Investigation of Security Issues in Wireless Body Area Networks in Assorted Networks

N.Haritha Assistant Professor,VIET Visakhapatnam

Abstract— Body Area Network (BAN) is an important technique for monitoring patient health in real time and detecting and analyzing diseases. There are some key issues that must be addressed in order to effectively implement and benefit from this technology, and security is one of those issues. WBAN will have to operate in a cooperative networking model of multiple networks, such as homogeneous networks for performance and reliability or heterogeneous networks for data transfer and processing from an application standpoint, with other networks such as hospitals, clinics, medical experts, and the patient himself / herself who may be moving from one network to another. This paper discusses security issues in WBAN in separate networks as well as multiple networks. The IEEE 802.15.6 standard is taken into account for WBAN working in a separate network. Security issues are taken into account for WBANs operating in multiple networks, particularly heterogeneous networks. The paper describes potential approaches to addressing these issues by modeling Security Mechanisms with various Artificial Intelligence techniques. The paper proposes Game Theory with Stacker-berg Security Equilibrium (GTSSE) for modeling security in Heterogeneous Networks in WBAN and describes the authors' experiments and results demonstrating the suitability of the modeling using GTSSE.

Index Terms— Body Area Network (BAN), Heterogeneous networking, Network security, Game Theory

1. Introduction

The body area network placed an important role in healthcare application to monitoring patient health in real time. The sensor devices are used to observe the patient health and identifying various diseases. For effective implementation of this technology in practice and benefit from it, there are some key issues which are to be addressed. Among them, security issue is one of them where research is going on. WBAN uses wireless sensors specifically for use within or on the human body and capture many parameters and so it enables various applications related to health or medical or even general purpose.

IEEE has published a IEEE 802.15.6 standard sensor networks which has been developed by the Task Group IEEE 802.15.6. [1]. The IEEE 802.15.6 Standards [2] has been specified for making the short range communication that is utilized in the industries and medical which is approved by the authorities. The sensor network has specific characteristics such as low power, quality of services and 10Mbps transfer rate. This process ensures the low specific absorption rate (SAR). The normal is available as a document in [2].

The WBAN applications addressed by IEEE 802.15.6 standard are either non-medical and medical applications as given in Figure 1 and Figure 2 [3] gives a pictorial description of the WBAN structural design for various applications.

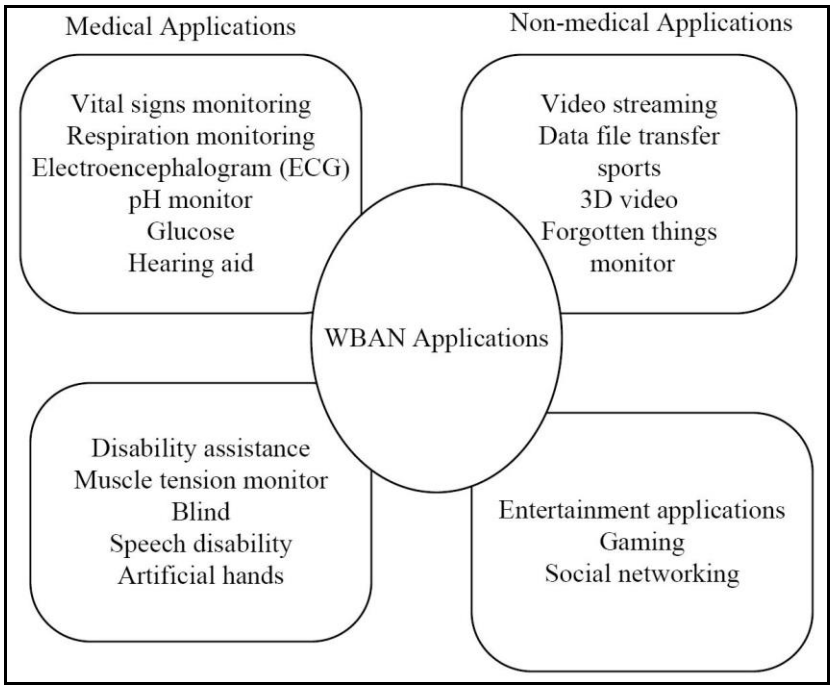

Figure 1 : IEEE 802.15.6 Standard based body sensor networks applications

This paper brings out the issues related to security in WBAN in separate network as well as in heterogeneous network and possible approaches which can be taken to address them. The section 2 defines the security issues in a WBAN in a single network and section 3 defines the security issues in WBAN in multiple networks. Section 4 describes the various artificial techniques which can be used to effectively model the security issues in WBAN and the section 5 gives a conclusion of the analysis of different techniques and proposes one of them for effective modeling with higher security.

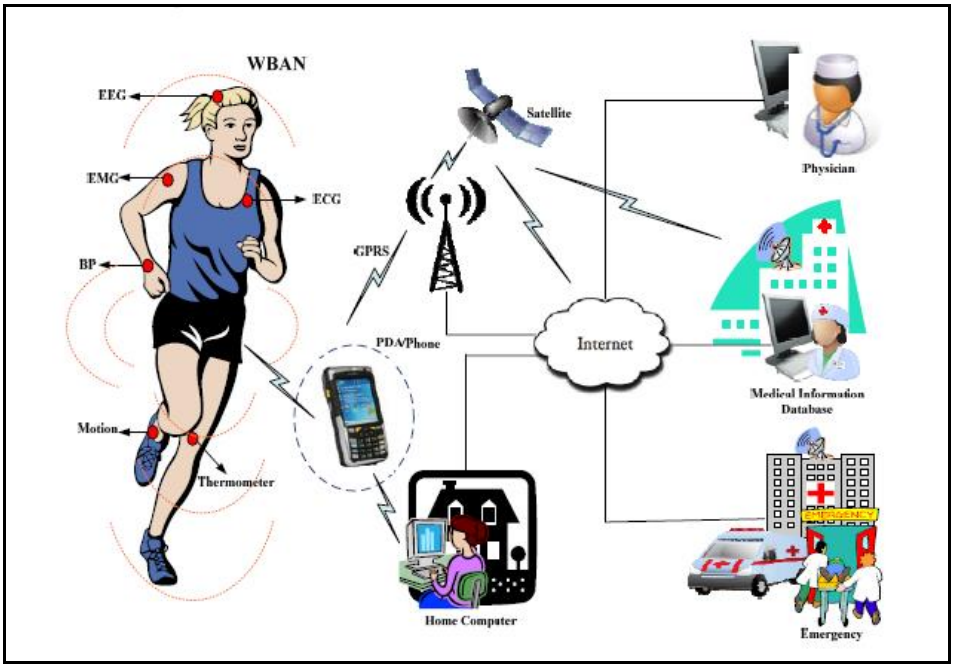

Figure 2 : Structure of Body Area Networks

2. Security Problems in a WBAN in a Single Network

In view of the WBAN applications, various research issues [4] have to be taken into account for effective and reliable usage of WBAN in the intended applications. They are design of radio frequency (RF) wireless systems, channel modeling, quality, antenna design, and reliability, PHY protocol design, MAC protocol design, dissimilar networks connectivity, security, monitoring and privacy. Among the several issues, security issues [5] are more considerable because it completely reduces the sensor-based communication. The main security requirements are listed as follows [3].

- Data Truthfulness, confidentiality, Freshness, Authentication, Security Administration and Availability.

Many new technology solutions are emerging and they have both advantages and disadvantages. The detailed security requirements are explained in [3]. Attacks on WBAN can be at various layers of data communications and the defenses against them are classified in the
Table 1 : "WBAN Security attacks and defenses" : [3]

Layers	**DoS attacks**	**Defences**
Physical	Jamming	Lower duty cycle, Spread-spectrum, mode change, region mapping and priority messages
	Interfering	Hiding and temper proofing
Link	Smash	Error Correction Code
	Unfairness	Small frames
	Collapse	Limitation rate
Network	Negligence and greediness	Searching and redundancy
	Homing	Encryption
	Misdirection	Monitoring authorization
	Black holes	Redundancy, observing and authentication
Transport	Flooding	Client Dilemmas
	De-synchronization	Authentication

Table 1 : WBAN Security attacks and defenses

2.1. IEEE 802.15.4 based Body sensor networks Security framework

Security requirements are attained by using the IEEE 802.15.4 standards in body sensor networks. This framework processes the low-data applications because of the minimum power standard. It is meant for lower network layers of a type wireless personal area network (WPAN) that is utilized to making the effective communication between the devices with high speed and low cost. This is different from more end-user oriented approaches of personal area networks for example Wi-Fi [3]. The IEEE standard is very simple and effective communication as similar to the body sensor networks because of requiring lower cost power and data rate etc.
The Table 2 : "Security in IEEE 802.15.4" shows how the security has been implemented in the standard [6].

Name	**Explanation**	**Access Control**	**Confidentiality**	**Frame integrity**	**Sequential freshness**
Null	No security				

AES-CBC-MAC-32	MAC-32 bit	✓		✓	
AES-CCM-32	MAC-32 bit and Encryption	✓	✓	✓	✓
AES-CTR	CTR and Encryption				
AES-CCM-64	MAC-64bit and Encryption	✓	✓	✓	✓
AES-CBC-MAC-64	MAC-64bit	✓		✓	
AES-CCM-128	MAC128bitand Encryption	✓	✓	✓	✓
AES-CBC-MAC-128	MAC-128 bit	✓		✓	

Table 2 : IEEE 802.14.6 standard related-security

The Table 3 : "Security in IEEE 802.15.6 Standards" shows the 3 levels of security. [1] The security structure is as per IEEE standard 802.15.4 with necessary changes.

Level- 0	Unsafe communication	Here, data has been broadcasted in unsafe frame which means no proper security mechanism is followed to maintain privacy, confidentiality, integrity and authentication.
Level-1	Authentication only	Here, data is transmitted only in secured manner but this process not support the privacy and confidentiality.
Level-3	Authentication and encryption	Data is transmitted in secured authentication and encryption frames addressing all problems not covered in the above levels 0 and 1. (See Figure 3) when every time, node enter in the network, the security is maintained with the help of master key, new key , group temporal key and pairwise temporal key. These keys are helps to achieve the multicast communication.

Table 3: Security in IEEE 802.15.6 Standards

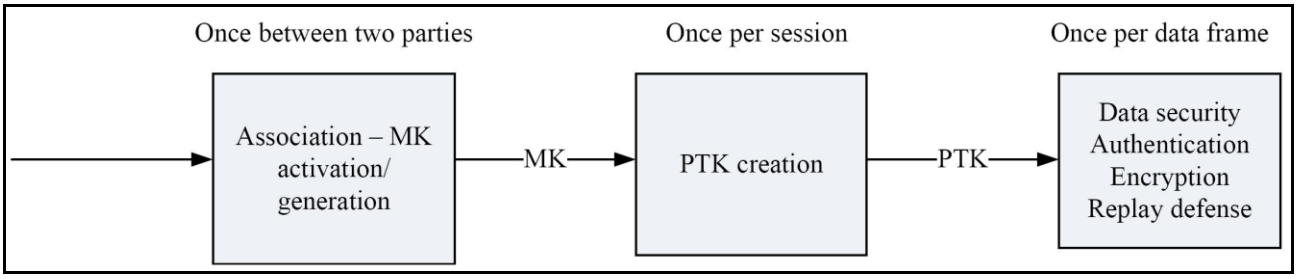

Figure.3. IEEE 802.15.6 Standards Security Structure

2.2. Security problems and solutions

The protocol well-defined in the IEEE 802.15.4 MAC has some security issues to be addressed. The protocol consists of a super frame configuration containing of active and inactive periods as illustrated in Figure 4. The system-consists are three constituents such as beacon, contention access period (CAP) and contention free period (CFP). The coordinator communicates with the nodes at the time of rest period (active and inactive). This communication is established only 7 GTS slots to minimize the traffics. During the beacon communication mode, CA/CSMA protocol is utilized to making the effective communication. Finally, the unspotted CSMA/CA protocol is utilized in the non-beacon mode communication.

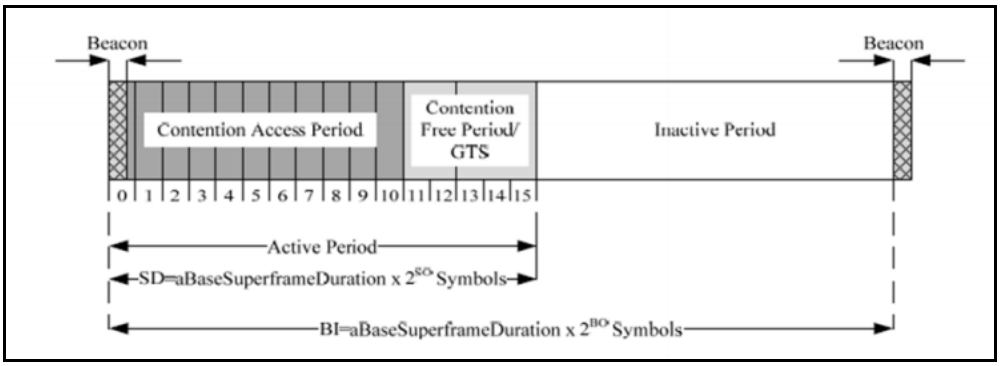

Figure 4 : Beacon enable mode based IEEE 802.15.4 communication structure

The IEEE 802.15.4 framework influenced by several attacks therefore, different GTS slots are required to enable the secure communication when compared to the weak and random attackers. Hence the framework is created to manage the various traffics and vulnerable attacks [7] during the communication. To attain the issues, different security structure is created to predict the intermediate and back off attacks. The introduced methods should manage the security by increasing the network throughput. In addition to this, different security approaches to develop for deciding the sender back off windows. The back off windows helps to identify the attacks and penalize the adversaries effectively in receiver side. To consider these factors, game theoretic approach is utilized to identify the threats and attacks effectively [3],[8].

3. Security issues in WBAN in Multiple Networks

The wireless communication for Body Area Networks has been increasing in terms of traffic and application recently. This has led to the use of WBAN networks in collaboration with multiple networks broadly called Cooperative Networks. They are of 2 types:

- Multiple similar or homogeneous WBAN networks collaborating and cooperating together from performance and reliability points of view: The objective is to communicate the data more effectively from source to destination.

- WBAN network communicating with other types of networks of different types from the application of view: The goal is to transfer the data to other networks of other types for transferring the data for further processing. As a part of this, there will be a scenario by which the WBAN consisting of the patient, sensors and data gathering may be mobile and will communicate through different and heterogeneous networks during the data gathering.

3.1. Cooperative Networks for Performance and Reliability

Jibe Dong and David Smith, in their paper "Cooperative Body-Area-Communications: Enhancing Coexistence without Coordination between Networks" has analyzing the co-occurrence of the various mobile body sensor networks. The sensor networks use the cooperative communications to manage the effective communication [9].

In general BAN should be responsible for extremely reliable communication with little transmission power. As there may be large path losses for single link star topology [10] [11], IEEE 802.15.6 provides two-hop cooperative communications as an option [12] which has been found to give significant performance benefits using either narrow-band [13] to [16] or ultra-wideband [17]. However as the WBAN is being used extensively with multiple WBANs being closer to each other, the coexistence is becoming an issue. IEEE 802.15.6 standard requires that system should maintain reliable performance with up-to 10 WBANs co-located in a 6 x 6 x 6m space. So a new technology called Cooperative Network Coding (CNC) addresses this issue by providing effective decode-forward protocol with two relays, two hop links and selection combining at hub (or gateway device) using suitable time-division multiple-access (TDMA) scheme enabling intra-network and inter-network operation [18]. It is found that this approach provides significant performance improvement, increased the throughput and network reliability. [9] [19].

3.2. Cooperative Networks for Data Transfer and Processing

Xizang Huang has done extensive research in the Efficient Cooperative Communications for Wireless Body Area Networks where the networks are of different types and hence called heterogeneous networks. [18]. The Cooperative networking is highly relevant in medical applications as the WBAN devices have to transmit data across various networks as given in the Figure 5. Also if the WBAN devices are attached to the patient who himself / herself is mobile (for example moving in a vehicle or ambulance to the network of the hospital etc.), then the WBAN communications should be communicated across different networks. The body sensors are classified as medical and non-medical sensor; classified as biosensor and motion sensor. Further the traffic is classified into video stream [20], parameter stream and wave-form real time stream.
The sensors are utilized in healthcare applications because, it has high priority data transmission, time and veridical based data acquisition, channel characterization and patient mobility, time varying and dynamic environment. In addition to this, the sensors are utilized to record ECG, EEG related uncompressed videos also records the human postures and limb movement.

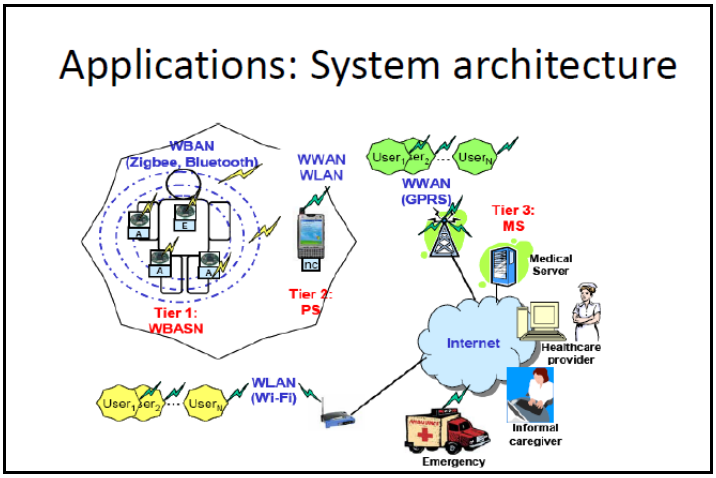

Figure 5 : Applications : System Architecture
In a cooperative network as above where data has to be transferred and processed across multiple networks and the networks have to be cooperative, issues arise in proper design of the protocols for the routing. Such routing typically is taken care at MAC layer level. So the issues in this level are

- Designing network MAC protocols to enable WBANs adaptively and intelligently balance the QoS requirements and unique constraints
- Designing cooperative communication protocols for WBANs
- Combining minimum energy route and low duty cycle scheduling to maximum network lifetime of WBANs while satisfying QoS requirements is a challenging issue.

Internetworking: (See Figure 6) : Issues [18]

The research shows that there are many challenges to be overcome in the type of cooperative networks which are heterogeneous

- It is obvious that allocating bandwidth efficiently when integrating heterogeneous wireless networks is a challenge
- How to provide medical QoS consistently over integrated WI-Fi- wireless networks is a challenge research.
- • How to efficiently manage radio resources, manage scheduling, and control connection admission are still open issues in networks; they are also critical in integrated Wi-Fi wireless networks for E-health services.
- Hand over management for seamless integration of wireless networks and for providing continuous E-health service for mobile users may be one of the most challenging issues, due to the transfer of vital medical in formation through dynamic wireless channels and networks.
- A challenge issue is how to efficiently manage the spectrum to accommodate different applications using cognitive radio technology.
- How to design are source-aware secure mechanism within WBAN and with heterogeneous networking.

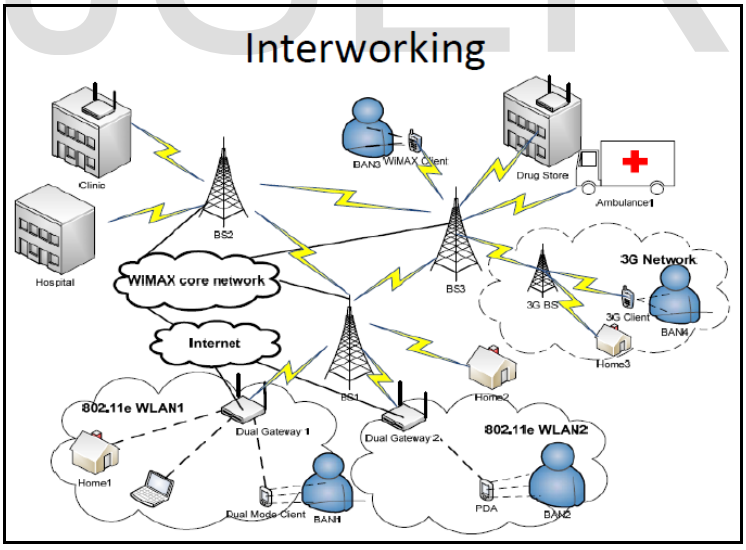

Figure 6 : Internetworking

Some of the Mechanisms being followed in cooperation are :

- With the dimensions DF and AF:
- Fixed relaying
- Selection relaying
- Incremental relaying
- Incremental transmission relay selection (ITRS)

- Multi-hop with relay selection (MHRS)

There is no cooperative protocol which has been designed for WBANs. The Cooperative Networking has to integrate WBANs or sensor networks to other heterogeneous networks such as cellular/WiFi networks in ubiquitous computing.

3.3. Need for Heterogeneous Networks for WBAN

As described above, WBAN requires operating in a heterogeneous network to effectively transfer data and for further processing. With this need, there are many issues which are to be examined for effective implementation of heterogeneous network. This has opened up many research issues [21].

3.4. Cognitive and Cooperative Communications for HetNet

Xing Zhang_, Yue Gaoy, et al, in their paper "Cognitive and Cooperative Communications in Wireless Heterogeneous Networks (Hetnet): Current Status and Technical Perspectives" have done extensive study in HetNet and has proposed an architecture for the integration of cognitive
Networks and co-operative communication in wireless HetNet. [22]. Based on the proposed architecture several techniques related to the integration of cognition and cooperation is evaluated. Techniques like cognitive relay network, geolocation-based cognition and cognitive and cooperative gateway can be effectively applied. Simulations and analysis have been conducted showing that the combination of cognition and cooperation can significantly improve the system performance.

3.5. Mobile Cloud Computing (MCC) Enabled WBAN Architecture

With the advent of Cloud Computing and Mobile Computing, the WBAN data gets created, transmitted to, processed at and stored at various nods in a network which include Cloud Computing environment and Mobile Computing front end interfaces. So this raises a scenario of another type of heterogeneous networks of WBANs. Figure 7 depicts such a MCC-capable framework for a pervasive healthcare system and it is studied in [23].

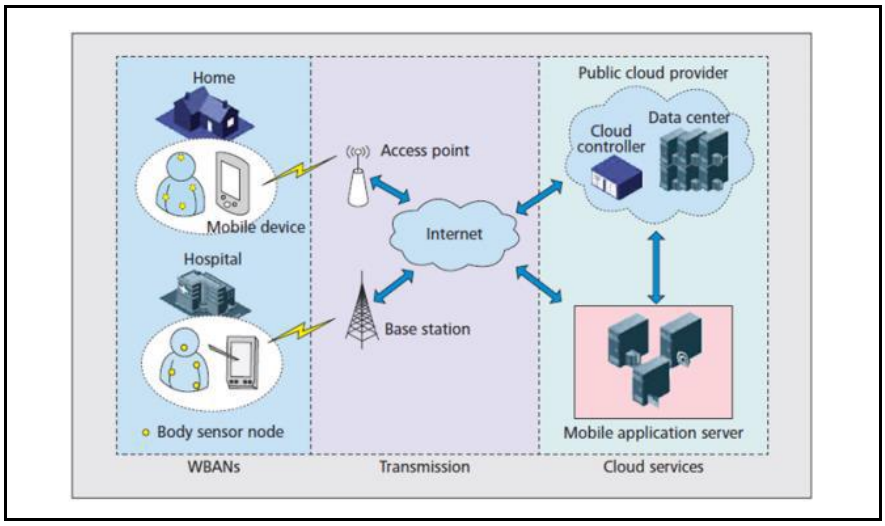

Figure 7: Conceptual architecture for WBANs with MCC capability

3.6. Protocols for Cooperative Communications: Coop-MAC

Cooperation means that a virtual antenna array is formed when multiple nodes in a wireless network collaborate to form a virtual antenna array. Across the nodes of the network deprived of separately node necessarily having numerous antennas. It is basically different from multichip communications in which the destination only receives one version of the message from the source.

Some basic aspects requiring study and research include: theoretical tools to aid in the design of cooperative networking systems, as well as effective incentive mechanisms the nodes to cooperate, new protocol design at physical and network (especially MAC) level for cooperative networks including security mechanisms. Such issues are under research.

Cooperative communications consists of schemes and techniques which implement the transmission of data from source station to destination station through one or more intermediate nodes called helpers. These are achieved at MAC layer level by modifying the MAC protocols as appropriate and such schemes and the security issues have been discussed. [24]. One of such MAC protocols is Cosmic which describes how the legacy IEEE 802.11 [25] can be modified to implement such cooperative communications and it is detailed in [26] and [27].

As the cooperative communication of data is through one or more helpers using the Coop MAC, the scheme raises a few potential security issues.

3.7. Security Implications in Cooperative Communications in Cosmic Protocol

As the cooperative communication of data is through one or more helpers using the Coop MAC, the scheme raises a few potential security issues:

- The assister may object services to the sender by not forwarding the data to destination. This requires that the source should every time ensure that the data has been received at the destination through helper within the given time by receiving an acknowledgement. The source should have a time out mechanism and if the source finds that the data has not been received within the time, the source should send the data through some other helper or send directly to the destination knowing that it will be in low rate.

- The major security issue is the intermediate user access the sources and the acknowledgement is sending in the name of destination. The sources wrongly assumed the destination person send that particular acknowledgement. Therefore, Cosmic is applied to identify the variation between the request, response and acknowledgement (CTS) scheme. The scheme generates the frame used to aware the destination activities in future. If the source does not have any frame value they NAV period is applied to detect the spoofing activities and the frame is transmitted to the destination to confirm about the frame.

- Another problem is a situation where the assistant changes the data and forwards it. The receiver will not be able to identify this and may even send back any sensitive data back to source through the helper. This requires an action by source at application level that it identifies wrong responses and hence takes appropriate action.

3.8. Security in presence of Cosmic

To address the above potential security issues in the cooperative communication using Cosmic protocol scheme, the packet header information has to be changed at the same not violating the IEEE 802.11i standard header format. As a result, the current approach to implementing Cosmic is incompatible with 802.11i [28]. Integrity

check is performed in both TKIP and AES modes are done by calculation of message integrity check (MIC) calculated at source and checked at destination. This check covers MAC packet header as well as actual data being transmitted. Thus if the helper changes or introduces new data, the check will fail and so destination will not send acknowledgement (ACK). So the source will identify that there is an issue and so will send the data again. So, in order to solve security concerns in a cooperative network, we must modify the protocol in terms of header data format.

Following a thorough examination of 802.11i and Cosmic implementation, Salik Makda, Anku- Choudhary, and colleagues proposed two possible solutions in their paper " Security Implications of Cooperative Communications in Wireless Networks" in order to make Cosmic compatible with the IEEE 802.11i architecture: [24], as shown in Figures 8 and 9.

Figure 8 : Scheme for two header

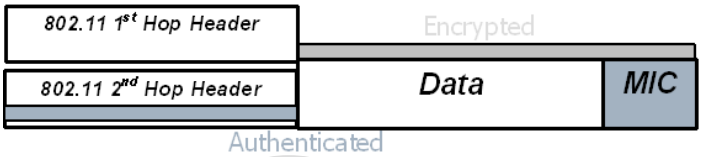

Figure 9 : Scheme for single header

4. Security Models using Artificial Intelligence techniques

As described in previous sections, the challenges in security can be largely addressed in the Data Link Layer in particular MAC layer. So the protocols implemented in MAC layer should have the intelligence to protect against various types of attacks and implement the defense mechanisms. The intelligence has to implement the defense mechanisms to address the known attacks and to modify or upgrade for newer attacks which we will come across in future. There can also be a provision for self learning over time.

Various artificial intelligence models have been used for modeling network security in the past. We can consider implementing such models for WBAN security in individual as well as heterogeneous networks.

Use of Bayesian Networks : In the paper by Peng Xie_, Jason H Li_, Xinming Ou†, Peng Liu, Renato Levy, "Using Bayesian Networks for Cyber Security Analysis", [29] the authors have presented their work on modeling cyber security considering that cyber security attacks are uncertain and hence have to be modeled accordingly. The authors have effectively used previous work in this area in [30] to [34].

Use of Neural Networks : The paper "Network Based Intrusion Detection Using Neural Networks" [35] by Alan Bivens, Chandrika Palagiri, Rasheda Smith, Boleslaw-szymanski, and Mark Embrechts used the neural network approach for modelling network based intrusion detection (using maps for data clustering) and detection. Many methods have been used to detect intrusions. In [36–41], the authors effectively used and compared previous work in this area.

Use of Game Theory : In their paper, "Game Theory for Network Security," IEEE Communications Surveys Tutorials, [42], Xiannuan Liang and Yang Xiao reviewed existing game-theory based solutions for network security problems, categorising their application scenarios into two categories (a) modelling for attack-defense

analysis and (b) modelling security measurement. Furthermore, they provided a brief overview of the game models in those solutions and classified them into two categories: cooperative and non-cooperative game models, with the latter consisting of subcategories. In [43–46], the authors effectively used and compared previous work in this area.

4.1. Game Theory for modeling WBAN HetNet Network Security

The effectiveness of the system is evaluated by investigating the defense-attack interactions which are analyzed using the below scenario. First, the attacks are happened in the computer devices or networks, or nodes and systems. Second, the network or system responds to the attackers. The below terms are utilized to investigate things the game theory modelling [42].

- The system which may be host, device, node, process and software entity that used to collect the data.
- The person creates the attacks and affects the system performance and causes to loss the data.
- The system is targeted and the attacked continuously.
- Intrusion detection system (IDS) that used to monitoring the system activities to identify the intrusion activities. The IDS system having the alarm process which helps to identify the attacks.

From the analysis, the system or applications are requires the security modelling to reduce the intermediate attacks and unwanted user activities. The game theory approach has players they are placed on the security activities; here two players are involved in these activities to identifying the attacker and defending activities. During the analysis, intrusion detection system detects the attackers because the security game is more important. The created intrusion system reduces the unwanted activities also ensures the error-free data transaction.

4.2. Restrictions of existing models and proposal for use of the models

The limitations of existing game models are discussed in detail in Biannual Liang and Yang Xiao's paper [42]. Despite their limitations, game theoretic approaches have proven to be effective tools for addressing network security issues. As a result, it is proposed that Game Theory be used to effectively model security attacks and counterattacks in WBAN in Heterogeneous Network. In this paper, however, an advanced model of Game Theory with Stackelberg Security Equilibrium (GTSSE) is proposed.

5. Game Theory with Stackelberg Security Equilibrium (GTSSE)

5.1. Overview of GTSEE

The body sensor network uses the set of sensor devices that collects the patient health information which is processed by using the Game Theory with Stackel-berg Security Equilibrium (GTSSE) approach. The GTSSE method works according to the player's involvement that maintains the patient authority. The position authority in GTSSE is the organizer and all the players react to the organizer decision. The organizer decision in WBAN handles the information with higher security through game theory approach. The organizer places security resources and handles all type of errors at various potential targets of WBAN. [47]

The leadership model is applied to analyze the data in which the leader moves first and their firms are moved. During this process, price function P is utilized to investigate the cost structure. Then the entire output is computed as P(Q1 + Q2) where the Q1 represents the leader and Q2 represents the follower. Suppose the leader firm has the cost structure C1(Q1). After observing the quantity of the leader, the leader considers how the follower will respond. Based on this, the leader selects a quantity that will maximize its profile or benefits, anticipating that the follower will observe the leader's action and respond accordingly to select a quantity that will maximize its profit or benefits. When the follower picks up this quantity, the market enters a state of equilibrium.

Stackelberg Security Equilibrium is introduced to handle the multiple patients' health monitoring simultaneously with minimal energy consumption in WBAN. In the case of heterogeneous network, the WBAN node has to consider itself as a leader and all the other nodes of heterogeneous networks as other players following the leader and potential attackers. Stackelberg Security considerably improves the strength of solution with higher security.

5.2. Experiment and results with GTSSE approach

This work discussing the secure patient health data transmission in the body sensor networks [48]. The main contribution of this work is listed as follows.

- The system uses the game theory approach is utilized to manage the data security also monitoring the patient health. The collected information sis interconnected with personal system and the stores the information in data server.
- Second, the system uses the Stackel-berg security equilibrium approach that helps to analyze the patient health monitoring with mathematical model.
- At last, the Kirchhoff-von Neumann theory is applied to reduce the response time and increase the high security while exchanging data using body sensor networks.

The discussed game theory approach compared with the existing methods such as batched group key management (BGKM) [50], Smart Wearable Systems (SWS) for Health Monitoring (HM) (SWS-HM) [49]. The discussed system is implemented using the NS2 simulation tool and the effectiveness is evaluated in terms of energy consumption and security factors. Thus the introduced system ensures the minimum response time, reduces the information loss with high data delivery rate.

6. Conclusion

In conclusion, the challenges of security in heterogeneous networks can be best addressed by implementing defense mechanisms in the MAC layer of WBAN network communication, addressing current attacks while also easily adapting to future attacks. Various artificial intelligence models have been used in the past to model network security. We can think about implementing such models for WBAN security in both individual and heterogeneous networks. The Stackel-berg Security Model, among the various game theory models, significantly improves the strength of the solution with higher security.

References

[1] Kyung Sup Kwak, Sana Ullah, Niamat Ullah, "An overview of IEEE 802.15.6 Standard", 3rd International Symposium on Applied Sciences in Biomedical & Communication Technologies (ISABEL2010) in Rome, Italy

[2] IEEE Standards Association : http://standards.ieee.org/about/get/802/802.15.html

[3] S. Saleem, S. Ullah, and K.S. Kwak, A Study of IEEE 802.15.4 Security Framework for Wireless Body Area Networks, Sensors, vol.11, No.2, pp. 1383-1395, 2011.

[4] Maulin Patel and Jianfeng Wang : Applications, challenges, and prospective in emerging body area networking technologies , Journal IEEE Wireless Communications Volume 17, Issue 1, February 2010, pp 80-88.

[5] Ming Li, Wenjing Lou and Kui Ren , Data security and privacy in wireless body area networks, Journal IEEE Wireless Communications Volume 17, Issue 1, February 2010, pp 51-58.

[6] Xiao, Y.; Chen, H.H.; Sun, B.; Wang, R.; Sethi, S. MAC security and security overhead analysis in the IEEE 802.15.4 Wireless Sensor Networks. EURASIP J. WCN 2006, doi:10.1155/WCN/2006/93830.

[7] S. Saleem, S. Ullah, and K.S. Kwak, A Study of IEEE 802.15.4 Security Framework for Wireless Body Area Networks, Sensors, vol.11, No.2, pp. 1383-1395, 2011.

[8] M.Somasundaram and R. Sivakumar, "Security in Wireless Body Area Networks : A survey" **,** International Conference on Advancements in Information Technology 2011 (ICAIT 2011), December 2011.

[9] Jie Dong, David Smith, "Cooperative Body-Area-Communications: Enhancing Coexistence Without Coordination Between Networks ', IEEE 23rd International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC) , 2012 , pp 2298-2303

[10] K. Yazdandoost and K. Sayrafian-Pour, "TG6 channel model ID: 802.15-08-0780-12- 0006," IEEE submission, Nov. 2010.

[11] D. Lewis, "IEEE 802.15.6 call for applications - summary ID: 802.15-05-0407-05," IEEE submission, July 2008.

[12] A. Astrin et al., "IEEE Standard for Local and metropolitan area networks part 15.6: Wireless Body Area Networks: IEEE Std 802.15.6-2012," Feb. 2012.

[13] J. Dong and D. Smith, "Cooperative receive diversity for coded gfsk body-area communications," Electronics Letters, vol. 47, no. 19, pp.1098 –1100, Sep. 2011.

[14] D. Smith and D. Miniutti, "Cooperative body-area-communications: First and second order statistics with decode-and-forward," in Wireless Communications and Networking Conference (WCNC), 2012 IEEE, Paris, France, Apr. 2012.

[15] R. D'Errico, R. Rosini, and M. Maman, "A performance evaluation of cooperative schemes for on-body area networks based on measured time variant channels," in Communications (ICC), 2011 IEEE International Conference on, June 2011, pp. 1 –5.

[16] P. Ferrand, M. Maman, C. Goursaud, J.-M. Gorce, and L. Ouvry, "Performance evaluation of direct and cooperative transmissions in body area networks," Annals of Telecommunications, vol. 66, pp. 213–228, 2011.

[17] Y. Chen et al., "Cooperative communications in ultra-wideband wireless body area networks: Channel modeling and system diversity analysis," Selected Areas in Communications, IEEE Journal on, vol. 27, no. 1, pp. 5 –16, Jan. 2009.

[18] A. Zhang, D. Smith, D. Miniutti, L. Hanlen, D. Rodda, and B. Gilbert, "Performance of piconet coexistence schemes in wireless body area networks," in Wireless Communications and Networking Conference (WCNC), 2010 IEEE, Sydney, Australia, Apr. 2010, pp. 1 –6.

[19] Gabriel E. Arrobo, Student Member, IEEE and Richard D. Gitlin, Life Fellow, IEEE, " Improving the Reliability of Wireless Body Area Networks', 33rd Annual International Conference of the IEEE EMBS Boston, Massachusetts USA, August 30 - September 3, 2011, pp 2192 - 2195

[20] Energy Efficient Cooperative Communications for Wireless Body Area Networks by Xigang Huang - A thesis presented to the University of Waterloo in fulfillment of the thesis requirement for the degree of Master of Applied Science : https://uwspace.uwaterloo.ca/bitstream/handle/10012/5753/Huang_Xigang.pdf?sequence =1

[21] "HetNets – A New Paradigm for increasing cellular capacity and coverage", Guest Editorial, IEEE Wireless Communications, June 2011

[22] Xing Zhang_, Yue Gaoy, Zhi Yan_, Xiao Jiang_, Fei Pengy, Laurie G. Cuthberty and Wenbo Wang, "Cognitive and Cooperative Communications in Wireless Heterogeneous Networks (HetNet): Current Status and Technical Perspectives', IEEE International Conference on Wireless Information Technology and Systems (ICWITS), 2012 , pp 1-4

[23] Jiafu Wan., Caifeng Zou., Sana Ullah., Chin-Feng Lai., Ming Zhou., Xiaofei Wang., "Cloud-Enabled Wireless Body Area Networks for Pervasive Healthcare," IEEE on Transaction on Network, (Volume:27 , Issue: 5), September / October 2013

[24] Salik Makda†, Ankur Choudhary_, Naveen Raman†, Thanasis Korakis†, Zhifeng Tao, Shivendra Panwar, " Security Implications of Cooperative Communications in Wireless Networks', Sarnoff Symposium, IEEE 2008, pp 1-6

[25] "Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," ANSI/IEEE Std 802.11, 1999 Edition, 1999.
[26] P. Liu, Z.Tao, and S. Panwar, "A Cooperative MAC Protocol for Wireless Local Area Networks," in Proceedings of IEEE ICC'05, June.
[27] T. Korakis, Z. Tao, S. Makda, B. Gitelman, and S. Panwar, "To Serve is to Receive Implications of Co-operation in a Real Environment," in Proceedings of Networking 2007, June.
[28] "Amendment 6: Medium access control (mac) security enhancements," ANSI/IEEE Std 802.11, 1999 Edition, 1999.
[29] Peng Xie_, Jason H Li_, Xinming Ou†, Peng Liu‡, Renato Levy, "Using Bayesian Networks for Cyber Security Analysis", Conference on Dependable Systems and Networks, 2010, pp.211-220.
[30] Magnus Almgren, Ulf Lindqvist, and Erland Jonsson. A multi-sensor model to improve automated attack detection. In RAID 2008. RAID, September 2008.
[31] Marcel Frigault and Lingyu Wang. Measuring network security using bayesian network based attack graphs. In STPSA'08, 2008.
[32] Marcel Frigault, Lingyu Wang, Anoop Singhal, and Sushil Jajodia. Measuring network security using dynamic bayesian network. In Proceedings of the 4th ACM workshop on Quality of protection, 2008.
[33] Saurabh Bagchi Gaspar Modelo-Howard and Guy Lebanon.Determining placement of intrusion detectors for a distributed application through bayesian network modeling. In RAID 2008. RAID, September 2008.
[34] Xinming Ou, Wayne F. Boyer, and Miles A. McQueen. A scalable approach to attack graph generation. In CCS 2006, pp 336–345, 2006.
[35] Alan Bivens, Chandrika Palagiri, Rasheda Smith, Boleslawszymanski, Mark Embrechts, " Network based Intrusion Detection Using Neural Networks", Proc of Intelligent Engineering Systems through Artificial Neural Networks (ANNIE) 2002, Vol 12, ASME Press, pp 579-584
[36] Kohonen, T, 1995, "Self-Organizing Maps," Springer Series, Springer-Verlang Berlin.
[37] Lippmann, R., and Cunningham, R., 1999, "Improving Intrusion Detection performance using Keyword selection and Neural Networks, " RAID Proceedings, Sept, West Lafayette, Indiana.
[38] Lippman, R., Haines, J.., Fried, D., Korba, J., and Das, K., 2000, "The 1999 DARPA offline intrusion detection evaluation," Computer Networks, 34, pp. 579-595.
[39] Niggemann, O., Stein, B., and Tölle, J., 2001, "Visualization of Traffic Structures," IEEE International Conference on Communications, ICC 2001, vol. 5, pp. 1516 -1521.
[40] Portnoy L., Eskin E., and Stolfo S. J., 2001, "Intrusion Detection with Unlabeled Data using Clustering," In Proceedings of ACM CSS (DMSA-2001), Philadelphia, PA, Nov 5- 8.
[41] Ryan, J., Lin, M., and Mikkulainen,R., 1998, "Intrusion Detection with Neural Networks," Advances in Neural Information Processing Systems, vol. 10, MIT Press.
[42] Xiannuan Liang and Yang Xiao, Senior Member, IEEE, , " Game Theory for Network Security", IEEE Communications Surveys Tutorials ", Vol 15, No. 1, First Quarter 2013, pp 472-486,
[43] T. Alpcan and T. Baser, "An intrusion detection game with limited observations," Proc 12th Int. Symp. on Dynamic Games and Applications, 2006. Available: http://www.tansu.alpcan.org/papers/isdg06.pdf.
[44] S. N. Hamilton, W. L. Miller, A. Ott, and O. S. Saydjari, "The role of game theory in information warfare," Proc. 4th information survivability workshop (ISW-2001/2002), 2002. Available: http://www.cert.org/research/isw/isw2001/papers/index.html.
[45] Security measurement- white paper, http://www.psmsc.com/Downloads/TechnologyPapers/SecurityWhitePaper v3.0.pdf.
[46] W. He, C. Xia, H. Wang, C. Zheng, and Y. Ji, "A game theoretical attack-defense model oriented to network security risk assessment," 2008 International Conference on Computer Science and Software Engineering, pp. 498 - 504, 2008
[47] Stackelberg competition, http://en.wikipedia.org/wiki/Stackelberg_competition

[48] M. Somasundaram and R. Sivakumar, "Game Theory Based Security in Wireless Body Area Network with Stackelberg Security Equilibrium", The Scientific World Journal, Volume 2015 (2015), Article ID 174512, 9 pages, http://dx.doi.org/10.1155/2015/174512

[49] M. Chana, D. Estèvea, J.-Y. Fourniolsa, C. Escribaa, and E. Campoa, "Smart wearable systems: current status and future challenges," Artificial Intelligence in Medicine, vol. 56, no. 3, pp. 137–156, 2012. View at Publisher · View at Google Scholar

[50] C. K. Ho, T. S. P. See, and M. R. Yuce, "An ultra-wideband wireless body area network: evaluation in static and dynamic channel conditions," Sensors and Actuators A: Physical, vol. 180, pp. 137–147, 2012. View at Publisher · View at Google Scholar · View at Scopus

****