Abstract. In the paper we reviewed wireless body area sensor networks and proposed an architecture for WBASN. Unique requirements for WBASN are bio-compatibility, small size, shape, long battery time, power, memory and computation restrictions, and the most important for accuracy of patient condition the information secrecy. We also proposed an energy optimized architecture for providing authentication and freshness in body area sensor networks, we have eliminated the use of acknowledgements for reducing communication cast.

Keywords- body area networks, BASN security, authentication, freshness

1. Introduction

Body area sensors are tiny sensors operating at radiofrequency and implanted within human body to monitor human body disorders. BAS are cheap equipments but having memory, processing and power constraints, these tiny sensors are implanted in human body not to work for hours or days but for months and years, the sensors form a star topology like network in human body having many sensors and a controller (Body Central Unit) which also acts as wireless switch that receives data from all the sensors in body area and transmits the collected data to some receiver outside human body [4]. BCU establishes an ad-hoc wireless network it provides access to all BAS, the information transmitted by in-body BCU is received by some nearby base station outside human body then the Information can be transmitted electronically to the doctor around the globe. BAS is very helpful for diagnosing their regularities in patients body. Using the information doctor can decide medication/precaution remotely. If there is some emergency the doctor can inform patient and his/her relatives about emergency and can suggest them nearby hospital/doctor for emergency treatment.

BAN are very useful but having two major drawbacks one is its resource constraints, the second one is the security of information transmitted by Body Control Unit.

Sensor networks are also having limited computation that is because of limited power, Sensors are also having low memory. In addition to these constraints physiological/biomedical sensors are restricted to size, shape and material used [4]. Even if we cope with limited power, computation and memory the sensor is useless if it can not function properly in human body, the size and shape must be taken in mind while designing of a biomedical sensor, the material used should be biocompatible otherwise human body will start reject the sensor. All Wireless sensor networks(biomedical and otherwise) are having power restrictions[1,4], the restrictions are because of its wireless nature and its constant power ON status, as there are no wires that means no source of power is available other than some battery, which lasts for a limited time. As biomedical sensors are implanted into human body so replacing battery means to dissect that part of the body in which the sensor was planted then change the battery of the sensor and implanted again, which is not viable.
There is another problem in this regard is the heat radiated from the sensor as much as power is used which can rise the temperature of the organ in one way and in the second way it will cause high blood pressure in the body and many others disorders like high metabolism of the body cells.

All wireless networks are inherently insecure as the only wireless medium through which they communicate is public to all so any one tune to same frequency as sensors are tuned to can breach the security. Even by purchasing and deploying the sensor of same company/type can enable the attacker to break the security.

Body area sensor networks work on ISM band which is public and known to every one so breaking the security of BAN is more attractive to adversary. If some adversary modify the message it can be very harmful as not only patient’s privacy is compromised but also adversary can generate false messages to health monitoring department/doctor at very late hours which results discomfort for both patient and doctor/health care staff etc. so an architecture for securing the contents of body area sensor network messages is required.

Overall architecture of WBASN is shown in figure 1, the biosensors implanted in human body sense the patient’s conditions and send the sensed information back to anchor node working as a cluster head. The anchor node is equipped with a transmitter, which transmit the aggregated data on ISM band which will be received by some base station outside the human body. The info received from the base station is connected to health care via an internet to, which will further prioritize the message delivery in emergency cases to department, doctor and an ambulance service, base station will decide the destination of the message.

Upon receiving the info doctor / healthcare staff will decide what to do either to inform the patient or his relatives about the medical condition of the patient or suggesting some nearby hospital/ doctor or about precautions/ cure etc.

2. Related Work

In [3] authors described the factors to be considered for biosensors health monitoring which are Reliability, Biocompatibility, Portability, Privacy and security, Prioritized traffic, RF radiation safety etc. it also proposed a logical architecture for body area sensor networks.
The unique security requirements for WBASN are authentication, confidentiality, integrity, freshness [2]. All these requirements should be met for uninterrupted medication of the patient. [1] Described an architecture for providing reliability and freshness in WSN, the author used network coding for reliability and eliminated the transmission of acknowledgements, which definitely saved bandwidth and ultimately reduced the energy consumed for communication of acknowledgements, they also used hash function for providing data specific codes to ensure freshness and dynamicity. [5] Proposed a bio-feedback system to monitor human movement. The sensors implanted in human body communicate to each other using star topology [5]. In [6] authors proposed a mechanism based on fuzzy vault for key exchange agreement. As human body movement is dynamic so instead of providing keys its far better to make them agree on some key exchange mechanism [6].

3. Proposed Architecture

The propose architecture for securing WBASN is as described in following figure 2. The body control unit and the message receiver outside human body will be pre deployed with an Initialization vector IV. The first message will be transmitted as the message and IV the passed to MAC function and the new fixed length authentication code will be appended to the message as

\[ P_1 = M_1 // C[M_1, IV] \]

Where \( P_1 \) is Message to be transmitted

For next message \( P_1 \) will be treated as initialization vector, now \( P_1 \) and \( M_2 \) will be passed to MAC function and the resultant authentication code will be concatenated to \( M_2 \) similarly with the next messages.

\[ P_2 = M_2 // C[M_2, P_1] \]

\[ P_n = M_n // C[M_n, P_{n-1}] \]

![Figure 2: BCU Block Diagram](image)

At receiving side as \( P_1 \) is received MAC function is applied to its message part that contains \( M_1 \) and IV vector then compare it with the code appended with message if both are same then place the message in message queue and replace IV by this value otherwise reject the message and keep previous IV. At arrival of second message again the MAC is applied to the message part of \( P_2 \) and \( P_1 \), and then compare the result with code appended at end of \( P_2 \) if result is same then store it in Message queue and replace the previous value of \( P \) by the new value rest of the process will be same.

\[ X_1 = C[M_1, IV] \]

\[ X_2 = C[M_2, X_1] \]

\[ . \]

\[ X_n = C[M_n, X_{n-1}] \]
The algorithm for transmission of data will be as follows

\[\text{Msg\_Transmit}(M, IV)\]

\[
\text{While (true)}
\]
\[
\text{Calculate MAC of M and IV and store it in variable } X
\]
\[
\text{Concatenate } X \text{ to } M \text{ and store it in variable } P
\]
\[
\text{Transmit the } P
\]
\[
\text{Assign } P \text{ to } IV
\]

The algorithm for receiving data will be as follows

\[\text{Receive\_Msg}(Pr, IV)\]

\[
\text{While(true)}
\]
\[
\text{Extract M from } Pr
\]
\[
\text{Concatenate IV to M and store it in variable } Y
\]
\[
\text{Calculate Mac of M and IV and store it in variable } Y
\]
\[
\text{Extract MAC value from } Pr \text{ and compare it with } Y
\]
\[
\text{If both are equal}
\]
\[
\text{M accepted}
\]
\[
\text{IV=Pr}
\]
\[
\text{Else}
\]
\[
\text{Reject the message}
\]

4. Conclusion & Future Work

We have proposed an architecture for providing data and sender authentication in wireless body area sensor networks. The architecture is power efficient as there are no acknowledgements and the communication of base station is solely with some cluster head so every in-body node do not communicate with base station we also provided freshness in our proposed architecture which ensures no man in middle attack, its implementation is kept for future work.

5. References


Figure 3: Base Station block diagram