Enhanced Energy Efficient Bio-trusted Anonymous Authentication Routing Technique of Wireless Body Area Network

Dr.R.Sudha
Associate Professor
Department of Computer Science
PSG College of Arts & Science,Coimbatore.
E-mail:sudha279@yahoo.com;sudha_r@psgcas.ac.in

Abstract— Wireless Sensor Networks (WSN) are rapidly developing technological platform with tremendous applications in several domains. Body Sensor Network (BSN) plays a major role in the fields of social welfare, medical treatment and sports. The major problems identified in health care based sensor networks are energy consumption and lifetime. These two factors directly depend on clustering and routing and hence this research resolves in enhanced uniform clustering of the sensor nodes. Initially, routing with better load balancing is determined by tree clustering technique. The K-Nearest Neighbor (K-NN) algorithm is used to enhance the uniform clustering of sensor nodes. Secondly, the biometric iris fusion based trusted anonymous secured routing protocol is proposed to preserve two factors namely anonymity and unlinkabilty of the wireless body area network. Finally, secure routing technique based on retina with DNA coding is made with the help of onion routing to avoid computational overheads.

Keywords— Sensor Network, LEACH, Anonymous,Authentication,Energy Efficiency,clustering,biometric security.

I. INTRODUCTION

Wireless Body Sensor Network (WBSN) system plays a major role in health care services which is similar to that of normal wireless sensor network. It is a wireless network of wearable computing devices. Wireless Body Area Networks (WBANs) is an emerging technology and has the potential to improve health care delivery, diagnostic monitoring, disease-tracking and related medical procedures. It consists of a number of lightweight materials and miniature sensors which could be placed on the body as tiny part, integrated into cloth or implanted under the skin or embedded deeply into the body tissues. The main purpose is to enable doctors and medical staffs to safely monitor the status of patients. The system is also used to allow continuous monitoring of patients signs and to monitor their physiological signals.

Energy saving is one of the important features for the sensor nodes to prolong their lifetime. In the wireless body sensor network, battery is the main power supply of a sensor node which consumes most of the energy for transmitting and receiving packets. However, the battery energy must be stable in a sensor node and draining of energy could make the sensing area uncovered. In traditional research methodologies, the system is continuously monitoring the patients by bedside sensor nodes attached to the monitors. When upgrading this system to wireless sensors, then there is no relation between sensors and the bedside equipment [1].

II. LITERATURE REVIEW

Recently several authors reported on body sensors in body area network. Milenković *et al.*, discussed about issues presented in personal health care monitoring [2]. During the last few years there has been a significant increase in the number of various wearable health monitoring devices ranging from simple pulse monitors, activity monitors and portable Holter monitors to refined and expensive implantable sensors. Traditionally medical monitoring systems like Holter monitors have been used only to collect data. A number of sensors such as physiological sensors can monitor vital signs, environmental sensors (temperature, humidity, and light), and a location sensors can be integrated into

a Wearable Wireless Body/Personal Area Network. They made a Wearable Wireless Body/Personal Area Network prototype model to verify the issue in designing a wearable wireless sensor network. The WWBAN consists of miniature sensors that can allow for long-term health monitoring with instantaneous feedback to the user about the current health status and real-time updates of the patient medical records. Ragesh *et.al.*, developed a computer-supervised system can be used for early detection of medical conditions [14]. For instance, intelligent heart monitors can warn the users about medical conditions or provide information for a specialized service. It describes a WWBAN architecture as well as prototype. WWBAN designed using Telos motes and application-specific signal conditioning modules. The prototype consists of several motion sensors that can monitor the user's overall activity and ECG sensor for monitoring heart activity. WWBAN has hardware and software platforms for medical monitoring, discusses open issues, and introduces solutions for time-synchronization. It provides efficiency on-sensor signal processing, and hence called energy-efficient communication protocol. Liu *et.al.,* have presented an outline on the range of characteristic of WBAN with usage of sensors, applications used, efficiency of power, protocols used for communication, security necessities, obtainable projects in WBANs and confront met by wireless body area networks[10]. They put forth discussion on requirement of energy, security and issues in different layers of WBAN. Based on communication protocols several survey are made by Cao *et al.,* and Chen *et al.*,[3,4]. Ehyaie *et al.,* analyzed efficient energy usage in sensor nodes to provide a long life time for the network [5]. They investigated the effect of adding a relay network to the network of body sensors to reduce energy consumption of sensor nodes when transmitting data to the sink. Braem *et al.*, presented an energy efficient slotted MAC technique in the presence of a Wireless Autonomous Spanning tree Protocol (WASP) [6]. This protocol has been used for on-body packet routing. Ali *et al.,* developed a security framework using Keyed Hashing Message Authentication Code (HMAC-MD5) to protect the soldiers and patient's personal information such as pulse oximeter data, blood pressure and cardiac output [7]. Kim *et al.,* reported an efficient routing protocol based on position information in mobile wireless body area sensor networks [8]. Miao et al., presented a novel key distribution solution which allows two sensors in one body sensor network to agree on a changeable cryptographic key [9]. They have applied a fuzzy vault to secure the random cryptographic key generated from Electrocardiographic (ECG) signals. Bao *et.al.*, proposed a novel solution to tackle the problem of entity authentication in body area sensor network (BASN) for m-Health[11]. It was carried out on 12 healthy individuals, each with 2 channels of photoplethysmogram (PPG) captured simultaneously at different parts of the body. Ramli *et.al.,* presented an overview of body area network and their related issues emphasis in security problem [12]. Kumar *et.al*., presented a summary of body area network and their connected problems stress in security downside [13]. WBAN could be a small-scale network that includes short communications vary together with the communication in/on an individual's body.

III. PROPOSED WORK

The proposed methodology is more effective and provide better solution. This method uses a K-Nearest Neighbor (K-NN) uniform clustering to make a cluster-tree routing to reduce data transmission distances and improve the lifetime of total network. The authentication in routing is made by an iris and retina fused with DNA coding. The approaches are discussed in this research are explained briefly in the following sections.

A. K-Nearest Neighbor (K-NN) based Clustering of Health Care Sensor Nodes

The health monitoring systems need to allow continuous monitoring for long period. During critical conditions, the failure of sensor nodes occurs due to the following reasons such as quick discharging of battery nodes and routing. In order to make effective routing, this work aims to develop a dynamic energy efficient protocol architecture with K-Nearest Neighbor (K-NN) based uniform

clustering which finds the nodes on the basis of the uniform cluster location[15]. The K-Nearest Neighbors algorithm (K-NN) is a non-parametric method used for regression. It is a type of instance-based learning where the function is only approximated locally and all computation is delayed until the classification. The K-NN algorithm is one among the simplest algorithm of all machine learning algorithms. Enhanced Saving Energy Clustering Algorithm(ESECA) achieves reduction of energy consumption.

The data transmission distances between the sensor nodes can be reduced by employing an adaptive multi-hop approach. A cluster-tree routing architecture is created for sensor nodes by using centralized and cluster based techniques. Finally, the overall power in wireless body sensor network is reduced and its lifetime is improved for applying in large scale detecting and sensing environments. The transmission distance between two nodes is also reduced considerably.

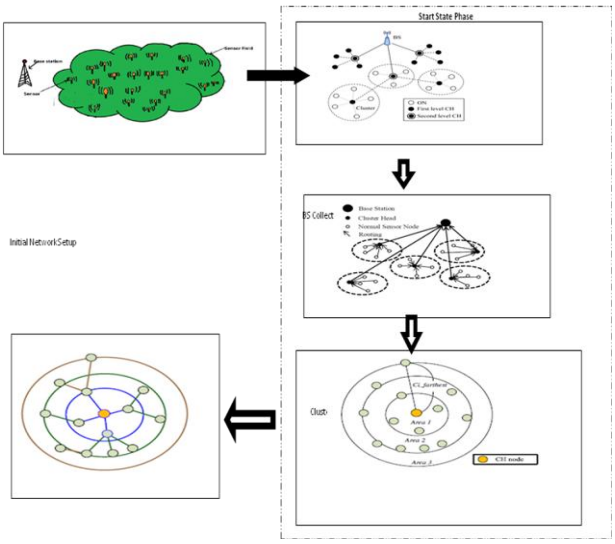

Figure 1 Enhance Saving Energy Clustering Architecture

B. Authentication and Routing using Iris Fused with DNA Coding

In recent body sensors networks, sensors are used to communicate to other control nodes of medical units through the control nodes like smart phones or medical sensors that can be interfaced with auxiliary types. This work aims to preserve two factors unidentifiably and unlinkabilty as essential characteristic of the wireless body area network. Traditional protocols are susceptible to the attacks of counterfeit routing packets, yet the node individualities are confined by pseudonyms. This research developed a new Biometric Fusion Based Trusted Anonymous Secured Routing Protocol (BFTASR) which assures prevention against such attacks[16].

Initially, the route request packets were authenticated by an iris fused with DNA coding to generate a dynamic complex group signature. Iris specification has very high recognition accuracy in comparison with many other biometric features. In which edge detection is performed both in vertical and horizontal directions. The iris images in database has iris radius 80 to 150 pixel and pupil radius from 30 to 75 pixel. The output of this method results in storing the radius and x, y parameters of inner and outer circles. If the space is less than the threshold it represents non-occlusion of eyelids.

The iris recognition process consists of five major tasks. The first task is the image acquisition of a person's eye at check time. The second task is to segment the iris out of the image containing the eye and part of the face, which localizes the iris pattern. The third task is the normalization in which the iris pattern will be extracted and scaled to a predefined size. The fourth task is the template generation here the iris information's are filtered, extracted and represented in a formatted code. The last task is the matching phase, where two iris codes will be compared and a similarity code is computed. After completing these processes, it is necessary to secure beside possible active attacks exclusive of preventing the node identities. Finally, it also prevented revealing real destination to intermediate nodes by adapting key-encrypted pairing onion. From the observed experimental results, the efficiency of the projected BFTASR protocol is improved with enhanced performance.

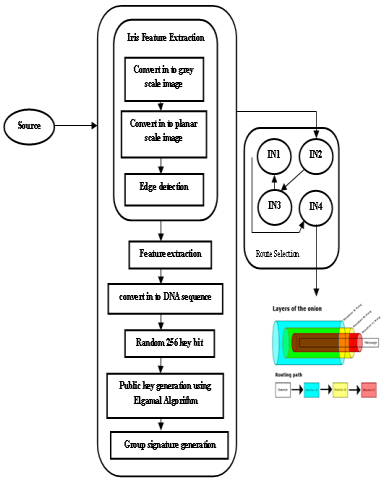

Figure 2: BFTASR Archiecture

C. Secure Routing Technique based on Retina with DNA Coding

Secure routing is necessary because the medical report gives a detailed view for diagnosing. To make it effective there is a need to develop the secure routing technique that converts the extracted features in the form of binary data of retina to a DNA based representation string. The proposed Retina Biometric Fusion Based Trusted Anonymous Secured Routing Protocol (RBFTASR) provides highest protection of them all. There are numerous advances in this field to translate binary data to a DNA string and these are identified as DNA coding technology. Here, a new DNA coding technology is proposed to convert binary data to DNA strings.

To manage secure transmission by public key generation this method adapts Elgamal algorithm. The Elgamal algorithm is selected because the security of the elgamal depends on the difficulty of computing discrete logs into a large prime modulus. Another merit is that the same plaintext gives a different cipher text each time it is encrypted. For the whole process, it uses The Onion Routing (TOR), which helps in encryption for reliable and protected data transmission.

Onion routing is a layered communication technique over a computer network. In an onion network, messages are captured in layers of encryption. The encrypted data is transmitted through a series of network nodes called onion routers. Here each node "peels" away a single layer, uncovering the data's next destination. When the final layer is decrypted, the message arrives at its destination. The sender remains anonymous because each intermediate nodes know only the location of the immediate preceding nodes and following nodes.

IV. EXPERIMENTAL RESULTS

The simulation is done using Network Simulator (NS2) to simulate the proposed methodology. This proposed work undergoes two different kinds of simulation results. In the first simulation, the performance is analyzed based on the behavior beneath the packet dropping, throughput and end to end delays in the presence of attacks with different levels. The second simulation is to evaluate the routing performances of proposed protocols after malicious attacks. Here assumed that 20% of the nodes are malicious nodes.

Table 1:Comparative analysis of protocols before malicious attack.

Sensor Nodes	Protocols	Packet Delivery Ratio (%)	Throughput (%)	End-to-End Delay (ms)
1000	RBFTASR	87.3	82	31
	BFTASR	85	79.5	33
	ESECA	82.3	68.2	35
	LEACH	70	59.4	42

Table 1 shows the performance comparison of Packet Delivery Ratio (PDR), Throughput and End-to-End delay with increase in number of sensor nodes after Malicious attacks. When compared to the traditional protocols, the packet delivery ratio of RBFTASR is increased 17% tentatively under high density network (1000 nodes). Throughput also follows similar trend as PDR but end-to-end delay gets minimized.

Table 2:Comparative analysis of protocols after malicious attack.

Sensor nodes	Protocols	Packet Delivery Ratio (%)	Throughput (%)	End-to-End Delay

				(ms)
1000	RBFTASR	96	78	23
	BFTASR	91	74.5	25
	ESECA	89	69.5	27
	LEACH	58.5	55.6	42

Table 2 shows the RBFTASR protocol using retina authentication requires less processing delays than the other protocol. If the protocol is under a heavy attack, it will launch new route discovery for the broken routes, which introduce more delays in average.

Compared to the attacked BFTASR, ESECA and LEACH the proposed RBFTASR reduces the need of re-routing, resulting in 23ms less of delay in average. Experimental results show that the extremely highest Packet Delivery Ratio of 96% and Throughput of 78% in the presence of attacks with different levels are achieved by authorized node of WBAN.

V. **CONCLUSION**

In this research, a security framework is designed to secure the body sensor communication with lower overheads by utilizing iris and retina information. To make an effective routing a K-Nearest Neighbor (KNN) based uniform clustering made a cluster-tree routing architecture. To authenticate the data, this research work proposed an iris fused with DNA coding approach that can model distinct biometric information and authenticate message signatures among body sensors with high accuracy. BFTASR routing protocol is capable of performing trusted routing behaviors according to the trust relationship among them. In BFTASR routing protocol, each node can assist mutually to achieve an objective opinion about another node's performances. Based on opinion threshold, the nodes can flexibly choose whether and how to perform cryptographic operations. Hence, the computational overheads are reduced in routing.

The results prove that onion routing has high throughput and packet delivery ratio, provided by authorized node of body sensor network and significantly decreases the average end to end delay and more secured.

References

[1]. Shnayder, V., Chen, B. R., Lorincz, K., Fulford-Jones, T. R., & Welsh, M. (2005). Sensor networks for medical care. Technical Report TR-08-05. Division of Engineering & Applied Sciences, Harvard University, Cambridge.

[2]. Milenković, A., Otto, C., &Jovanov, E. (2006). Wireless sensor networks for personal health monitoring: Issues and an implementation. Computer communications, 29(13), 2521-2533.

[3]. Cao, H., Leung, V., Chow, C., & Chan, H. (2009). Enabling technologies for wireless body area networks: A survey and outlook. IEEE Communications Magazine, 47(12), 84-93.

[4]. Chen, M., Gonzalez, S., Vasilakos, A., Cao, H., & Leung, V. C. (2011). Body area networks: A survey. Mobile networks and applications, 16(2), 171-193.

[5]. Ehyaie, A., Hashemi, M., &Khadivi, P. (2009, June). Using relay network to increase life time in wireless body area sensor networks. In World of Wireless, Mobile and Multimedia Networks & Workshops, 2009. WoWMoM 2009. IEEE International Symposium on a (pp. 1-6). IEEE.

[6]. Braem, B., Latre, B., Moerman, I., Blondia, C., &Demeester, P. (2006, July). The wireless autonomous spanning tree protocol for multihop wireless body area networks. In 2006 Third Annual International Conference on Mobile and Ubiquitous Systems: Networking & Services (pp. 1-8). IEEE.

[7]. Ali, A., Irum, S., Kausar, F., & Khan, F. A. (2013). A cluster-based key agreement scheme using keyed hashing for Body Area

Networks. Multimedia tools and applications, 66(2), 201-214.

[8]. Kim, K., Lee, I. S., Yoon, M., Kim, J., Lee, H., & Han, K. (2009, December). An efficient routing protocol based on position information in mobile wireless body area sensor networks. In Networks and Communications, 2009. NETCOM'09. First International Conference on (pp. 396-399). IEEE.

[9]. Miao, F., Jiang, L., Li, Y., & Zhang, Y. T. (2009, September). Biometrics based novel key distribution solution for body sensor networks. In 2009 Annual International Conference of the IEEE Engineering in Medicine and Biology Society (pp. 2458-2461). IEEE.

[10]. Liu, J. and Kwak, K.S. (2010, June). Hybrid security mechanisms for wireless body area networks. In Ubiquitous and Future Networks (ICUFN), 2010 Second International Conference on (pp. 98-103). IEEE..

[11]. Bao, S.D., Zhang, Y.T. and Shen, L.F. (2005). Physiological signal based entity authentication for body area sensor networks and mobile healthcare systems. In Engineering in Medicine and Biology Society, 2005. IEEE-EMBS 2005.

[12]. Ramli, S.N. and Ahmad, R. (2011, December). Surveying the wireless body area network in the realm of wireless communication. In Information Assurance and Security (IAS), 2011 7th International Conference on (pp. 58-61). IEEE.

[13]. Kumar, R., and Mukesh, R. (2013). State of the art: Security in wireless body area networks. International Journal of Computer Science & Engineering Technology (IJCSET) Vol, 4(5), 622-630.

[14]. Ragesh G K., Dr.Baskaran K. (2012). "An Overview of Applications, Standards and Challenge in Futuristic Wireless Body Area Networks" IJCSI International Journal of Computer Science Issues, 9(1), 180- 186.

[15]. Sudha R, Dr.Devapriya M. (2016), "An Energy Saving Approach in Wireless Body Sensor Networks for Health Care Monitoring" in the International Journal of Applied Engineering Research (IJAER) in Vol 11,(7), 4797 - 4802.

[16]. Sudha R, Dr.Devapriya M.(2016), "Enhanced Bio-trusted anonymous authentication routing technique of wireless body area network " in Biomedical Research 2016 in Special Issue: S276 - S282