Volume 5, Issue 11, November 2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

A Hybrid Security Paradigm for Intra-WBAN and Inter-WBAN Communication Mechanism

Sanchari Saha
(Assistant Professor) Department of CSE, MVJCE,
Bangalore, India

Dr. Dinesh K Anvekar
(Dean, Academics, Director R&D) Alpha College of Engg.,
Bangalore, India

Abstract*— Wireless body area networks (WBANs) and their supporting information network provides tremendous opportunities to monitor health status without burdening a user's routine activities. These mobile point-of-care systems have become realizable due to the convergence of various modern technologies such as low-power wireless communication standards, plug-and-play device buses, off-the-shelf development kits for low-power microcontrollers, handheld computers, electronic medical records, and Internet. For wide acceptance of Wireless Body Area Networks, advancement in interoperability (at both the system and device levels) and security should be achieved. In this paper, firstly we show a model or architecture of WBAN communication, and then focus on highlighting the major differences between WSN and WBAN, and also different security needs for WBAN communication. Our paper mainly focuses on the intra-WBAN and inter-WBAN communication paradigm where the work-flow of both intra and inter WBAN approach can be realized.

***Keywords*— Inter-WBAN, Intra-WBAN, Plug-and-Play, WSN, Hybrid Key**

I. INTRODUCTION

A Wireless Body Area Network (WBAN) is a collection of intelligent, miniaturized, low-power sensor nodes that are deployed in or around human body to monitor health status and the surrounding environment. It has great scope to revolutionize the future healthcare technology and has already attracted a number of researchers in and around the world. WBANs have a wide range of applications including medical, non-medical, and entertainment applications~~.~~ It is a system which can continuously monitor the health conditions of patients to prevent ill-health and to enable early risk detection by sharing information with caretakers and physicians. Based on the operating environments this can be classified into two types: 1) wearable body area network which is operated on the surface of body and 2) implantable body area network which is operated inside the human body. Wireless Body Area Networks (WBAN) is a forthcoming technology which utilizes wireless sensor nodes to implement real-time wearable health monitoring of patients. These sensor nodes can be worn externally or implanted inside the body to monitor multiple bio-parameters (such as blood oxygen saturation, blood pressure and heart activity) of multiple patients at a central location in a hospital. It is a radio frequency based wireless networking technology. With a WBAN, patients' health status can be monitored anytime and anywhere without restricting his/her mobility. Thus, patient can live through his/her normal daily life activities. A WBAN can be used to offer assistance to the disabled. For example, a paraplegic can be equipped with sensors for determining the position of the legs or with sensors attached to the nerves [1]. Another area of application can be found in the domain of public safety where a WBAN can be used by firefighters, policemen or military personnel [2]. For example, a WBAN can monitor the level of toxics in the air and warn~~s~~ the firefighters or soldiers if a life threatening level is detected.

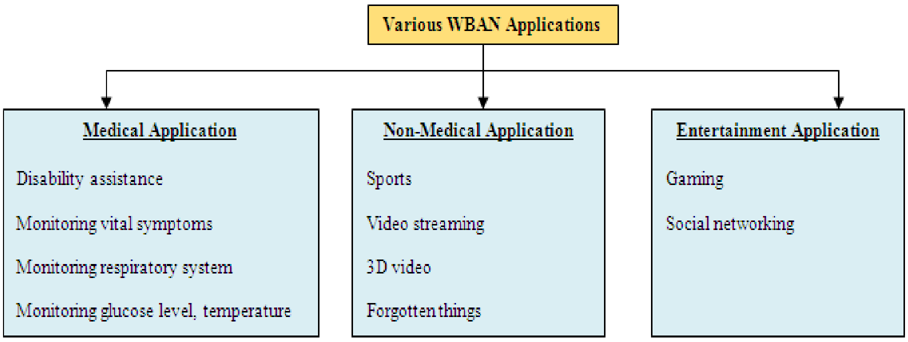

Various WBAN Applications
Medical Application
Disability assistance
Monitoring vital symptoms
Monitoring respiratory system
Monitoring glucose level, temperature
Non-Medical Application
Sports
Video streaming
3D video
Forgotten things
Entertainment Application
Gaming
Social networking

Fig 1: WBAN Applications

II. WBAN MODEL

Wireless Body Area Networks (WBAN) is a forthcoming technology which utilizes wireless sensor nodes to implement real-time wearable health monitoring of patients. Different nodes to capture diagnostics such as Electrocardiogram (ECG), and Electroencephalograph (EEG), Blood Pressure (BP), Motion etc., are deployed on the human body and to forward the collected physiological parameters to a remote medical server for further analysis. Generally, WBAN consists of in-body and on-body area networks. An in-body area network allows communication between invasive/implanted devices and a base station. An on-body area network, on the other hand, allows communication between non-invasive/wearable devices and a base station.

The sensor nodes in a WBAN can be worn externally or implanted inside the body to monitor multiple bio-parameters (such as blood oxygen saturation, blood pressure and heart activity) of multiple patients at a central location in a hospital. Data collected by the medical sensors is transmitted to the coordinator. The sensors are always activated and continuously transmit data to the coordinator. This configuration causes high energy consumption in all medical sensors and reduces their operational time. Different types of medical sensors can be used for monitoring various vital parameters.

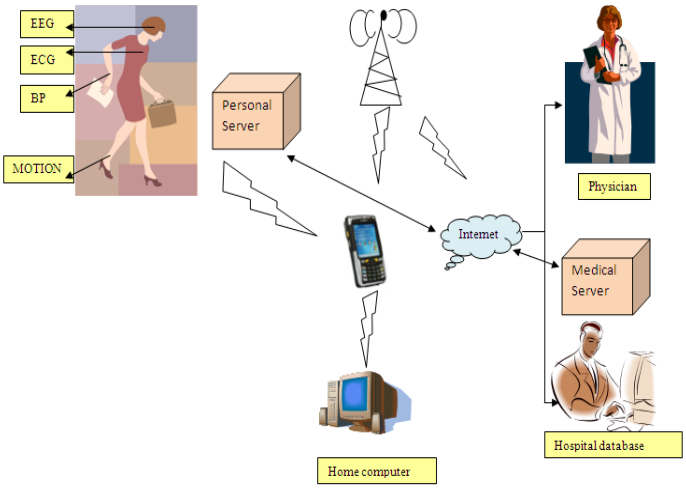


Fig 2: WBAN Model

We assume a WBAN to consist of sensor devices that are capable of measuring biometrics related to human body and also a high power and high storage device known as personal server (PS), which can be a laptop or a hand-held device. A Medical server (MS) receives all the information collected by a PS through the sensor nodes. All sensor nodes are directly connected to their relevant PSs. Sensor nodes measure biometrics and forward them to the PS. PS in turn transmits collected information to the MS through the Internet. Each WBAN is associated with one human body. Multiple WBANs are associated with the central MS. PS can communicate with other PSs as well as the MS. The MS stores and processes the information of all the WBANs that are associated with it. All sensor nodes are constrained in energy because they use rechargeable batteries.

Sensor nodes are ordinary devices with limited computation, communication, energy supply, and storage capabilities. On the other hand, a PS is a powerful node and has more computation, communication, energy supply, and storage capabilities. We assume that a PS is preloaded with node identities and relevant keys before deployment. Keeping in view the storage constraints in intra-WBAN communication, only one key is preloaded in sensor nodes before deployment. The application scenario of inter-WBAN communication includes multiple entities under surveillance and all entities communicating with a remote base station. For example, in the battlefield, the soldiers are deployed in the enemy territory and they communicate to the remote base station in their own territory. As shown in figure, the PSs of all the entities communicate to the base station and then through Internet to the remote MS.

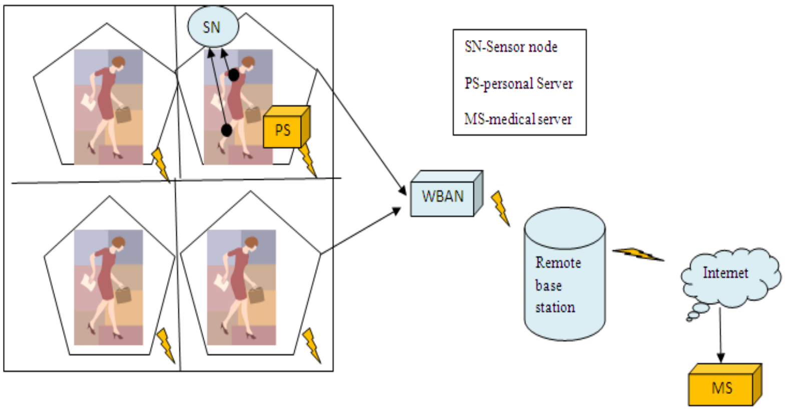


Fig 3: Information transfer between personal server & medical server

III. SECURITY THREATS & ATTACKS IN WBAN

The introduction of WBANs to e-Health monitoring system has revolutionized the field of health monitoring and resulted in better quality of life [3]. Since the patient-related data stored in the WBAN plays a critical role in medical diagnosis and treatment, it is essential to ensure the security of these data. Failure to obtain authentic and correct medical data will possibly prevent a patient from being treated effectively, or even lead to wrong treatments.

WBAN communication can be classified into intra-WBAN communication and inter-WBAN communication. Intra-WBAN communication refers to the on-body sensors communication while inter-WBAN communication refers to the communication between two different WBANs. WBAN communication faces security issues as biomedical sensors implanted on the human body for mobile healthcare monitoring communicate with external networks, and thus, increase~~s~~ the security risk. Since biomedical sensor nodes are allowed to monitor and transmit potentially sensitive medical data, security and privacy become a major concerns in WBANs. The security mechanism of the system is responsible for providing the following security services on specified biomedical data when requested to do so by the applications:

Data Encryption—the data is encrypted so that it is not disclosed whilst in transit. Data encryption service provides confidentiality against eavesdropping attacks.

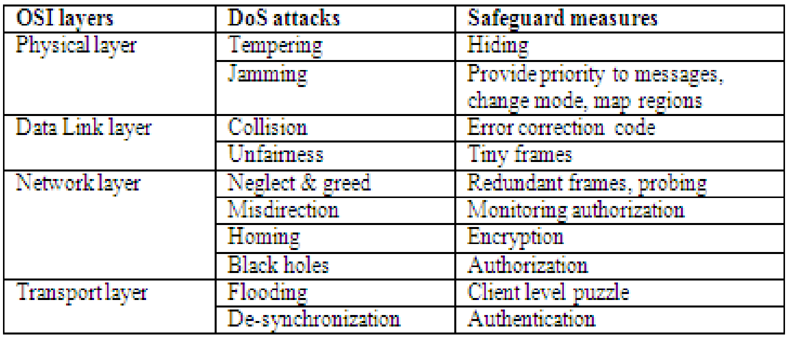
Data Integrality—Data integrality service consists of data integrity and data origin authentication. Proper data integrity mechanisms at the BN and the BNC ensure that the received data is not altered by an adversary.

Freshness Protection—Data freshness ensures that the data frames are in order and are not reused.

Authentication— an efficient method against impersonation attacks.

A WBAN is vulnerable to a considerable number of key attacks. These attacks are conducted in different ways, i.e., Denial of Service (DoS) attacks, privacy violation, and physical attacks. Due to restrictions on the power consumption of the sensor nodes, protection against these types of attacks is a challenging task. A powerful sensor can easily jam a sensor node and can prevent it from collecting a patient's data on a regular basis. Attacks on WBAN can be classified into categories given in Table 1 [3].

Table I Security threats and attacks in WBAN



OSI layers	DoS attacks	Safeguard measures
Physical layer	Tempering	Hiding
	Jamming	Provide priority to messages, change mode, map regions
Data Link layer	Collision	Error correction code
	Unfairness	Tiny frames
Network layer	Neglect & greed	Redundant frames, probing
	Misdirection	Monitoring authorization
	Homing	Encryption
	Black holes	Authorization
Transport layer	Flooding	Client level puzzle
	De-synchronization	Authentication

IV. RELATION OF WBAN TO WSN

WBANs are assumed to be a special form of Wireless Sensor Network (WSN) with its own requirements. But, existing wireless sensor networks are not able to handle the critical challenges related to human body monitoring. The major difference is the need for efficient reliable communication with each and every WBAN node, as opposed to the redundant character of WSN nodes. This corresponds to the typical medical application of WBANs, where only a single sensor per vital parameter is used. Moreover, the WBAN is very small in scale compared to typical large scale deployments of WSNs. In a WBAN, up to twenty nodes are expected to be deployed on a single person, while WSN protocols are usually designed for hundreds of nodes deployed in areas with diameters of hundreds of meters. A lot of research is being done toward energy efficient routing in ad hoc networks and WSNs. However, the proposed solutions are inadequate for WBANs. For example, in WSNs maximal throughput and minimal routing overhead are considered to be more important than minimal energy consumption. Energy efficient adhoc network protocols only attempt to find routes in the network that minimize energy consumption in terminals with small energy resources, thereby neglecting parameters such as the amount of operations (measurements, data processing, access to memory) and energy required to transmit and receive a useful bit over the wireless link.

Basically, WBAN is a communication network between the humans and computers through wearable devices. In order to realize communication between these devices, techniques from Wireless Sensor Network and ad hoc networks could be used. A typical sensor node in WBAN should ensure the accurate sensing of the signal from the body, carry out low-level processing of the sensor signal and wirelessly transmit the processed signal to a local processing unit [4]. However, because of the typical properties of a WBAN, current protocols designed for these networks are not always well suited to support a WBAN.

The main differences between Wireless Body Area Networks and Wireless Sensor Networks are brought out below:

There are no redundant devices in WBANs in spite of WSNs. All nodes in the network must be highly robust, reliable, and accurate. The lost information from one node often cannot be recovered by other nodes. Because of the special features of the environment in which the WBAN operates (human body) the data loss is more significant. The signals of the sensors, specially the implanted ones, are considerably attenuated because the propagation of the waves taking place in or on a very lossy medium. Proprietary mechanisms may be required to ensure the QoS and real time data interrogation capabilities.

However, in WSNs the data loss may be covered by other sensors. The sensors which are either implanted into a tissue or attached on the surface of body must be very small in size to support unobtrusive monitoring of the patients. However, in WSNs the sensor size is not the main concern though smaller sensors are preferred. The small size of the WBAN sensors severely affects the power resources of the devices.

The power supply recharge of the devices is often impossible. Thus, a long lifetime of the sensors is required. The sensors in a WBAN are located in or on the human body which can be in motion. This challenge for WBAN is rarely faced in WSNs.

V. INTRA WBAN WORKING PROCEEDURE

In the intra-WBAN communication, sensor nodes attached to human body communicate with the personal server. Key management in intra-WBAN communication follows a hybrid approach. For the purpose of saving memory and computational feasibility, only a single key named as secret key $K_{SN,MS}$ is used in this approach and is preloaded in the sensor nodes and is used in case of PS compromise. Other keys are generated by sensors themselves using their biometrics. The Intra-WBAN workflow follows a two-step approach. First it generates features and then performs key agreement.

Feature generation step: During feature generation step, features are first extracted and then quantized for secure intersensor communication with the help of EKG using discrete wavelet transform (DWT). DWT allows good localization both in time and spatial frequency domains and is computationally inexpensive. In the process of communication between SNs and PS, sensors sample the EKG signal at the sampling rate of 125Hz in time duration of 5 seconds. To remove unnecessary frequency components, the signal is then filtered. 625 samples are produced from a five-second sample of EKG, and then divided into 5 parts of 125 samples each. DWT is applied on each part after applying filtration. The 320-coefficients feature vector is formed by concatenating the 64 coefficients horizontally. In the quantization phase, the generated feature vector is divided into 20 blocks, each containing 16 coefficients, and then they are quantized into a binary stream.

Key Agreement step*:* Once the quantization process is completed (i.e., creation of feature vectors is done and blocks are formed properly), the key agreement process is performed. During key agreement phase, PS broadcasts data request message ‘m’ that consists of IDPS, DataReq, and nonce. All sensor nodes which have the required data first compute the shared pair wise key with the PS by applying keyed hash function on feature blocks, ID_{PS} and ID_{SN} as follows:

$K_{PS,\,SN}$=HMAC ((b11,$_N$)……. (b$_{21}$,N), ID_{PS} || ID_{SN})

m_1: PS $\longrightarrow$ *: ID_{PS} , DataReq, nonce

m_2: SN $\longrightarrow$ PS: ID_{SN} , $EK_{PS,\,SN}$ (ID_{SN} , Data),

MAC $K_{SN,MS}$ (ID_{SN} ,nonce, Data)

SN encrypts the data with key $K_{PS,SN}$ and also computes MAC on IDSN, nonce, and data using the same key $K_{PS,SN.}$ SN sends its ID, encrypted data, and MAC to the PS as found in message m. When PS receives this message, first it calculates the $K_{PS,SN}$ by applying the keyed hash function on the feature blocks, ID_{PS} and ID_{SN}. As feature blocks are the same on both sides, $K_{PS,SN}$ generated by PS will be same as that of SN. Incorporation of IDSN in key generation process ensures the establishment of unique pairwise key of PS with all communicating SNs. PS decrypts the message with $K_{PS,SN}$ and compares IDSN and received feature blocks (data) with decrypted message ID_{SN} and feature block on PS to ensure that both parties have generated the same key. The message authenticity is checked by PS through MAC verification with $K_{PS,SN}$.

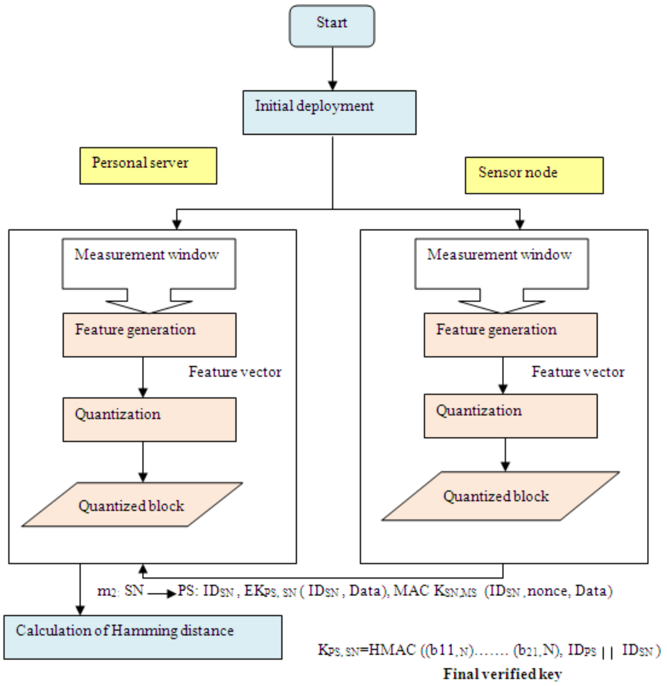


Fig 4: Intra-WBAN work flow

VI. INTER WBAN WORKING PROCEEDURE

Inter-WBAN communication includes the communication of a PS with other PSs. Each body in the WBAN contains one PS. The communication of different PSs is needed when a PS is out of range of the MS. PS communicates with other PSs and transmits data to the MS through the nearby PS. The inter-WBAN working procedure supports the use of biometric measurements. Keys are generated with the help of biometrics of any PS. The PS generates key pool using its biometrics and then transmits to the whole network. This scheme for inter-WBAN communication also makes use of key refreshment mechanism schedule. MS assigns any PS (key generator) the responsibility of refreshing the key.

Inter-WBAN working procedure consists of four types of keys: administrative key (Kadmin), network key (Knet), basic keys of all personal servers, and $K_{\mathrm{MS,\ PS}}$ key shared between MS and PS. Administrative key and basic keys are preloaded in all PSs. Network key K_{net} is a network wide key and is used to transfer data through the network in a secure manner. In this scheme, K_{net} is managed by the MS. Since K_{net} is used very frequently, it may come under cryptanalytic attacks and must be refreshed regularly. Administrative key K_{admin} is used to refresh Knet. K_{admin} is also a group key but it is not used as frequently as K_{net}. Naturally, K_{admin} is less exposed as compared to K_{net}. Also, K_{admin} needs to be refreshed through some other key at some point in time. Therefore, basic keys

$K^i{}_{\mathrm{bsc}}$ are employed in the key management framework. Every PS has its own $K^i{}_{\mathrm{bsc}}$ which it shares only with the MS.$K_{\mathrm{MS,PS}}$ is used by PS to send data to the MS and it is only shared between PS and MS.

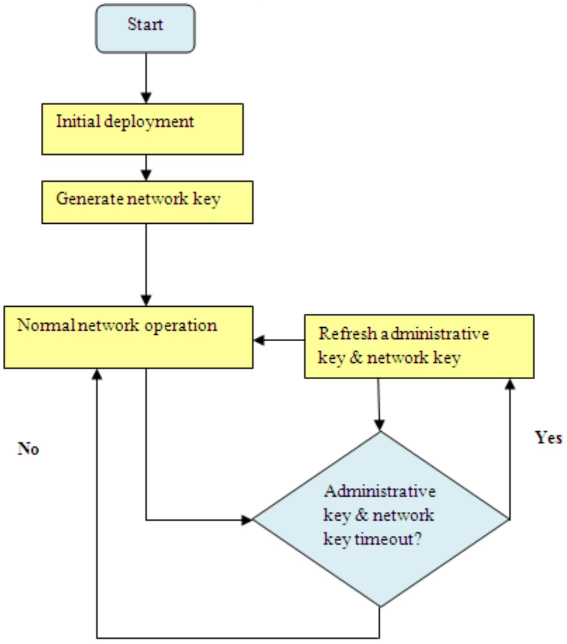

Start
Initial deployment
Generate network key
Normal network operation
Refresh administrative key & network key
No
Yes
Administrative key & network key timeout?

Fig 5: Inter-WBAN work flow

VII. CONCLUSIONS

Wireless body area networks (WBANs) have numerous applications, including patients monitoring and assisted living. In case of patients monitoring, the human personal data is communicated over an unreliable wireless media, exposing the WBANs to a variety of attacks. Providing a security solution for WBANs will increase the user confidence, which will eventually cause increase in its usability and applicability.

The technique presented in this paper is a hybrid security technique for intra-WBAN and inter-WBAN communications. The hybrid technique uses both auto generation of keys as well as the preloading which makes it efficient in terms of both storage and security and is analyzed by considering both insider and outsider attacks. WBAN faces both types of attacks. In passive eavesdropping, the attacker records encrypted keys. In replay attacks, the attacker captures legitimate messages and replays these messages in the network. Insider attacks include physical access of the nodes and attacker can launch multiple attacks such as unauthorized access to data, false injection of data, and alteration of health data. Security in intra-WBAN is ensured by eliminating key exchange between sensor nodes and the PS. A preloading-based technique is presented for the security of inter-WBAN communication. Due to its hybrid security mechanism, the technique has a good tradeoff between security and resource constraints.

ABBREVIATIONS

WBAN: Wireless body area network
WSN: Wireless sensor network
MS: Medical server
PS: Personal server
SN: Sensor node
$K^i{}_{\mathrm{SN,MS}}$: Key shared between sensor node *i* and the MS. It is preloaded in every node and refreshed whenever it is used.
$K^i{}_{\mathrm{bsc}}$: Basic key of PS*i* shared with the PS. It is preloaded in every node and is refreshed whenever it is used
K_{net}: Network wide key
K_{admin}: Administrative key
m_i: Message number in a particular communication sequence
EK $\{A|\,B\}$: Values$A$ and B are put together in a block/ chunk and then the chunk is encrypted using key K.

REFERENCES

[1] D. Raskovic, T. Martin, and E. Jovanov, "Medical monitoring applications forwearable computing," *Computer Journal*, vol. 47, no. 4, pp. 495–504, 2004.

[2] T. Martin, E. Jovanov, and D. Raskovic, "Issues in wearable computing for medical monitoring applications: a case study of a wearable ECG monitoring device," in *Proceedings of the 4th Intenational Symposium onWearable Computers*, pp. 43–49, October 2000.

[3] S. Ullah, H. Higgins, B. Braem et al., "A comprehensive survey of wireless body area networks," *Journal ofMedical Systems*, vol. 36, pp. 1065–1094, 2012.

[4] S. Saleem, S. Ullah, and H. S. Yoo, "On the security issues in wireless body area networks," *International Journal of Digital Content Technology and Its Applications*, vol. 3, no. 3, 2009.

[5] D. Djenouri, L. Khelladi, and N. Badache, "A survey on security issues in mobile ad hoc and sensor networks," *IEEE Communications Surveys & Tutorials*, vol. 7, no. 4, pp. 2–28, 2005.

[6] Y.Wang, G. Attebury, and B. Ramamurthy, "Asurvey of security issues in wireless sensor networks," *IEEE Communications Surveys & Tutorials*, vol. 8, no. 2, pp. 2–23, 2006.

[7] K.-U. R. S.Muhammad, H. Lee, S. Lee, and Y.-K. Lee, "BARI+: a biometric based distributed key management approach for wireless body area networks," *Sensors*, vol. 10, no. 4, pp. 3911– 3933, 2010.

[8] S. Cherukuri, K. Venkatasubramanian, and S. K. S. Gupta, "BioSec: a biometric based approach for securing communication in wireless networks of biosensors implanted in the human body," in *Proceedings of the International Conference on Parallel ProcessingWorkshops (WiSPr '03)*, Taiwan, 2003.

[9] A. Darwish and A. E. Hassanien, "Wearable and implantable wireless sensor network solutions for healthcare monitoring," *Sensors*, vol. 11, no. 6, pp. 5561–5595, 2011.

[10] P. Kumar and H.-J. Lee, "Security issues in healthcare applications using wireless medical sensor networks: a survey," *Sensors*, vol. 12, no. 1, pp. 55–91, 2012.

[11] G. Selimis, L. Huang, F. Mass´e et al., "A lightweight security scheme for wireless body area networks: design, energy evaluation and proposed microprocessor design," *Journal of Medical Systems*, vol. 35, no. 5, pp. 1289–1298, 2011.

ABOUT AUTHOR

Ms Sanchari Saha holds a Master of Engineering degree from CMRIT (VTU), Bangalore, and Bachelor of Engineering degree from NIT, Agartala. Currently, she is working as an Assistant Professor in MVJCE, Bangalore, and also pursuing research work towards her PhD degree. She has published a text book titled "Object Oriented Modeling & Design pattern" which has been suggested under VTU syllabus upon recommendation by VTU Vice Chancellor. She has published total 21 papers in reputed national & international journals and conferences. She has received gold medal from VTU for securing 1st rank during her Master's degree. She is a member of Indian Society for Technical Education.

Dr. Dinesh Anvekar is currently working as Dean, Academics, Director R&D at Alpha College of Engineering, Bangalore. He worked as Director Entrepreneurship and Professor of Computer Science at CMRIT. He obtained his Bachelor degree from University of Visvesvaraya college of Engineering. He received his Master and PhD degree from Indian Institute of Technology. He received best Ph. D Thesis Award of Indian Institute of Science. He has completed two Nokia sponsored projects in Indian Institute of Science during 1997-1998. He has 15 US patents issued for work done in IBM Solutions Research Center during 1998-99, Bell Labs during 1993-94, and Lotus Interworks during 2000-04, and for Nokia Research Center, Finland. He has authored one book and over 55 technical papers. He has received Invention Report Awards from Nokia Research Center, Finland, Lucent Technologies (Bell Labs) Award for paper contribution to Bell Labs Technical Journal and KAAS Young Scientist Award in Karnataka State, India. He is a Fellow of IETE and Senior Member of IEEE. He has supervised over 40 undergraduate and graduate engineering projects and research students in the Indian Institute of Science.