

Security issues in Mobile Wireless Body Area Networks

Manisha Mittal
Phd Scholar
Noida International University
Uttar Pradesh, India

Dr. D.K. Chauhan
Director Technical
Noida International University
Uttar Pradesh, India

Abstract – When a Body Sensor Network (BSN) that is linked to the backbone via a wireless network interface roams from one coverage zone to another then in between wireless-body-area-networks (WBAN) interference created, which can cause serious throughput degradation and energy waste. When a wireless body area network become mobile then problem arises of inter process interference A necessity appears for efficient WBAN monitoring information extraction, high spatial reuse, dynamically fine tuning the monitoring process to suit the data quality, provision for allowing the translation of high-level requirements of medical officers to low-level sensor reconfiguration. Issues related to security and possible solutions must be taken in the research. Study brings out that the current proposed solutions in security are still having limitations needing further research. This paper proposes an optimized BSN handover strategy, RASS (Real-time Accurate & Scalable System) and VMISO (Virtual Multiple Input Single Output) system implementation in WBAN, and procedure to maximize the network throughput by jointly selecting stable routes and assigning channels avoiding inter- and intra-flow interferences based on mobility prediction.

Keywords – Body Sensor Network (BSN), wireless-body-area-networks (WBAN), RASS (Real-Time, Accurate, and Scalable System), VMISO (Virtual Multiple Input Single Output), Inter-WBAN scheduling (IWS)

I. INTRODUCTION

A Wireless Body Area Network can be treated as a “Personal Sensor Network” as it is formed by combination of simple star network of a group of Wireless Sensor Nodes and a Central Processing Node. Fig.1. Show some of basic network type and WBAN.

Recent advances facilitate Body Area Networks with personal gadgets, sensing and monitoring technology for in-body and near-body use, miniaturization, and energy-efficient wireless and sensor networks. A WBAN thus has a high chance of encountering other WBANs, which creates new issues of inter-WBAN scheduling (IWS). Corresponding discussions [5], [6], [7], [8], [9] have just been opened and comprehensive studies are still required. Apart from the more macro platforms such as cell phones and laptops, computing devices are now being worn or even implanted into patients and used to monitor various aspects of wearer’s physiology and ambient environment.

Unfortunately, WBANs have unique constraints as compared to traditional networks, rendering the existing security measures implemented for wired or wireless communication network impracticable. These constraints are basically due to the limitations on the sensor nodes’ memory, energy, processing power and the ad hoc wireless channel used. To adhere to the constraints faced by sensor nodes, the security scheme should be carefully designed and should be based on the intended applications and be aware of the possible threats to the applications. In other words, the security scheme should be developed after identifying the type and nature of the intended applications.

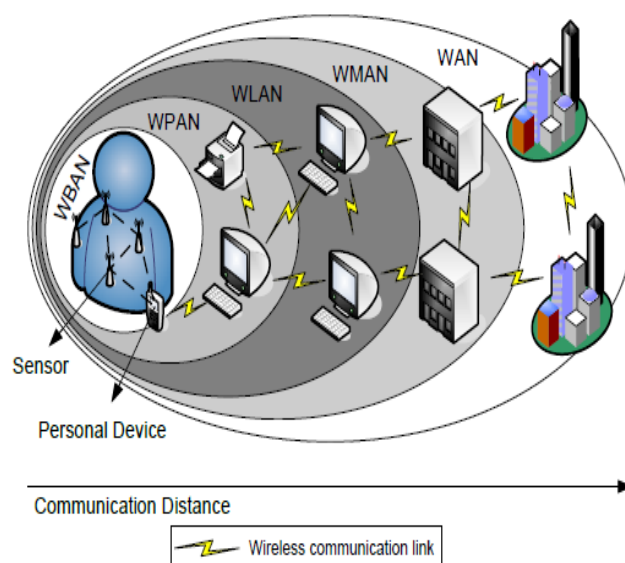


Fig. 1 Positioning of a Wireless Body Area Network in the realm of wireless networks. [22]

Examples include heart-rate monitors, glucose-monitors, accelerometers, medical implants and so on.

II. PROBLEMS IN MOBILE WBAN

In multichannel monitor system, as shown in fig 2. Different sensor nodes which are tracking different fields interfere each other. Problem also rises of best node deployment and decision of number of nodes per channel deployment. As more number of nodes results improvement in tracking accuracy but side by side increase interference.

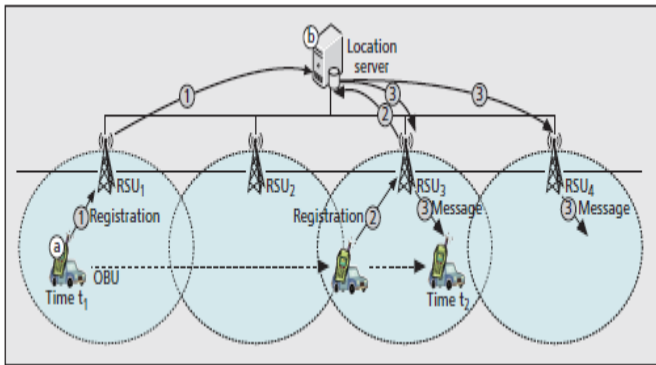


Fig.2 Basic Mobility Management Mechanism (BMM) [23]

Also one approach is to enable more efficient monitoring techniques, which could provide various benefits, like the examination of patients based on their criticality, which in turn enhances doctor's time efficiency in examining patients, and lowers queues in emergency rooms, and accurate monitoring of patients conditions and trends over a period of time. [2]. But problems rises during this process like ability for medical officers to set requirements and, where these requirements can drive the operation of the sensors

II. SECURITY THREATS IN WBAN AND SOLUTIONS

A common scenario of BSN is utilized by [1] the physiological information collected by body sensors is forwarded through a portable personal server to an access point (AP). The AP can then forward the information to the target system or end-user. If handover strategy is implemented on the portable personal server of a BSN, then if the BSN user roams from one AP's coverage zone to another. Then the handover strategy comprises four steps, viz. trajectory tracking, position prediction, formulation of confidence probability, and hand over initiation.

Mostly invasive attacks happen through the physical capture of the sensor node. While preventing node capture in large distributed WSNs deployment area is almost impossible, the focus should be on securing the confidential data in the sensor node. Non-invasive attacks, such as side-channel attacks, are also possible in sensor networks. Study by [12,13] have shown that side-channel attacks can be launched by taping the signal from the chip and using simple power analysis as well as differential power analysis to reconstruct the data. Their results suggest the possibilities of extracting several key bits through the power analysis attack.

Another form of non-invasive physical attack is by exploiting the Bootstrap Loader (BSL) and happens mostly during the boot up process. By having access to the boot devices and debug session, attackers will be able to analyze the systems and its operation thus providing them with

enough information to clone the system, insert malware and disturb the overall operations of the sensor node and its systems [14, 15].

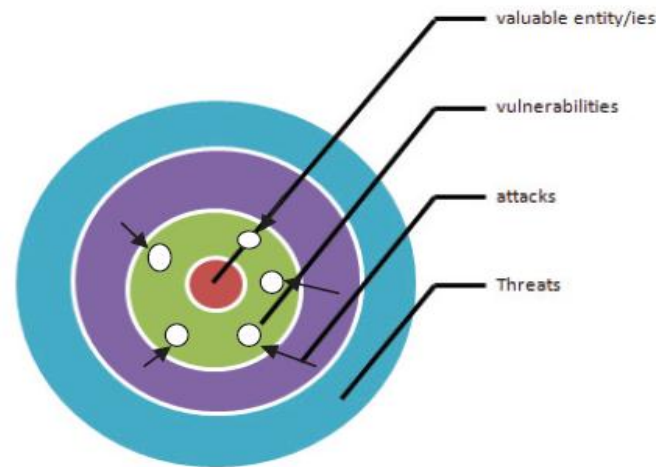


Fig 3. Threats, attacks and vulnerabilities (TAV)[24]

More recently, over-the-air programming has been employed for remote software update. Although it has been found useful for researchers and network owners, the procedure generally leaves the door "wide open" for injection of malicious code. Even though it is hardly done due to Harvard architecture type of memory, Francillon [15] in his work has successfully injected malicious code in Micaz class nodes thus triggering the alarm for the need of holistic security scheme for wireless Body Area Network.

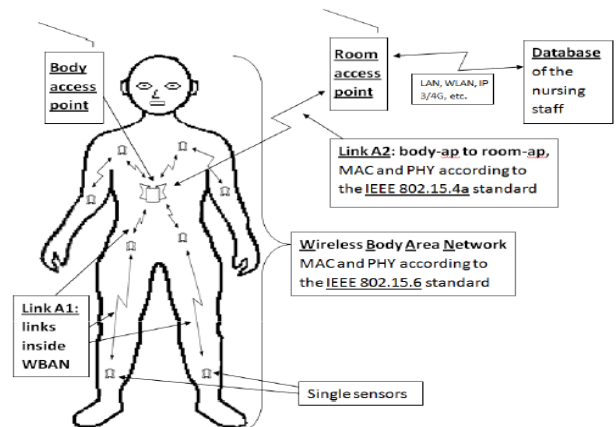


Fig 4. Various research area in WBAN[16]

Another interesting work reported by [17] further classifying the attacks into semi-invasive attacks. Semi-invasive attacks require repackaging of the processor to get access to its internal layer. However, no electrical contact is required as compared to invasive attacks and therefore represents greater threat to the hardware based security. So if fault injection is done successfully towards attacks to modify

memory content and also extract data from powered-off memory devices.

It can be concluded that the intention of the physical types of attacks can vary from destroying the sensor node, extracting confidential data and finally to being falsely authenticated or authorized in the network. Successful physical attacks will usually leads to node cloning attack and therefore create another demand to differentiate between cloned and genuine node in the network. Today, in embedded systems, crypto-processors or physically secure processors have been used extensively to provide some level of resistance to physical tampering. Even though attacks on crypto-processors are known to occur, they still provide the first line of defence against physical tampering. Therefore, optimizing crypto-processors to fit the low-cost, lowenergy requirements of sensor networks can play a significant role in raising the security level. Subsequent section will briefly discuss on the available and possible security chips to address the above physical tampering issues in WSN.

RASS tracking system utilizes TelosB [10] sensor nodes in multi channels to monitor different area of the tracking field. It suggests Space Time communication technique that leverages the spatial and temporal variations of the channel to significantly enhance the performance of wireless networks [3]. This communication paradigm can be realized using multiple antenna element arrays where the antenna elements are separated sufficiently (of the order of the wavelength of the carrier used) such that the channel fading of each antenna is independent. This approach is called *cooperative communication* or a virtual antenna array communication.. Depending on the number of cooperating nodes used at the transmitting and receiving ends of a link, a virtual MISO (VMISO), virtual SIMO (VSIMO) or virtual MIMO (VMIMO) link can be established.

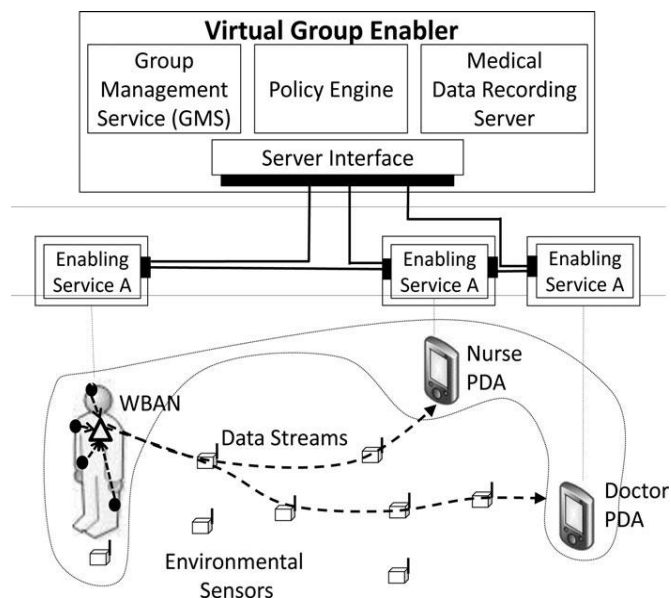


Fig 3. Overall virtual group enabling architecture. [2]

First part is the Virtual Group Enabler (VGE), is a technique which allows virtual collaboration groups to be formed between patients, nurses, and doctors (and possibly environmental sensors). As shown in fig [2]. These groups allow data from WBANs to be analyzed remotely can be modified and changed depending on the patient's condition or requirements from the medical officers. The change in virtual group configuration can be easily adjusted through high-level policies.

MOBILE Ad hoc Cognitive Networks (MACNets) is also another solution for solving frequency scarcity problem through dynamic spectrum access [4]. Here unused spectrum opportunities license is given to primary node. Mobility prediction based joint stable and channel assignment approach is used to maximizing network throughput.

The one of WBAN issues is security. Threats in WBAN are also analyzed differently according to the application. Generic threats in WBAN are Eavesdropping/Interception, Interruption / Communication jamming, Modification of data, Unauthorized access, Repudiation. So some Security Requirements feels like Data Confidentiality, Data integration, Authentication, Non-repudiation, Access control, Privacy, Communication flow security

There is no distinguishing roles of the vertices in the networks some vertices are members of cluster or hub or just outliers. The situation is illustrated in Figure5.

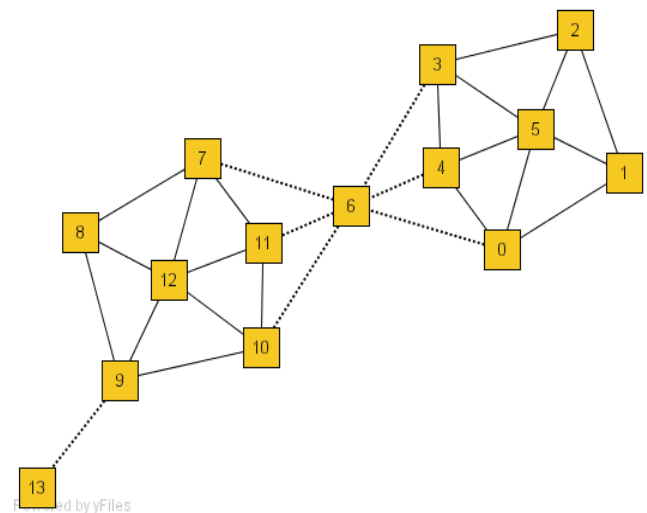


Figure 5. A Network with 2 Clusters, a Hub and an Outlier.[5]

So, for network clustering SCAN (Structural Clustering Algorithm for Networks)[11] is used by which, It detects meaningful clusters, hubs, and outliers by using the structure and the connectivity of the vertices as clustering criteria. • It is fast. Its running time on a network with n vertices and m edges is $O(m)$. To achieve this goal, use the neighborhood of the vertices as clustering criteria instead of only their direct

connections. Vertices are grouped into the clusters by how they share neighbors. Doing so makes sense when you consider the detection of communities in large social networks. Two people who share many friends should be clustered in the same community.

Two basic requirements of Inter Wireless Body Area Scheduling are: 1) fast convergence and 2) high channel utilization. In the case of a WBAN user walking on a sidewalk, network topology changes frequently when the user keeps encountering other WBAN users. Therefore, a quick IWS that rapidly detects and responds to every topology change is expected, which could adopt coloring for MANET [18]. Also, IEEE 802.15 TG6, the standard task group of WBAN, requires that the WBAN protocol should support at least the sensor density: 60 sensors in a 63 m³ space [19]. Such dense WBANs create a high probability of mutual interference. It can significantly decrease the number of coexisting WBAN users due to poor channel utilization [6]. Thus, high channel-utilization IWS is also required, which could adopt an optimal spatial-reuse coloring for dense sensor networks [20]. Random incomplete coloring is proposed to realize a fast and high spatial-reuse inter-WBAN scheduling. Unlike conventional complete coloring schemes, RIC is not limited by the tradeoff between coloring speed and spatial reuse. RIC can always provide fast convergence with time-complexity in any spatial reuse requirement. Furthermore, RIC can support an increase of up to 90 percent of spatial reuse over the conventional complete coloring using chromatic colors, which is known to be the optimal coloring of complete coloring. In the simulation, RIC is applied in a CPN-based IWS protocol with TDMA framing structure. Simulation results show that RIC does overcome inter-WBAN collisions and thus provides high system throughput for mobile wireless body area networks. This study focuses on the scenario of random-user position, which is modeled as a 2D random graph. In the future, we would like to analyze the performance of RIC in other special scenarios. For example, users in a waiting line, a movie theater, or a coffee bar. These scenarios can be modeled as a line, a grid, and a clustered graph, respectively. Also, in our future work, we will try to relax the strict assumptions made in this paper, such as perfect super frame synchronization. We will implement RIC in a mote-base WBAN to evaluate its real-world performance and make comparisons with existing WBAN solutions, IEEE 802.15.4 and Bluetooth networks.

IV. CONCLUSION

We have reviewed many researches and come to a result that if we have to design a problem free and security threats free WBAN, which causes improvement in throughput and reduces energy waste. A efficient WBAN system has monitoring information extraction, high spatial reuse, possibility of dynamically fine tuning the monitoring process to suit the data quality, provision for allowing the translation of high-level requirements of medical officers to low-level

sensor reconfiguration. Issues related to security and possible solutions must be taken in the research. This paper proposes an optimized WBAN handover strategy, RASS (Real-time Accurate & Scalable System) and VMISO (Virtual Multiple Input Single Output) system implementation in WBAN, and procedure to maximize the network throughput by jointly selecting stable routes and assigning channels avoiding inter- and intra-flow interferences based on mobility prediction. And this whole process can be implemented using NS-2.

REFERENCES

- [1] Suna, Lianying Jib, Wai-Choong Wonga Awareness for Body Sensor Networks “Wen The 2nd International Conference on Ambient Systems, Networks and Technologies (ANT) Optimized Handover Strategy with Movement Trend “, *National University of Singapore, 119613 Singapore b Graduate University of Chinese Academy of Sciences, Beijing, 100049 China*
- [2] Stepan, Ivanov, Christopher Foley, Sasitharan Balasubramaniam, and Dmitri Botvich 3238 IEEE TRANSACTIONS ON BIOMEDICAL ENGINEERING, VOL. 59, NO. 11, NOVEMBER 2012 Virtual Groups for Patient WBAN Monitoring in Medical Environments
- [3] Dian Zhang , Yunhuai Liu, Xiaonan Guo, Lionel M. Ni “RASS: A Real-Time, Accurate, and Scalable System for Tracking Transceiver-Free objects” IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 24, NO. 5, MAY 2013
- [4] Feilong Tang, Leonard Barolli, and Jie Li, A Joint Design for Distributed Stable Routing and Channel Assignment over Multi-Hop and Multi-Flow Mobile Ad Hoc Cognitive Networks
- [5] B. De Silva, A. Natarajan, and M. Motani, “Inter-User Interference in Body Sensor Networks: Preliminary Investigation and An Infrastructure-Based Solution,” Proc. Sixth Int’l Workshop Wearable and Implantable Body Sensor Networks, pp. 35-40, 2009.
- [6] S.H. Cheng and C.Y. Huang, “Power Model for Wireless BodyArea Network,” Proc. IEEE Biomedical Circuits and Systems Conf., pp. 1-4, 2008.
- [7] S.H. Cheng, M.L. Liu, and C.Y. Huang, “Radar Based Network Merging for Low Power Mobile Wireless Body Area Network,” Proc. Fourth Int’l Symp. Medical Information and Comm. Technology, 2010.
- [8] I. Howitt, “Mutual Interference between Independent Bluetooth Piconets,” IEEE Trans. Vehicular Technology, vol. 52, no. 3, pp. 708- 718, May 2003.
- [9] A. El-Hoiydi, “Interference between Bluetooth Networks – Upper Bound on the Packet Error Rate,” IEEE Comm. Letters, vol. 5, no. 6, pp. 245-247, June 2001.
- [10] “XBOW Corporation,” TelosB Mote Specifications, <http://www.xbow.com/Products/productdetails.aspx?sid=252>, 2005.
- [11] Xiaowei Xu, Yuruk, Zhidan Feng, Thomas A. J. Schweiger “SCAN: A Structural Clustering Algorithm for Networks” in press IEEE
- [12] K. Okeya, T. Iwata, R. Molva *et al.*, “Side Channel Attacks on Message Authentication Codes Security and Privacy in Ad-hoc and Sensor Networks,” Lecture Notes in Computer Science, pp. 205- 17: Springer Berlin / Heidelberg, 2005.
- [13] K. Schramm, K. Lemke, C. Paar *et al.*, “Embedded Cryptography: Side Channel Attacks Embedded Security in Cars,” pp. 187-206: Springer Berlin Heidelberg, 2006.

- [14] W. Znaidi, M. Minier, and J.-P. Babau, *An Ontology for Attacks in Wireless Sensor Networks*, National De Recherche En Informatique Et En Automatique, Montbonnot Saint Ismier, 2008.
- [15] A. Francillon, and C. Castelluccia, "Code injection attacks on harvard-architecture devices," in Proceedings of the 15th ACM conference on Computer and communications security, Alexandria, Virginia, USA, 2008.
- [16] Jari Iinatti, Matti Hämäläinen, Ryuji Kohno On the Recent and Future Topics of Wireless Communications in Healthcare JAPANESE-FINNISH JOINT SYMPOSIUM ICT and Technology in Medical and Health Research Helsinki, Finland. Department of Communications Engineering, University of Oulu
- [17] S. P. Skorobogatov, *Semi-invasive attacks – A new approach to hardware security analysis*, Technical Report, University of Cambridge, 2005.
- [18] C. Zhu and M.S. Corson, "A Five-Phase Reservation Protocol (FPRP) for Mobile Ad Hoc Networks," *Wireless Networks*, vol. 7, no. 4, pp. 371-384, Aug. 2001.
- [19] IEEE 802.15 WPAN Task Group 6 Body Area Networks, "15-08-0644-09-0006-tg6 Technical Requirements Document," 2008.
- [20] S. Gandham, M. Dawande, and R. Prakash, "Link Scheduling in Wireless Sensor Networks: Distributed Edge-Coloring Revisited," *J. Parallel and Distributed Computing*, vol. 68, no. 8, pp. 1122-1134, Aug. 2008.
- [21] Shih Heng Cheng, and Ching Yao Huang, "Coloring-Based Inter-WBAN Scheduling for Mobile Wireless Body Area Networks" *IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS*, VOL. 24, NO. 2, FEBRUARY 2013 pg 250- 260
- [22] Benolt latre, bart Braem, Ingrid Moerman, Chris Blondia , Piet Demeester A survey on Wireless Body Area Networks.
- [23] CHIEN-CHUN HUANG-FU AND YI-BING LIN, NABIL ALRAJEH, KING SAUD UNIVERSITY MOBILITY MANAGEMENT OF UNICAST SERVICES FOR WIRELESS ACCESS IN VEHICULAR ENVIRONMENTS
- [24] Yusnani Mohd Yussoff , Habibah Hashima, Roszainiza Roslib, Mohd Dani Babac" A Review of Physical Attacks and Trusted Platforms in Wireless Sensor Networks" International Symposium on Robotics and Intelligent Sensors 2012 (IRIS 2012) SCIVERSE SCIENCreE DIRECT Procedia Engineering 41 (2012) 580 – 587