

When master nodes fails, then whole communication shifted to Router. The next master nodes will be router, it will accept the data sink requests and update all the sensors nodes final destination as router node. Second thing the router will ensure, it will maintain local routing where external link communication established with inter WBAN communication.

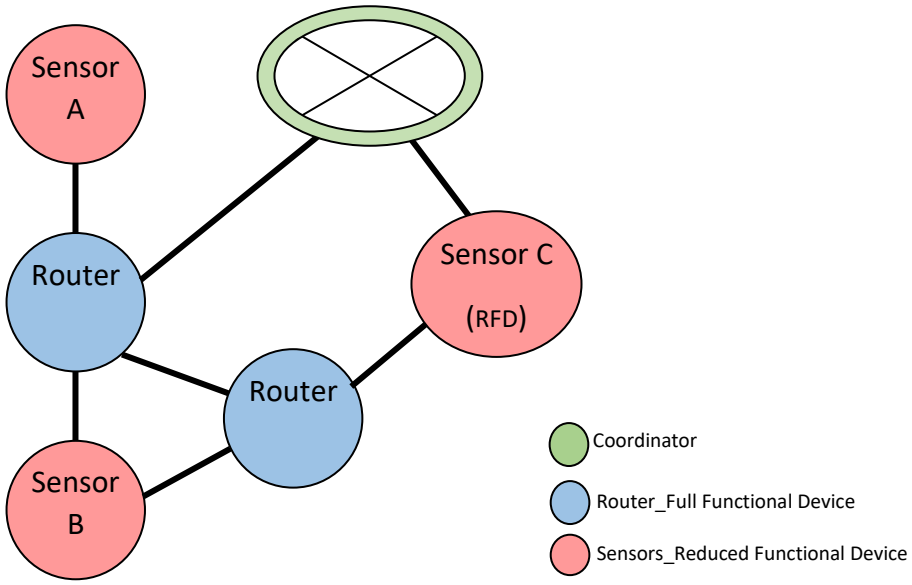


Fig. 11 (a). WBAN Scenario_01 Single Point Failure Architecture (Master Node failure)

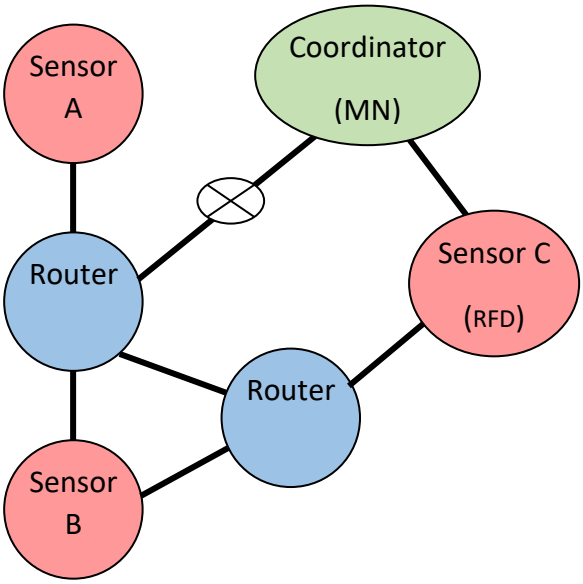


Fig. 11 (b). WBAN Scenario_02 Single Point Failure Architecture (Master Node link failure)

In second case of the scenario_02 Fig 11(b), when master node link failure occur due to some interference or jamming, at that all communication routed to second router via router M, now the sink node will be router B. In the third scenario, Fig 11 (c), the direct link of the sensor node C fails with Master Node. In that case, the router B will direct the communication to router A and subsequently router to Master node.

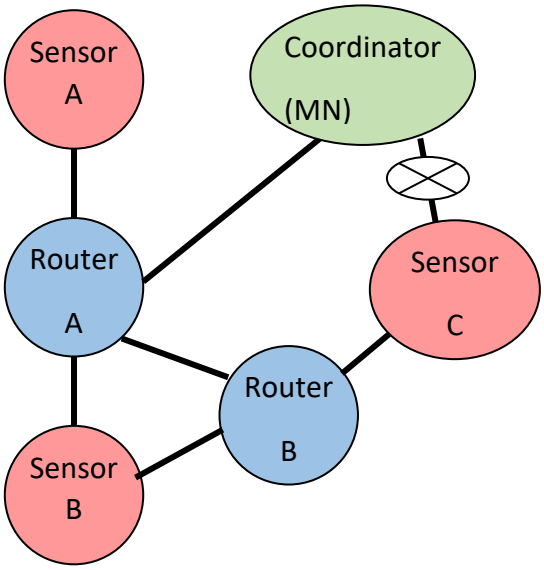


Fig. 11 (c). WBAN Scenario_03 Single Point Failure Architecture (Sensor Direct link Failure)

4.2. PROACTIVE PROTOCOL

In contrast to previous scenario of single point of failure, the proactive solution is intelligent in term of resource utilization. The efficient resource management deals with the case when all links are available but the performance and reliability factors are not optimal, so there is need of help. In that case, there are four parameters that decide the enable cooperation. These parameters will help in deriving the equation for optimal relay selection and achieving less end to end delay from source to destination. These parameters are as follows

- Master node load threshold
- Relay node assistance
- Weak Link optimization
- Network life time

The relay node parameters help us to design the when and where relay required in WBAN communication. Such, relaying on demand can also be used mitigate DoS attacks.

4.2.1. MITIGATING DOS ATTACK

The Denial of Service (DoS) attack occurs when intended access or network resources are jammed or block by some other user conscious deadlock mechanism. DoS are categorized in mainly two categories. Active and passive DoS. In active jamming the attack intentionally launches this attach and results in no access in fulfillment of intended users requests. The active DoS attack can be avoided but the passive attacks required intelligent mechanism to overcome the sluggish behavior of the WBAN nodes. The proposed solution will help in mitigating the DoS attack using relay node, as shown in Fig. 12. The access mechanism of the WBAN nodes will be added with request validation scheme. Where networks nodes getting service at more shaper time will be encounter and equal chance of servicing will be ensures.

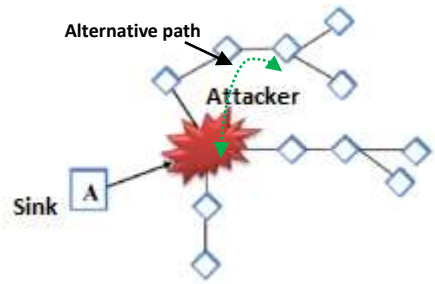


Fig. 12 Attack Mitigation via Cooperation

5. CONCLUSION

This paper elaborated the performance and reliability challenges of the WBAN systems. The application and challenges are briefly discussed, later on the need cooperation is emphasized. The proposed cooperation model in discussed and objective of WBAN cooperation are discussed. Subsequently, this article discussed the proposed two solutions to cater the challenging issues of WBAN coordinator failure and DoS Mitigation. To overcome these issues a novel strategy proposed so that the maximum network life time can be ensured. The second solution ensure the DoS mitigation in

WBAN systems. The access validation mechanism is proposed so that DoS attack can be dealt in more intelligent and better way.

The future work of this paper will be implementation of both the proposed solution using testbed. It also includes the selection of secondary coordinator algorithm when main Master nodes fails or overloaded.

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] M. Asam and T. Jamal, "Security Issues in WBANs", in proc of Arxiv, Volume arXiv:1911.04330 [cs.NI], November 2019.
[4] A. A. E.Kartsakli, S .Tennina, A. Lalos, P.V.Mekikis, L.Alonso, F.Graziosi, M. Di Renzo and Ch.Verikoukis. (2013, Enhancing quality of life with wireless sensor technology. IEEE Life Sciences.
[5] (2011) ACM SIGCOMM Computer Communication Review. CM SIGCOMM Computer Communication Review.
[6] 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.
[7] 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.
[8] A. D and K. K. Venkatasubramanian, "Biomedical devices and systems security,," USA, September 2011.
[9] X. L. X. Liang, Q. Shen, "Exploiting prediction to enable secure and reliable routing in wireless body area networks," 2012.
[10] 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.
[11] 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.
[12] M. G. Nabi, MCW. Basten, AA., "MoBAN: A Configurable Mobility Model for Wireless Body Area Networks," March 2011.
[13] S. F. a. M. Collier, "On the problem of energy efficiency of multi-hop vs one-hop routing in Wireless Sensor Networks," Research Institute for Networks and Communications Engineering (RINCE), Dublin City University, Dublin 9, Ireland.
[14] C. J. M. Shanmukhi, "A Review on Mobility Feature in Wireless Body Area Networks," vol. 6, June 2017.
[15] Y. Birgani, N. Javan, and M. Tourani, "Mobility enhancement of patients body monitoring based on," Indonesia, May 2014.
[16] B. Braem and C. Blondia, "Supporting mobility in wireless body area networks: An analysis," Ghent, Belgium, November 2011.
[17] W. Z. Feng Xia, Youxian Sun and Yu- Chu Tian, "Fuzzy Logic Control Based QoS Management in Wireless Sensor/Actuator Networks," Sensors, vol. 7, pp. 3179-3191, 2007.
[18] J. L. Gang Zhou, Chieh-Yih Wan, Mark D. Yarvis, and John A. Stankovic, "BodyQoS: Adaptive and Radio-Agnostic QoS for Body."
[19] 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.
[20] M. H. A. Md. Taslim Arefin, A. K. M. Fazlul Haque, "Wireless Body Area Network: An Overview and Various Applications," Journal of Computer and Communications, vol. 5, pp. 53-64, 2017.
[21] I. Dimitriou and N. Pappas, “Performance analysis of a cooperative wireless network with adaptive relays,” Ad Hoc Networks, vol. 87, pp. 157–173,2019, doi: 0.1016/j.adhoc.2018.12.007.
[22] T. Jamal, P. Mendes, and A. Zúquete, "Relayspot: A Framework for Opportunistic Cooperative Relaying," in IARIA ACCESS, Luxembourg, June, 2011.
[23] M. Asam and Z. Haider, "Novel Relay Selection Protocol for Cooperative Networks", in proc of Arxiv, Volume arXiv: 1911.07764 [cs.NI], November 2019.
[24] 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.
[25] SA Butt and T. Jamal, "A multivariant secure framework for smart mobile health application", in Transactions on Emerging Telecommunications Technologies, Aug. 2019.

