Secured Solutions for Mobility in Wireless Body Area Networks

Manisha Mittal¹, Dr. D. K. Chauhan²

¹PhD Scholar, ²Director Technical, Noida International University, UP, India

Abstract—Body Sensor Network (BSN) that is linked by a wireless network interface roams from one coverage zone to another then interference between wireless-body-area-networks (WBAN) created, which can cause serious throughput degradation. Scattering of WBAN and Remote Base Station (RBS) will not be in range. 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, and hop by hop method to reach RBS (Sink), and a method to maximize the network throughput by using stable routes to avoid inter- and intra-flow interferences based on mobility prediction.

Keywords—Body Sensor Network (BSN), wireless-body-area-networks (WBAN), RBS (Remote Base Station) RASS (Real-Time, Accurate, and Scalable System), VMISO (Virtual Multiple Input Single Output), Inter-WBAN scheduling (IWS), PS (Personal Server).

I. INTRODUCTION

A Wireless Body Area Network can be treated as a “Personal Sensor Network” as it combination of biometric sensors clothes on the human body. Fig. 1. Show some of basic network type and WBAN.

Recent advances facilitate Body Area Networks with personal sensing and monitoring technology for in-body and near-body use 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] have just been opened and comprehensive studies are still required. Apart from the more macro platforms, many computing devices are implanted into patients and used to monitor various aspects of wearer’s physiology and ambient environment need of holistic security scheme for wireless Body Area Network.

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 Inter –WBAN communication architecture][13]

Examples heart-rate monitors, glucose-monitors, accelerometers, and so on. PROBLEMS IN MOBILE WBAN

II. PROBLEMS IN MOBILE WBAN

In multichannel monitor system, as shown in fig 2. Different sensor nodes which are tracking different fields interfere with 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.

Due to resource limitation, physiological data from the body of its wearer is collected using sensor nodes, not compromising the safety and security.
For this Personal Server (PS - single centralized entity) gathers data from the sensor node using hop by hop method. This PS acts as a interface between the body and outside world.

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

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.

III. SECURITY THREATS IN WBAN

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 tapping 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].

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 motes thus triggering the alarm for the

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.

IV. SOLUTION SUGGESTED

In 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 defense against physical tampering. Therefore, optimizing crypto-processors to fit the low-cost, low energy 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.

We consider powerful sensors as a channel to communicate in a hierarchical structure for inter WBAN communication as local data processing, reduces communication load in the network and provides a scalable solution. As shown in fig.3.

This is achieved by firstly doing key pre-distribution, then secure cluster formation in inter WBAN communication, then neighborhood discovery is done in inter WBAN communication. Now inter cluster and intra cluster pair wise keys generation in inter WBAN communication is done. Lastly, Re-clustering and WBAN addition is done.

Inter WBAN communication act as WSN’s communication, due to availability of powerful devices and high resources. So, we compare our proposed inter WBAN scheme with LEAP+[3], Light weight extensible authentication protocol for WSN security. 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 Figure4.

![Cluster Formation][16]

![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.

V. LIMITATIONS

In inter WBAN communication, Transmission and movement of nodes is very frequently, so the backhand data (keys) need to be updated regularly and it greatly increases the computation and communication costs of the scheme. The computation cost depends upon the network size which is equal to total number of decryptions taking place in the key agreement process. As every node has to decrypt and encrypt the message.

VI. 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. An 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, using multi hop clustering technique 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 MATLAB.

REFERENCES


[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


Xiaowei Xu, Yuruk, Zhidan Feng, Thomas A. J. Schweiger “SCAN: A Structural Clustering Algorithm for Networks” in press IEEE


Jari Inatti, 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


