Secure Data Transmission In E-Health Care System

B. Yesaswini Sindhura
PG Student, Department of CSE, Adhiyamaan College of Engineering, Hosur, Tamil Nadu, India

ABSTRACT

In this paper implemented in Ad hoc On-Demand Distance Vector (AODV) Routing is a routing protocol for WSN. Here it can deploy nodes in the network formation module. Sensor Nodes named as ECG, EEG, Thermal, BP etc., Then the Euclidean distance is used to find the Node position, and distance of the nodes in the network. Then the Relay node is deployed it is used to forward the sensor communication to the Doctor. The registration Phase is used to allow the Authentication process for sending Process. If it is authenticated means it will allow for uplink and downlink handoff Phase, the uplink handoff Phase Modules is used to search the available channel to destination and Downlink handoff Phase is used to verification process for broadcast Acknowledgement message. Finally it can calculate the proposed method results like Packet delivery ratio, Delay, Energy Consumption, Throughput and Network life time done by Network Simulator version2.
Keyword: Ad hoc On-Demand Distance Vector, Blake-2 Algorithm, Wireless Body Sensor Network.Wireless Sensor Network.

I. INTRODUCTION

A WBAN system can use wireless technologies as gateways to reach longer ranges. Through gateway devices, it is possible to connect the wearable devices on the human body to the internet. This way, medical professionals can access patient data online using the internet independent of the patient location. The body area network field is an interdisciplinary area which could allow inexpensive and continuous health monitoring with real-time updates of medical records through the Internet. A number of intelligent physiological sensors can be integrated into a wearable wireless body area network, which can be used for computer-assisted rehabilitation or early detection of medical conditions. This area relies on the feasibility of implanting very small biosensors inside the human body that are comfortable and that don't impair normal activities. The implanted sensors in the human body will collect various physiological changes in order to monitor the patient's health status no matter their location. The information will be transmitted wirelessly to an external processing unit. This device will instantly transmit all information in real time to the doctors throughout the world. If an emergency is detected, the physicians will immediately inform the patient through the computer system by sending appropriate messages or alarms. Currently the level of information provided and energy resources capable of powering the sensors are limiting. While the technology is still in its primitive stage it is being widely researched and once adopted, is expected to be a breakthrough invention in healthcare, leading to concepts like telemedicine and mHealth becoming real.

II. EXISTING SYSTEM

Our work differs from all these works in that we propose a new synchronization scheme to dynamically adjust synchronizing frequency and maximize the interval between two synchronization, which could largely reduce the overhead. More importantly, we do not independently consider the energy issue. Instead, we minimize the energy while satisfying QoS constraints via optimal slot allocation.

Using static TDMA, a node will obtain consecutive slots and thus its frames are transmitted one by one. If a frame is lost due to deep fading, the subsequent transmission would be, most probably, dropped again because the deep fading of WBAN lasts for such a long interval (up to 400 ms) that multiple frames could be scheduled for transmission by WBAN radio. The advancement of BSN in healthcare applications have made patient monitoring more feasible. Recently, several wireless healthcare researches and projects have been proposed, which can aim to provide continuous patient monitoring, in-ambulatory, in-clinic, and open environment monitoring (e.g. athlete health monitoring). This section describes few popular research projects about healthcare system using body sensor networks. CodeBlue is a popular healthcare research project based on BSN developed at Harvard Sensor Network Lab. In this architecture, several bio-sensors are placed on patient's body. These sensors sense the patient body and transmit it wirelessly to the end-user device (PDAs, laptops, and personal computer) for further analysis. The basic idea of the Code Blue is straightforward, a doctor or medical professional issues a query for patient health data using their personal digital assistant (PDA), which is based on a published and subscribed architecture. Besides, Code Blue's authors acknowledge the need of security in medical applications, but until now security is still pending or they intentionally left the security aspects for future work. Subsequently, a heterogeneous network architecture named Alarm-net was designed at the university of Virginia. The research is specifically designed for patient health monitoring in the assisted-living and home environment. Alarm-net consist of body sensor networks and environmental sensor networks. Besides, the authors have developed a circadian activity rhythms program to aid context-aware power management and privacy policies. Furthermore, Alarm-net facilitates network and data security for physiological, environment, behavioral parameters about the residents. However, Wood have pointed out some confidentiality infringement scenarios on Alarm-net, such as the fact it is susceptible to adversarial confidentiality attacks, which can leak resident's location; refer to for details. Thus, security and privacy is still not implemented in Mobi Care healthcare monitoring or may have been left out for future work. Nevertheless, there are many security issues such as secure localization, anonymity etc, have not even mentioned in Mobi Care system. In their description of Median its author acknowledged the need for encryption for PMs, however they did not mention which crypto-system has been used for data privacy and how they have checked the integrity of the received data. Thus, although the authors included some of the security properties to Median, their study did not reveal much information about their security implementation. As we have seen, all the above ongoing healthcare monitoring projects enable automatic patient monitoring and provide potential quality of the healthcare without disturbing patient comfort. All the projects focus on the reliability, cost effectiveness and power consumption of their prototypes, but although most of the healthcare projects mentioned above addresses the requirement for security and privacy for sensitive data, only a few embed any security. Besides, none of the above projects addressed all the security requirements and their implication, which is greatly imperative for critical applications. Hence, it can be argued that security and privacy have not been investigated in much depth, and challenges still remain for real-time wireless healthcare application. These are the facts, greatly inspired us to propose a secure IoT based healthcare system using BSN, in which we will clearly demonstrate that how easily and efficiently to achieve all the aforesaid security requirements.

Drawback of Existing System

- Large overhead in the periodic synchronization.
- Consume extra energy.
- Unacceptable throughput and frame loss.
- Channel is not efficient.

III. PROPOSED SYSTEM

Body Sensor Network (BSN) allows the integration of intelligent, miniaturized low-power sensor nodes in, on or around human body to monitor body functions and the surrounding environment. It has great potential to revolutionize the future of healthcare technology and attained a number of researchers both from the academia and industry in the past few years. Generally, BSN consists of in-body and on-body sensor networks. An in-body sensor network allows communication between invasive/implanted devices and base station. On the other hand, an on-body sensor network allows communication between non-invasive/wearable devices and a coordinator. Now, our BSN-Care is a BSN architecture composed of wearable and implantable sensors. Each sensor node is integrated with bio-sensors such as Electrocardiogram (ECG), Electromyography (EMG), Electroencephalography (EEG), Blood Pressure (BP), etc. These sensors collect the physiological parameters and forward them to a coordinator called Local Processing Unit (LPU), which can be a portable device such as PDA, smart-phone etc. The LPU works as a router between the BSN nodes and the central server called BSN-Care server, using the wireless communication mediums such as mobile networks 3G/CDMA/GPRS. Besides, when the LPU detects any abnormalities then it provides immediate alert to the person that wearing the bio-sensors. For example, in general BP less than or equal to 120 is normal, when the BP of the person reaches say 125, the LPU will provide a gentle alert to the person through the LPU devices (e.g. beep tone in a mobile phone). When the BSN-Care server receives data of a person (who wearing several bio sensors) from LPU, then it feeds the BSN data into its database and analyzes those data. Subsequently, based on the degree of abnormalities', it may interact with the family members of the person, local physician, or even emergency unit of a nearby healthcare center. Precisely, considering a person (not necessarily a patient) wearing several bio sensors on his body and the BSN-Server receives a periodical updates from these sensors through LPU. Now, our BSN-Care server maintains an action table for each category of BSN data that it receives from LPU. Table III denotes the action table based on the data received from BP sensor, where we can see that if the BP rate is less than or equal to 120 then the server does not perform any action. Now, when the BP rate becomes greater than 130, then it informs family members of the person. If the BP rate becomes greater than 145 and there is no one attending the call in family, then the server will contact the local physician. Furthermore, if the BP rate of the person cross 160 and still there is no response from the family member or the local physician then the BSN-Care server will inform an emergency unit of a healthcare center and securely provides the location of the person. Here, the response parameters "FR" (Family Response), "PR" (Physician Response), and "ER" (Emergency Response) are the Boolean variables, which can be either true (T) or false (F). If the value of any response parameter is false, then the server repeats its action. For example, when the family response parameter "FR: F", then the server repeatedly call his family members. Once, the family members of the concern person pick-up the call, then the value of the family response parameter (FR) will become true i.e. "FR: T". Now, if "FR:F" and BP > 130 then the BSN-Care server will call the local physician. In case, when the physician also does not respond to the server's call, then the value of the physician response parameter "PR" will stay in false. In this regard, the server will repeatedly call both the family members and the the physician. Unless any of the response parameter (FR, PR) value becomes true. Meanwhile, if "FR: F", "PR: F" and BP > 160, then the BSN-Care server immediately inform to the emergency unit of a healthcare center nearest to the concern person. Once the emergency unit responds, then the value of the emergency response parameter "ER" will become true i.e. "ER: T". It should be noted that, our BSN-Care system is not only designed for the patient, instead of that it can be useful for providing a decent quality of life for the aged people.

Merits of Proposed System

- ✓ Improves the overall network lifetime and Achieving maximum throughput.
- ✓ Delay is reduced.
- ✓ QOS is improved.
- ✓ Latency is reduced and efficient performance in energy.
- ✓ The packet delivery in the network is increased than the existing system.
- ✓ Security is high when compare with an existing system.

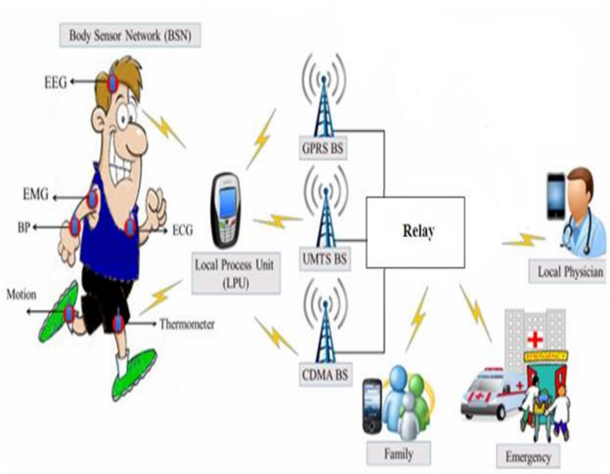

Figure 1. System Arhitecture

MODULES

Proposed system contains the following Phases

1) Network Formation
2) Key Generation
3) Up-link Hand-off Phase.
4) Down-link Hand-off Phase.

NETWORK FORMATION

- ➢ File Transfer Protocol (FTP) and randomly choose different source-destination connections.
- ➢ Here we create a Gateway nodes.
- ➢ The enhanced mobility protocol mainly simplifies the procedure of home registration and handoff.
- ➢ To achieve this goal, a new gateway format is proposed to increase the speed of data transmission, and to reduce the signaling cost and handoff delay.
- ➢ It avoid the traffic in the network.

1)

KEY GENERATION

- ➢ In the proposed system, the cryptographic mechanism is used for providing packet security.
- ➢ This mechanism performs encryption and decryption process.
- ➢ A source node wants to transmit packet to the destination node.
- ➢ Using a simple hashing algorithm we get hashed value from a string of plain text.

2)

UP-LINK HAND-OFF PHASE

- ➢ The body sensor performs an active scan that searches a list of all the available channels by periodically sending a request to all the nearby gateways.
- ➢ The nearby gateways, that receive the ACK message request from the body sensor, advertise ACK message including their MAG-IDs.
- ➢ MAG-IDs in the received messages are the same, the movement represents intra-PAN mobility, and the body sensor has moved within the same PAN area.

DOWN –LINK HAND-OFF PHASE

- ➢ This phase aims to reduce the handoff delay and signaling cost during the handoff period.
- ➢ Upon received IP configuration messages, the n-MAG stores the IP address and sends a received acknowledgement message to the coordinator of the body sensor.

➢

➢ After the coordinator receiving the acknowledgement message, the coordinator will broadcast the ACK to the rest of the body sensors.

IV. CONCLUSION

We propose a BSN, energy saving of nodes and security of transmission data are challenging tasks. In this project, secure communication is proposed to solve the energy-efficiency and security problems simultaneously. The BSN data's are transmit thought the base station to doctor. In the transmission is very secure and select optimal path in the network. In data transmission, the modified method is proposed to improve the security of image compressive encryption by utilizing two mechanisms. The simulation results show that the encryption performance is excellent.

V. FUTURE WORK

In future work, the QOS performance of the network is increased by providing efficient and secure routing for transferring the sensed information. If sensor nodes are compromised, the attackers are able to know all the confidential information stored on them and may launch a variety of malicious actions against the network through these compromised nodes. The subverted nodes may reveal the cryptographic key information and thus allow the attackers to compromise the whole network. False malicious nodes can be added to exhaust other sensor nodes, attract them to send data only to it preventing the passage of true data. Besides the sensor nodes, attackers can target the routing information which is used to maintain the communication between sensor nodes and the base station. False routing information transmitted by a host may partition the network by misguiding the traffic to a small group of nodes and thus causes difficulty in communication. The standard security goals such as confidentiality, integrity, authentication and availability will be achieved for increasing the performance of the network.

VI. REFERENCES

[1]. H. Li and J. Tan, "Heartbeat-driven medium-access control for body sensor networks," IEEE Trans. Inf. Technol. Biomed., vol. 14, no. 1, pp. 44-51, Jan. 2010.

[2]. S. Marinkovic, E. Popovici, C. Spagnol, S. Faul, and W. Marnane, "Energy-efficient low duty cycle mac protocol for wireless body area networks," IEEE Trans. Inf. Technol. Biomed., vol. 13, pp. 915-925, Nov. 2009.

[3]. B. Kang, J. Im, C. Chung, and J. Kim, "A energy-efficient system by reducing beacon listening for periodic vital sign monitoring," in Proc. IEEE 54th International Midwest Symposium on Circuits and Systems (MWSCAS), Seoul, South Korea, Aug. 2011, pp. 1-4.

[4]. Y. Tselishchev, L. Libman, and A. Boulis, "Reducing transmission losses in body area networks using variable tdma scheduling," in Proc. 2011 IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM), Jun. 2011, pp. 1-10.

[5]. B. Liu, Z. Yan, and C. W. Chen, "CA-MAC: A hybrid context aware mac protocol for wireless body area networks," in Proc. 13th IEEE International Conference on e-Health Networking Applications and Services (Healthcom), Columbia, MO, Jun. 2011, pp. 213-216.

[6]. Z. Yan and B. Liu, "A context aware mac protocol for medical wireless body area network," in Proc. 7th International Wireless Communications and Mobile Computing Conference (IWCMC 2011), Istanbul, Turkey, Jul. 2011, pp. 2133-2138.

[7]. M. Ameen, J. Liu, S. Ullah, and K. S. Kwak, "A power efficient mac protocol for implant device communication in wireless body area networks," in Proc. 2011 IEEE Consumer Communications and Networking Conference (CCNC), Las Vegas, USA, Jan. 2011, pp. 1155-1160.

[8]. A. Argyriou, A. Breva, and M. Aoun, "Optimizing data forwarding from body area networks in the presence of body shadowing with dual wireless technology nodes," IEEE Trans. Mobile Comput., early access, 2014.

[9]. N. Torabi and V. Leung, "Realization of public m-health service in license-free spectrum," IEEE Journal of Biomedical and Health Informatics, vol. 17, no. 1, pp. 19-29, Jan. 2013.

[10]. V. Chaganti, L. Hanlen, and T. Lamahewa, "Semi-markov modeling for body area networks," in Proc. 2011 IEEE International Conference on Communications (ICC), Jun. 2011, pp. 1-5.

[11]. D. B. Smith, L. W. Hanlen, J. A. Zhang, D. Miniutti, D. Rodda, and B. Gilbert, "First-and second-order statistical characterizations of the dynamic body area propagation channel of various bandwidths," Annals of Telecommunications, vol. 66, no. 3-4, pp. 187-203, Apr. 2011.