Wireless Pers Commun (2015) 83:2975–2997
DOI 10.1007/s11277-015-2577-x

An Energy Efficient Method for Secure and Reliable Data Transmission in Wireless Body Area Networks Using RelAODV

Kanaga Suba Raja[1] · Usha Kiruthika[2]

Published online: 14 April 2015

Abstract Growing population, sedentary lifestyle and spreading epidemics in today's world have led to a need for ubiquitous healthcare systems. Wireless body area network (WBAN) is one such concept which serves as a health monitoring technology. In a WBAN sensors are attached to various parts of the human body to monitor the health or in general the bodily functions such as heart rate and blood pressure of a person. The readings obtained from the patient are transmitted to a medical professional so that the patient will be constantly and remotely monitored. This gives location flexibility for the patient instead of being in a hospital or being bound at home. But one of the downsides in adopting WBAN is the security and privacy issues. Medical records are sensitive information and hence for a patient to trust the system, data needs to be sent securely. Moreover, every detail captured by the sensors need to be reliably transmitted to the medical authorities concerned. Another issue is the limited battery power of the sensors. A sensor should not be taxed to do too many computations as that will drastically drain the battery. In this work, we propose a power efficient methodology for secure transmission of patient data to the medical authorities. To improve the reliability of the system we propose a modified adhoc on-demand distance vector (AODV) protocol called RelAODV (Reliable AODV). Simulations have shown that the proposed methodology is energy efficient and improves the overall QoS of the system.

Keywords Wireless Body Area Networks · RelAODV · Sensor networks · Routing · Remote health monitoring

✉ Kanaga Suba Raja
skanagasubaraja@gmail.com

Usha Kiruthika
usha.kiruthika@gmail.com

[1] Department of Information Technology, Easwari Engineering College, Chennai, India

[2] Department of Computer Technology, Madras Institute of Technology, Chennai, India

1 Introduction

In today's world there are many factors that have led to an unhealthy lifestyle and as a consequence the rate of occurrence of many diseases that were unknown in the past has increased. The need for disease management and health care systems is more than ever. Many chronic diseases require continual monitoring and management. Moreover as our population ages and the younger generation finding less time for caring the elderly the need for geriatric healthcare grows exponentially. In order to meet our healthcare needs many medical systems have been developed. A wireless body area network is one such system. A wireless body area network (WBAN) involves attachment of sensors on the human body for monitoring and management of bio-medical information. In addition to healthcare, WBAN has its uses in fitness and entertainment. BAN (Body Area Network) technology is still an emerging technology. It emerges as the natural by-product of existing sensor network technology and biomedical engineering. In healthcare, a WBAN could be used to monitor patients in critical conditions in hospital or even outside the hospital environment. While outside, the sensors may transmit information through cell phone network or the Internet. The sensors may send messages containing the patient's physiological information through the patient's cell phone as short message (SMS). A global trend for interconnection of data networks is to use IP (Internet Protocol). WBAN packets can be translated into IP datagrams by a gateway at the edge of a WBAN. In particular, such a gateway can be a smart phone equipped with multiple network interfaces, which enables the owner to interact with his/her WBAN and forward data anywhere in the world through, say, e-mail. Whatever network is used, the security of these messages needs to be ensured. Since the applications of WBAN are varied, the security requirements are also varied. One of the most important applications that require topmost security is medical application. In medical systems, the physiological information reaching the medical personnel securely on time may be a matter of life and death. An intruder tampering with the medical information of a patient could push the patient into very serious consequences. In this work, we have generally assumed a medical WBAN though the concepts are applicable to any WBAN or even any wireless sensor network.

This paper proposes an energy efficient method for securely and reliably transmitting messages from the sensor nodes to the medical server to be viewed by medical personnel. It discusses secure transmission of packet information and proposes a routing protocol called RelAODV (Reliable Ad hoc Distance Vector) for improving reliability. The rest of the paper is organized as follows: In the next section, we review some of the related works in the literature. In Sect. 3, we give the motivation for this work. In Sect. 4, we describe the architecture and features of the proposed system. In Sect. 5, we explain how secure transmission is done in our system. We describe the working of RelAODV protocol in Sect. 6. Section 7 describes the overall working of the system in an example scenario. The results and conclusion are in Sects. 8 and 9 respectively.

2 Related Work

The concept of Wireless Body Area Network (WBAN) is relatively new and the work done in this area is limited compared to other similar areas like Wireless Sensor Networks (WSN) and Mobile Ad hoc Networks (MANET).

2.1 WBAN Technology and Applicability to Healthcare

There are numerous survey papers on WBANs and its technologies. In [1], the authors introduce a multi-tier telemedicine system and describe how they optimized our prototype WBAN implementation for computer-assisted physical rehabilitation applications and ambulatory monitoring. The system performs real-time analysis of sensors' data. In addition, all recorded information can be transferred to medical servers via the Internet and seamlessly integrated into the user's electronic medical record and research databases. In [2], recent progress in non-invasive monitoring technologies for chronic disease management is reviewed. In particular, devices and techniques for monitoring blood pressure, blood glucose levels, cardiac activity and respiratory activity are discussed. The authors of [3] present an energy-efficient MAC protocol for communication within the Wireless Body Area Network. In [4] the authors present a multi-hopping network for a Mobility management in WBAN system that can be used in medical environments for remote monitoring of physiological parameters. The proposed system offers mobility to patients and flexibility to Doctor & medical staff to obtain patient's physiological data on continuous basis via Internet or Mobile. The collected data is transferred to remote stations with a multi-hopping technique using the medical gateway. In [5] the authors describe a one main advantage of WBAN is that it enables automatic bio-signal collection in real time which is essential in medical treatment and healthcare vigilance. Multi-hop mechanism is adopted to guarantee reliable connection. In case of less of medical resources such as in emergency, in rural or isolated areas, the system can send the corresponding bio-signal to a remote hospital in real time to help patient management by introducing satellite communication links. In [6] the authors present a prioritization mechanism for emergency case in both medical and non-medical WBANs applications. The main idea of this mechanism is to allow higher priority nodes or nodes of emergency to get the channel immediately at the expense of low priority nodes. This mechanism postpones the reservation of low priority nodes until the all high priority nodes are resolved. A collision resolution protocol, tree algorithm, has been applied to achieve this goal.

2.2 WBAN Security

In [7] a novel lightweight protocol for data integrity in wireless sensor networks has been presented. The protocol is based on a leapfrog strategy in which each cluster head verifies if its previous node has preserved the integrity of the packet using the secret key it shares with two hop up tree nodes. In [8], the authors first highlight major security requirements and Denial of Service (DoS) attacks in WBAN at Physical, Medium Access Control (MAC), Network, and Transport layers. They explain the IEEE 802.15.4 security framework and identify the security vulnerabilities and major attacks in the context of WBAN. Different types of attacks on the Contention Access Period (CAP) and Contention Free Period (CFP) parts of the super frame are analyzed and discussed. It is observed that a smart attacker can successfully corrupt an increasing number of GTS slots in the CFP period and can considerably affect the Quality of Service (QoS) in WBAN. [9] presents a security suite for WBANs, comprised of IAMKeys, an independent and adaptive key management scheme for improving the security of WBANs, and KEMESIS, a key management scheme for security in inter-sensor communication. The novelty of these schemes lies in the use of a randomly generated key for encrypting each data frame that is generated independently at both the sender and the receiver, eliminating the need for any key exchange. An approach that exploits physiological signals [electrocardiogram (ECG)] to address security issues in WBAN is presented in [10]. This approach manages the generation and distribution of symmetric cryptographic keys to constituent sensors in a WBAN (using ECG signal) and protects the privacy. We have presented a trust key management scheme for wireless body area network. Our protocol attempts to solve the problem of security and privacy in WBANs. It also aims to securely and anciently generating and distributing the session keys between the sensor nodes and the base station to secure end to end transmission. In [11] the authors discuss the security issues to WBANs and propose feasible hybrid security mechanisms to meet the security requirements of WBANs with strict resource constrains. The scheme in [12] makes use of key refreshment schedule, which depict the turn of each node for key refreshment. The personal server (PS) issues new key refreshment schedule periodically. Each node refreshes the key in the slot allotted to it. This scheme uses three types of keys to manage a WBAN: communication key, administrative key and basic key. The authors present BARI, which is a key management scheme designed specifically for WBAN applications. BARI provides required level of security in WBAN while exploiting the application characteristics of WBAN, which other schemes are unable to do. In [13] An efficient secure data transmission scheme in WBAN is proposed with data integrity. The scheme is user-centric and the secure key is shared among all sensors in a WBAN to minimize any additional memory and processing power requirements. The secure communication between medical sensors and PDA, as well as ensuring QoS for the real-time traffic has been investigated. The proposed secure communication scheme can minimize the key storage space and need less computation. Patient privacy is ensured by using pseudo identity. A priority based traffic scheduling scheme for real-time application in WBAN is proposed and analyzed.

2.3 WBAN Reliability

Lee et al. [14] proposed and implemented an efficient and reliable backup scheme for bridge monitoring systems. It is mainly using a wireless sensor network (WSN) to gather the related environmental parameters and to transmit the numerical data to the gateway through multiple-hopping relay. And then it further stores data in the back-end database for the professional monitoring staffs to analyze and study. In [15] a distributed Prediction based Secure and Reliable routing framework (PSR) for emerging Wireless Body Area Networks (WBANs) has been proposed. It can be integrated with a specific routing protocol to improve the latter's reliability and prevent data injection attacks during data communication. In [16], MBStar, a new real-time, high-frequency, reliable, secure protocol for WBAN has been proposed. MBStar utilizes channel hopping and channel blacklist to minimize noise interference. It also supports acknowledged transmission and retransmission to provide link reliability. MBStar employs both public/private key mechanisms for provisioning devices before join and uses AES (Advanced Encryption Standard) for encrypting health data after join. A data-centric multi-objective QoS-aware protocol (DMQoS) [17] was proposed to address the reliability and delay issues in Body Sensor networks. Each data packet sent through the network is classified as ordinary data packet, reliability-driven data packet, delay-driven data packet and critical data packet depending on the priority that needs to be given for a specific type of data. DMQoS provides a dynamic and modular system for rendering quality data delivery services. Another similar scheme is the Energy-aware peering routing (EPR) protocol [18] which aims at reliable and energy-efficient routing. The EPR protocol consists of three parts namely, the modified Hello protocol, neighbor construction algorithm and routing table construction algorithm. It is shown that EPR protocol increases reliability and traffic load while the nodes use only less transmission power. But the scheme is suitable only for indoor hospital environment.

3 Motivation

3.1 Need for Security and Reliability

The communication of health related information between sensors in a WBAN and over the Internet to servers is strictly private and confidential and should be encrypted to protect the patient's privacy. Furthermore, medical staff who collect data need to be confident that the data is not tampered with and indeed originates from that patient. It cannot be expected that an average person or the medical staff plays the role of a network administrator who can set up and manage authentication and authorization processes. Moreover the network should be accessible when the user is not capable of giving the password (e.g. accessibility in trauma situations by the paramedics). Security and privacy protection mechanisms use a significant part of the available energy and should therefore be energy efficient and lightweight.

A proper quality of service (QoS) handling is an important part in the framework of risk management of medical applications. The critical factor is the reliability of the transmission, meaning that it is crucial that messages with monitoring information are received correctly by the health care professionals. The reliability can be considered either end to end or on a per link base. Examples of reliability include the guaranteed delivery of data (i.e. packet delivery ratio), in-order delivery. Besides that, messages should be delivered in reasonable time. The reliability of the network directly affects the quality of patient monitoring and in a worst case scenario it can be fatal when a life threatening event has gone undetected. Other QoS parameters such as minimum guaranteed bandwidth, low delay and support of real time communication have a strong impact on MAC and PHY layers. The desired quality of service will affect the energy consumption.

3.2 Need for Multi-hop Communication

The WBAN consists of several sensor nodes deployed in or near human body. Since the nodes in the body are within a short range, it may look like routing is not required between the sensor nodes. But there are several reasons for which multi-hop transmission is unavoidable. First, the topology of the WBAN goes through slight changes due to posture of the person. Though node mobility is limited in WBANs, postural mobility is significant. A node which is within reach at one point in time (e.g. When a person is standing) may become unreachable later (e.g. when the person sits). At that time packets may have to be routed through other nodes. Secondly, propagation loss through the human body is very high. Even nodes located in short ranges may need routing for reliable communication. Finally, the power of transmission for sensor nodes is very limited. It is better to use less power in more number of nodes and route the packets through multiple nodes rather than using high power to pass them in single hop. Studies [19] have shown that in an open environment with low transmission power there is a significant improvement in packet delivery ratio (PDR) when there is multi-hop communication between the nodes.

4 Secure and Reliable Data Transmission

We now explain the proposed system and call it the SRDT (Secure and Reliable Data Transmission) system. We try to address the security requirements of Data Confidentiality, Data Authentication, Data Integrity and Data freshness protection. For reliability we focus on packet-driven reliability and event-driven reliability. In the following sections we introduce the basic architecture of a WBAN system and detail the features of SRDT system.

4.1 WBAN Architecture

The WBAN architecture [20] illustrated in Fig. 1 is a 3-tier system with the first tier forming the sensor nodes located over a person's body. The second tier is the personal server containing the coordinator located nearer to the nodes. The third tier is medical server which is responsible for monitoring the health of the wearer. The sensor nodes connect to the personal server and then through the Internet to a medical server tier that resides at the top of this hierarchy. The system is not merely a distributed data logger, which in itself would provide great advantage over current systems, but provides distributed data processing and analysis functions.

Messages are generated in the sensor nodes. For example, ECG is done by a sensor on a person and it has to be sent to the doctor reliably and securely. The data has to be passed on through the nodes present in the body to the personal server and then to the medical server.

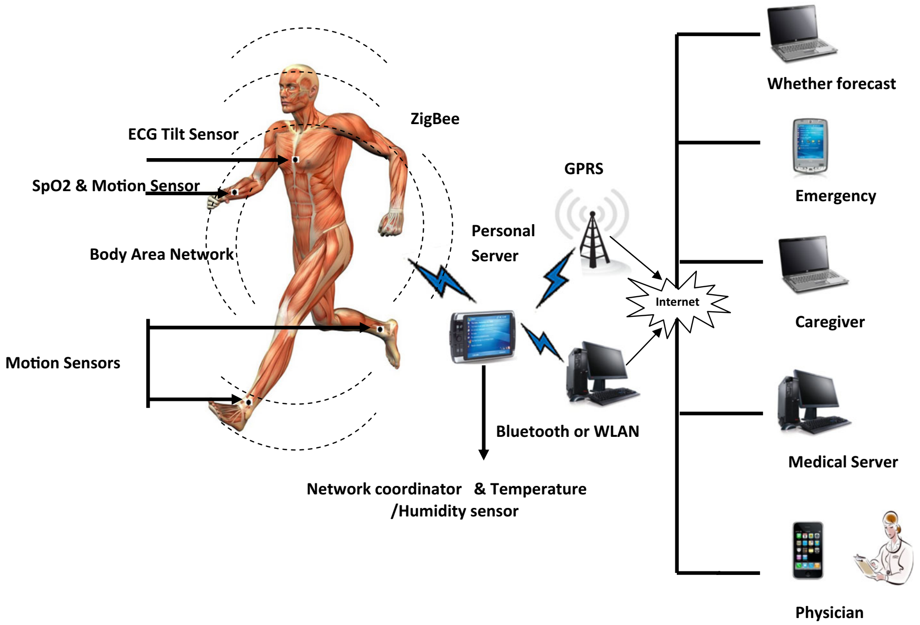

Fig. 1 Architecture of WBAN

4.2 Direct Mode and Relay Mode

All the nodes in the WBAN have node id. Every node has a controller and a small memory to keep the data. Every node has trans-receiver so that they can get the data and transmit it. The nodes may be sensor nodes or relay nodes. Sensor nodes can sense events in addition to transmission and reception. These nodes form tier 1. All the nodes are controlled by a coordinator which lies in tier 2 within the personal server. The personal server in turn communicates data to the destination in tier 3 which is the medical server controlled by, for example, may be a doctor. In this network, the nodes are modeled in such a way that it possesses two modes: direct mode (DM) and relay mode (RM). The nodes are illustrated in Fig. 2.

The primary reason for classifying a node into direct mode and relay mode is to save power. In direct mode the transmission power will be set to the maximum level. Only minimum number of hops or just one hop is required when the sensor nodes are set in this mode. By default, all nodes are in DM. In relay mode the power level will be low and consequently nodes will be able to communicate to only nearby nodes in this mode. Hence more number of hops will be required to transmit a message to the coordinator. The mode of a sensor node can be set manually. Also, the nodes change mode by calculating the signal-to-noise ratio (SNR) and the residual battery power. The mathematical estimation of SNR and residual battery power is given in the following sub-sections.

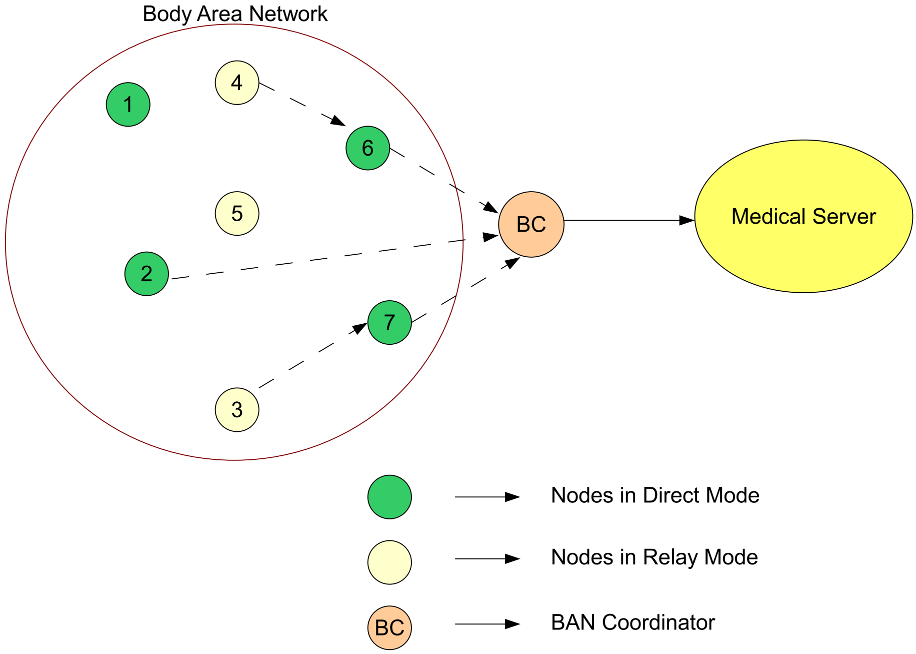

Fig. 2 Nodes in direct and relay modes

4.2.1 Estimation of Signal-to-Noise Ratio

The signal-to-noise ratio (SNR) is the ratio of the actual message transmitted to the background noise. Each node is able to get SNR from other neighboring nodes. The nodes can transmit to only those nodes whose SNR is less than a threshold region. The threshold should be determined according to the requirement of the network at the time of deployment.

The SNR, in dB, of the link to the BAN coordinator which is at d distance apart is estimated by the sensor nodes. The estimated value of SNR (t) at time t is described using the following equation

$$\mathrm{SNR}(t) = \mathrm{SNR}_{\min} + (\delta)(t, d) - \mathrm{Ps}) \tag{1}$$

where Ps—power sensitivity in dBm, δ(t, d)—currently received power in dBm.

Both Ps and δ(t, d) values depends on sensor and $\mathrm{SNR}_{\mathrm{min}}$ is based on the pre-defined bit error rate (BER).

4.2.2 Estimation of Residual Battery Power

The residual battery power ($\mathrm{BP}_{\mathrm{res}}$(t)) of the sensor node can be estimated from the difference of the initial battery power (BP_{i}) and consumed battery power (BP_{c}) at time t. ($\mathrm{BP}_{\mathrm{res}}$(t)) is estimated using the following equations.

$$\mathrm{BP}_{\mathrm{res}}(\mathrm{t}) = \mathrm{BP}_{\mathrm{i}} - \mathrm{BP}_{\mathrm{c}}(\mathrm{t}) \tag{2}$$

$$\mathrm{BP}_{\mathrm{res}}(t) = \mathrm{BP}_{\mathrm{i}} - \sum_{0}^{t} \left(BP_{tx}(t) + BP_{rx} + BP_{idle}(t)\right) \tag{3}$$

where $\mathrm{BP}_{\mathrm{tx}}$—battery power during the process of data transmission, $\mathrm{BP}_{\mathrm{rx}}$—battery power during data reception, $\mathrm{BP}_{\mathrm{idle}}$(t)—battery power during nodes idle period. BP_{c}(t) is based on power management scenario which constitutes power during transmission, reception and idle period.

Let $\mathrm{SNR}_{\mathrm{th}}$(t) be the pre-defined threshold value of the signal to noise ratio. Let $\mathrm{BP}_{\mathrm{th}}$ (t) be the pre-defined threshold value of the residual battery power.

```
if (SNR (t) > $\mathrm{SNR}_{\mathrm{th}}$ (t)) && ($\mathrm{BP}_{\mathrm{res}}$ (t) > $\mathrm{BP}_{\mathrm{th}}$ (t))
then
      The node remains in direct mode (DM)
else
      The node switches to relay mode (RM)
end if
```

4.3 Classification of Messages

In a WBAN used for medical applications the patient physically wears sensors and is constantly monitored for particular signals. For example, a patient may wear sensors for ECG alone or for blood pressure and pulse. Most applications require continuous transmission of signals and the records are collected over a long period of time so that any abnormal variations are monitored remotely by medical professionals. This leads to two different types of messages—one for the regular messages which are transmitted constantly and are recorded at the medical server. The other type of message is when an abnormality is sensed by the sensor.

4.3.1 Non-critical Messages

Messages which carry regularly monitored data like body temperature, ECG, Blood Pressure, pulse rate, etc. are sent as non-critical messages. The corresponding data are classified as non-critical data. Non-critical data are sent very frequently over the network. These data are analyzed by a human through tier 3. Hence, if there is any modification of this data it will be noticed by a human. If an adversary tries to scramble the encrypted data, the data reaching tier 3 may be impossible values. For example, if body temperature is sent as 400 degree Celsius, a doctor viewing that data will only doubt the system rather than doubting the health of the patient. Moreover even if one packet gets lost, the next packet will immediately inform the sensed data which may not have undergone many changes compared to the lost packet. For these reasons, these types of data and messages are classified as non-critical.

4.3.2 Critical Messages

Messages that carry data related to a sudden alarming change like a raised or very low blood pressure or sudden heart rate changes are classified as critical messages. On-sensor processing significantly improves system robustness and power efficiency. Wireless transfer typically requires at least an order of magnitude larger power than processing. In addition, on-sensor processing significantly reduces the amount of data that should be transmitted to the upper level of hierarchy. As an example, transferring raw ECG signal requires:

$$\begin{aligned}\mathrm{BW_{raw}} &= [1\ldots3](\text{Channels}) \times [250\ldots500](\text{Hz sampling rate}) \times [12\ldots16]\ (\text{bits/sample}) \\ &= [3000\ldots24000]\ \text{bps}\end{aligned}$$

If the signal is processed on sensor to detect inter beat intervals (RR intervals from R peak events), required bandwidth is reduced to:

$$\begin{aligned}\mathrm{BW_{event}} &= [1](\text{channel}) \times [0.6\ldots4]\ (\text{events/heart-beats/ sec}) \times [16]\ (\text{bits/sample}) \\ &= [9.6\ldots64]\ \text{bps}\end{aligned}$$

Therefore, on-sensor processing is essential for power efficient system operation. However, in the case of critical events (e.g. cardiac arrhythmia), the system should provide raw samples on request of the medical server or the operator.

In contradiction to non-critical messages, critical messages are not as frequent. Hence even if one packet is lost it is lost forever. The message that was about to be conveyed will never be conveyed. Though at tier 3 the doctor will eventually realize the change by viewing the abnormality, it may be already too late. Critical messages will be delivered directly to, say, the mobile phone of the doctor or any other place that will serve as an alarm. On the other hand non-critical messages will only be recorded in a database, which, medical personnel may take his own time to view. It is very essential that critical messages are delivered securely and reliably to improve the overall reliability of the network. The reliable transmission of critical messages also helps in lesser frequency of transmission of non-critical messages thus reducing network traffic and helping in improving the QoS of the network.

4.4 Nonce for Security and Authentication

One of the aspects of security is data freshness protection. A replay attack by an adversary in a network may easily mislead medical personnel into believing that the patient is fine when in reality the patient may be in a serious problem. In order to avoid replay attacks we introduce the concept of using random numbers. A random number is generated by each sensor and is appended to the message before it is sent. These random numbers are called as nonces. All the random numbers sent by the sensors are stored at the destination and every received number is checked against the table. If there are any repetitions, the message is discarded. The use of nonce serves as an effective protection against replay attacks. Another use of including random numbers is they help in authentication between the personal server and the medical server. The primary requirements for the management of these random numbers are:

- Since these numbers are generated by sensors it is mandatory that the generation process does not take too much energy.
- For a sensor an already generated number should not be generated again as this will lead to a repeated number being recognized as a replay attack.
- A large database is required for storing all the previous numbers at the medical server.

4.4.1 RSA-Encrypted Nonces

RSA-encrypted nonces provide a way for very secure authentication. We propose the implementation of this method in the authentication between the personal server and the medical server i.e., between tier 2 and tier 3. It is inefficient to use in tier 1 as these are sensor nodes which cannot be overloaded with computational tasks. This is because RSA-encrypted nonces require the use of a cryptographic hash function. It is assumed that the personal server and the medical server are capable of more computations than sensor nodes. A cryptographic hash function is a function which generates a hash value for a given input; but, given the hash value the original input cannot be recovered back. Hence these are one-way functions which produce a message digest for a given message. In our system we use SHA-1 to generate the digest. RSA-encrypted nonces work this way: Let P be the personal server and M be the medical server. P generates a nonce that it encrypts along with its own identity with M's public key using RSA algorithm. P transmits the cipher text to M. While P does this, M encrypts a generated nonce along with its identity using P's public key. Once P receives the encrypted packet from M, it decrypts the packet using its own private key. After the packet has been decrypted, P removes both the nonce and M's identity from the packet. P then hashes M's nonce and M's identity and sends the hash back to M. M performs all these operations simultaneously on the other side. After both M and P receive their respective hash, each device hashes its own nonce and identity. Each side then compares the calculated hash with the received hash from the other side. When both these hashes match authentication has occurred. After this initial authentication, other communication can take place between these two parties. This method is applied between every personal server and the medical server.

4.4.2 Nonce Database Management

The sensor nodes generate random numbers for every message sent to the destination (personal server and medical server). These numbers have to be stored in a database at the server side for comparison and verification that a replay attack has not taken place. For each message, the sender identity, the nonce and received timestamp are stored in a separate table while the actual data is stored in a different table. Selecting the range of random numbers is important. If the range is too large, the actual data attached in every packet will increase and consequently more number of packets will be required to convey a message. Also the database will become larger. On the other hand, if the range is too small it would be difficult to generate the numbers without repetitions. Another issue is when to delete the database. Obviously nonces cannot be stored forever. In our implementation we clear the contents of the database whenever the keys are updated. Periodically it is essential that new public and private keys are generated for the nodes in the system. At this time the values in the database are deleted and the new values are recorded.

The stored values are sorted in the order of the sender identities first. Then among the messages from a single sender, the records are sorted according to nonce values. This makes searching much easier than unsorted database or database sorted in the timestamp order. We employ binary search to search for a particular sender and a nonce. The sender identity from a received packet would be taken first. All the records having that sender identity would be returned. Among those records the nonce to be searched for is looked up. If the nonce does not show up it means there is no replay. Another major advantage in using binary search is that it is very fast to verify whether a given value is available or not.

5 Security of Transmitted Messages

5.1 Message Transmission at the Source

For any message transmitted in the network, encryption and authentication are required. RSA algorithm [20] has been used for encryption and decryption. Both authentication and confidentiality is achieved using this.

$$\mathrm{Z} = \mathrm{encrypt}(\mathrm{encrypt}(\mathrm{Pr_a}, \mathrm{X}), \mathrm{Pu_b})$$
$$\mathrm{X} = \mathrm{decrypt}(\mathrm{decrypt}(\mathrm{Pr_b}, \mathrm{Z}), \mathrm{Pu_a})$$

where Z is encrypted text and X is decrypted text. a is the sender and b is the receiver.

Initially all sensor nodes and the coordinator have a public key (Pu) and a private key (Pr). When data is to be sent from a sensor, a random number is appended to the data. This ensures freshness protection of the message thus preventing any replay attack. Then it is encrypted with the public key of the coordinator (destination). A criticality flag is set if the message is critical. The sender digitally signs the message for authentication. The packet design for initially sent packet is shown in Fig. 3.

In the Fig. 3, shaded portion denotes encrypted data. This packet may be sent directly to the coordinator if the coordinator is in the range. Otherwise the flag is set. Here flag on indicates that the data can be modified by the end node (relay mode) and can be re-transmitted. Sender sends the data-packet to the end points with the above described method.

Sender id/ signature	Destination	(Data + random number) encrypted with $\mathrm{Pu_c}$	Other info	reserved	Criticality flag	flag

Fig. 3 Packet at the sender

First the relay node looks into the destination address. If the destination is in the routing table of the relay node then the intermediate node sets the flag to 0. The relay node abstracts the data from the data packet makes a new data packet. This depends on the criticality flag. If the flag is set, i.e., if the message is critical, the message is encrypted with the private key of the relay node. Moreover, the node temporarily switches over to direct mode if it is not so already. It adds its node id at the reserved place. Then it transmits to the next hop. If it is unable to find the destination as a next hop then it adds its id in the reserved field and keeps the flag on. Then it has to transmit the data packet to its next hop node known from the routing table.

The second node also abstracts the data and checks for availability of the destination in the routing table. If it is present, makes the flag off and transmits the data. If the second node is also unable to locate the destination as next hop in its routing table, then in the regeneration of data packet it encrypts data with its private key, keeps the flag on and adds its id with the existing ids and transmits it to nearby nodes except the sender and all those nodes whose ids are present in the reserved field.

Figure 4 shows encrypted data again encrypted with private key of the intermediate node x. In case the criticality flag is not set by the sender, the encryption of data is not done at the intermediate nodes. Instead the signature of the intermediate node is appended to the node id in the reserved place (Fig. 5). This saves battery power wasted in encryption and decryption. Also for some applications, instead of sending data regularly only critical data could be sent reducing the network traffic and improving the QoS.

5.2 Message Interpretation at the Destination

When a node receives a packet, it checks the destination field. If the packet is addressed to itself, it decrypts the data. If the criticality flag is set, it checks the last node and applies the public key of that node to decrypt the data. This process is repeated for each node on the path until the destination node reaches the data encrypted with its own public key.

For both critical and non-critical packets, the destination node decrypts the data by applying its own private key. Now the data is appended with a random number. This random number is checked with a database of stored random numbers from previous messages sent by that particular sender. If the received random number is not in the database, no replay attack has taken place and hence the data is genuine. The received random number is also stored in the database in sorted order. We have applied binary search for searching for a random number in the database.

The coordinator directs the received data to the proper destination, a doctor, for example. It then sends acknowledgement to the sender. The acknowledgement is first appended with the received random number for ensuring protection against replay attacks. The acknowledgement is then encrypted with the private key of the coordinator. This information is sent towards the original sender in the reverse order of the path. At each intermediate node, the node finds its next hop from the packet and sends the acknowledgement to it.

Sender id/ signature	Destination	[(Data + random number) encrypted with Pu_c] encrypted with Pr_x	Other info	<node id> <node id> ….	Criticality flag = 1	flag

Fig. 4 Packet at intermediate nodes for critical messages

Sender id/ signature	Destination	(Data + random number) encrypted with Pu_c	Other info	<node id, signature> <node id, signature> …	Criticality flag = 0	flag

Fig. 5 Packet at intermediate nodes for non-critical messages

5.3 Overall Algorithm

At the Sensor on sensing an event

```
if event.isCritical()
        set criticality flag =1
data = data + random number
encrypt (data, $Pu_c$)
search for next hop in routing table
if next hop != destination
        set flag = 1
        nextHop = lookupRouteTable()
add signature
send packet to nextHop
```

At intermediate relay nodes

```
if criticality flag == 1
        encrypt(data, $Pr_{my}$)
add MyNodeID to reserved
search for destination
if nextHop == destination
        set flag = 0
else
        set flag = 1
add signature
send packet to nextHop
```

At the destination

```
repeat until reserved == NULL
        LastNodeID = getLastNode()
        if criticality flag == 1
                info = decrypt($Pu_{lastNode}$)
        data = decrypt($Pr_c$)
        rand = extract(data)
        search rand in DB
        if not found
                send data to authority
                ack = encrypt(ack,$Pr_c$)
                LastNodeID = getLastNode()
                Send ack to LastNodeID
```

6 Reliable Routing Using RelAODV

Many routing protocols were considered for implementation in this system. DSDV (Destination sequenced Distance vector routing) [21] is effective for creating adhoc networks for small populations of mobile nodes. But it is a fairly brute force approach because it depends for its correct operation on the periodic advertisement and global dissemination of connectivity information. AODV (Adhoc On-Demand Distance Vector) [22] improves upon the performance characteristics of DSDV and other similar protocols in the creation and maintenance of adhoc networks. All the sensor nodes in our system are either in direct mode or relay mode based on the SNR and battery residual power. This information is used for deciding the next hop node. Generally, a node is more reliable if it is in the direct mode. This is because its SNR and battery power are above the set threshold limit. Since in WBANs the mobility of nodes is very limited, a neighboring node in direct mode would mean that it is more reliable compared to another node in relay mode. We propose a routing protocol called RelAODV (Reliable AODV) in which preference is given to the nodes in direct mode rather than nodes in relay mode.

6.1 Route Set-Up Phase

The source sensor node broadcasts RREQ packets to find the destination if does not already have the route to destination. All the neighboring nodes receive the RREQ packet. Multiple RREQ packets may be received by a node. The packet with the lowest hop count is selected. The source address is saved in the routing table until REV_ROUTE_TIMEOUT.

The node then checks the destination address field on the packet. If the destination address does not match with its own address, it checks its routing table for availability of a route to the destination. If a route to the destination is not known, the node checks for its mode. If it is in relay mode, a relay penalty is added to the hop count before broadcasting the RREQ again. If a route is available and the sequence number of the route is greater than or equal to the sequence number in the RREQ, the node checks for its mode. If it is in relay mode, a relay penalty is added to the hop count before sending the RREP. If the node itself is the destination, it simply sends a RREP. As the RREP is sent towards the source, all the intermediate nodes update their routing table for the route for the destination.

6.2 Route Maintenance Phase

Routes in the routing table are active as long as nodes successfully transmit data through those routes. When a node changes from direct mode to relay mode, or from relay to direct mode or when a link breaks while trying to send a message to the destination the node generates an RERR message and sends it towards the source to inform the invalidity of that route. A new route needs to be established if RERR is received for a particular route. At the intermediate nodes, the decision for selecting the next hop node does not depend solely on whether the next hop is in direct mode or a relay mode. This is because if there are much lesser hops through relay nodes compared to hops through direct nodes, selecting the path through direct nodes would cause more network traffic and would seriously affect the QoS of the system. First priority for selecting next hop is given to hop count as in AODV. Knowing whether the node is in direct mode or relay mode will improve the reliability of the network. The relay penalty is for selecting a next hop in relay mode. This is a preset value in the network. If this is set to be too high relay nodes would never be selected against direct nodes. Else if its value is too low there would not be much difference between direct nodes and relay nodes during selection.

The relay penalty is decided based on how much preference should be given relay nodes as against direct nodes. Due to lesser mobility in WBANs, the generation of RERR message due to link failure is a rare occurrence.

Most of the time, a link failure occurs only due to powering off of a node due to battery depletion. Hence the generation of a RERR message when a node switches from direct to relay mode or vice versa does not result in frequent flooding of RERR messages compared to usual mobile sensor network. An example network and the working of RelAODV is illustrated in Fig. 6. Node x is the source and node y is the destination. When RREQ from x reaches node b, that node is in relay mode. Hence a relay penalty of 1 added to the hop count. So when the route through node b reaches node e the hop count value will be 3. Therefore a better route through c will be selected. In this case, though route x → b → e → y and route x → c → e → y have the same number of intermediate nodes, the latter route is selected because all the nodes are in direct mode.

7 Example Scenario

Table 1 presents an overview of all the methods used in this work to make data transmission in a WBAN more secure and reliable. Important security requirements of confidentiality and authentication are addressed. In addition, reliability problem is also addressed.

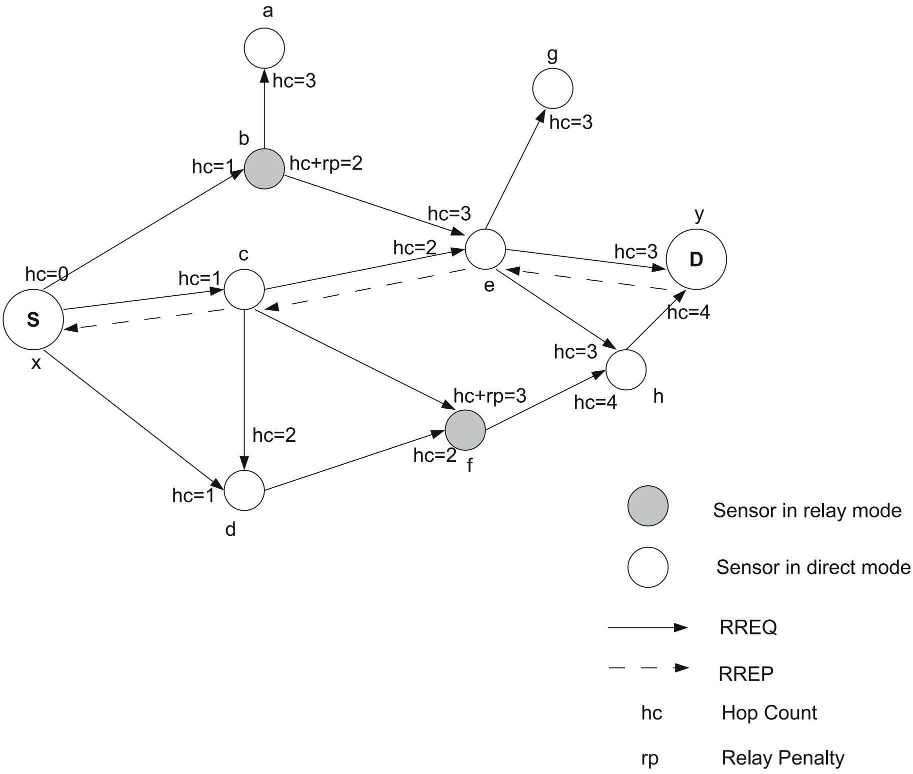

Fig. 6 RelAODV routing in a network

As an example, a WBAN system with sensors to monitor the heart rate of the patients is considered. The sensors are fed with the normal values of heart rate. The activity of a person can be guessed by knowing the heart rate values. The sensors are also programmed to send critical message when the value goes below a threshold limit of 45 or exceeds a threshold limit of 130.

The regular values are sent every 5 min. Whenever a message needs to be sent, the sensor has to apply the RSA algorithm to encrypt and also generate a random number to be attached to the message. The node will be in direct mode but the transmission power should not exceed 13.98 dBm. When the power exceeds this limit it is harmful for the human body and may cause damage to the tissue. When the power goes lesser than 10dBm threshold, a node goes to the relay mode.

To send a message, RelAODV protocol sends RREQ message to find the route to the coordinator. Since a message is sent every 5 min, a route once established may not undergo much change for a number of messages. The routing table will have only one entry and that is the route to the coordinator (available in personal server). The sensor will send the message to the coordinator in one or more hops through the other sensors in the body.

The personal server maintains a cache of random numbers. Once a message arrives, it checks for the random number in the cache. If the currently received random number is not in the cache, the message is accepted and it is forwarded to the medical server without decryption. All the messages received are saved at the personal server for 1 h. Not decrypting the message at the personal server improves the security of the system as the personal server should not become a point-of-failure. However, if the patient himself wants to view the heart rates collected for the past 1 h, all the saved messages are decrypted. This is done only on providing a password known only to the patient.

From the personal server, data is forwarded to the medical server through the Internet. In case of critical messages, i.e., heart rate exceeding the threshold, the data is passed on as SMS directly to the doctor. The medical server maintains a large database and logs all the received data from hundreds or even thousands of personal servers. At the medical server, each medical professional is provided with a login. Data which can be viewed by a person is decided by the access control policies provided by the administrator of the server. Thus a medical professional can remotely view his patient's data and may initiate action whenever necessary.

8 Results

The performance of the system and a comparison of SRDT with EPR [18] and RelAODV with C-AODV [24] have been done taking various parameters into consideration. The following metrics are used to measure the quality of the proposed system.

Table 1 Methods in SRDT and their placement

Methods	Use	Present at
RSA algorithm	Confidentiality, authentication	Sensor node, personal server, medical server
Random number generator	Prevents replay attacks	Sensor node
Nonce database	Prevents replay attacks	Personal server
SHA-1 [23]	Authentication	Personal server, medical server
RelAODV	Reliability	Sensor nodes, personal server

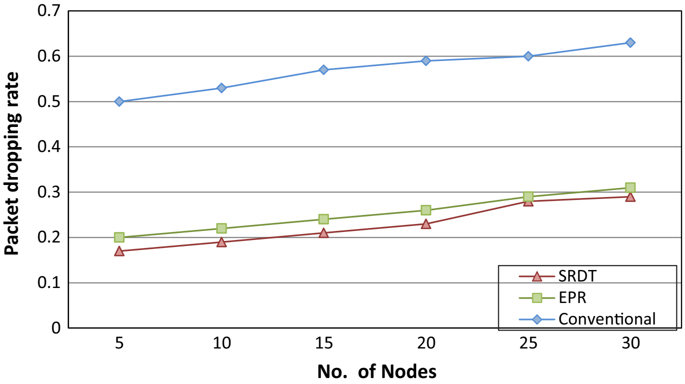

Fig. 7 No. of nodes versus Packet dropping rate

8.1 Performance of SRDT

First a comparison has been done between SRDT, EPR [18] and IEEE 802.15.4 with AODV routing which is referred to as conventional system. Different metrics like packet dropping rate, throughput and energy spent have been analyzed in order to find which of the systems is more reliable.

Figure 7 shows packet dropping rate plotted against varying number of nodes. The graph shows that there is not much variation in packet dropping rate when the number of nodes is increased. It remains almost constant. The performance of SRDT is significantly higher and has much lesser packet dropping rate than the conventional system. It is also better than EPR. The graph also shows the scalability of SRDT as pretty much stable.

Figure 8 shows variations in packet dropping rate when the transmission power is changed. As expected, the more the transmission power, the lesser the number of packets dropped. Again, this graph shows better reliability of SRDT as it has lesser dropping rate compared to EPR and the conventional system. Though the analysis has been done for transmission power up to 20 dBm, in real life the transmission power of a node cannot be increased above 13.98 dBm as any higher rate may cause damage to the tissue. The graph clearly shows the advantage of using nodes in direct mode (transmission power above 10 dBm). In relay mode packet dropping rate increases significantly.

The throughput of the system, that is, the percentage of packets successfully transmitted against the total number of packets sent through the network is compared for the three schemes (Fig. 9). A high throughput of about 80 % is observed when SRDT scheme is implemented. From the graph it can be inferred that it is higher than the EPR and conventional schemes.

The graph in Fig. 10 takes an important parameter viz., energy and compares the amount of energy spent in SRDT and EPR systems. As shown, the energy spent by the EPR system is higher than SRDT. Considering WBAN this shows a significant improvement as these are required to be highly energy efficient networks. The energy efficiency is due to the nodes going to relay mode below a certain threshold. RelAODV also gives lesser priority to relay nodes and hence saves a lot of energy.

8.2 Performance of RelAODV

In this section, the performance of RelAODV is compared with C-AODV [24] and AODV. C-AODV is a co-operative routing algorithm based on AODV. In C-AODV, multiple routes to a single destination are maintained and the most congestion-free route is selected for transmission thus improving reliability. The comparisons in this section target the reliability of these two protocols.

The graph in Figs. 11 and 12 compare the packet delivery ratio by varying the pause time and number of nodes in the network respectively. Packet delivery ratio is the ratio of the number of packets received successfully and the total number of packets transmitted. For lesser pause times, the packet delivery ratio of RelAODV is slightly higher than C-AODV and significantly higher than AODV. The effect of RelAODV over AODV is significant in WBANs with higher postural mobility.

The graph in Fig. 12 compares RelAODV, C-AODV and AODV for packet delivery ratio similar to the previous graph but this time the number of nodes is varied. Both for RelAODV and AODV lesser number of nodes gives better reliability. Still, comparatively RelAODV gives higher packet delivery ratio.

Figure 13 shows the graph depicting the routing overhead comparison of RelAODV and AODV by varying the number of nodes. Routing overhead is the number of control packets sent by the routing protocol. RelAODV has a slightly higher routing overhead since RERR packets are sent whenever a node switches over from direct mode to relay mode and vice versa.

In conclusion, based on all the simulations and comparisons performed RelAODV and SRDT in general has performed well and has shown better reliability than the existing systems. Only the routing overhead is slightly higher but the advantages shadow this slight disadvantage.

8.3 Security Analysis

The energy analysis of SRDT (Fig. 10) shows that adding security to the system has not affected its performance in terms of the parameters that were taken into consideration. Since RSA algorithm is used, the data sent as both critical message and non-critical

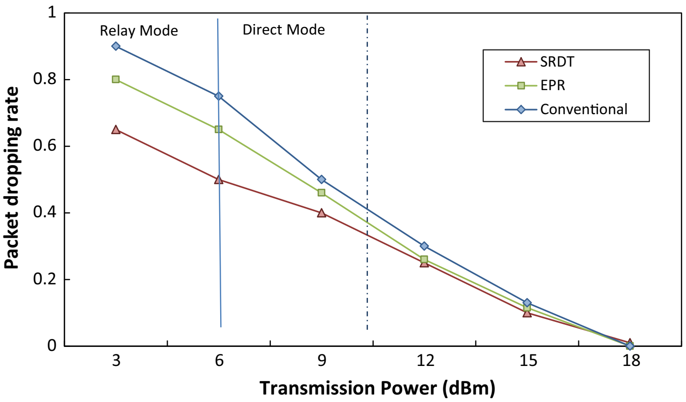

Fig. 8 Transmission power versus packet dropping rate

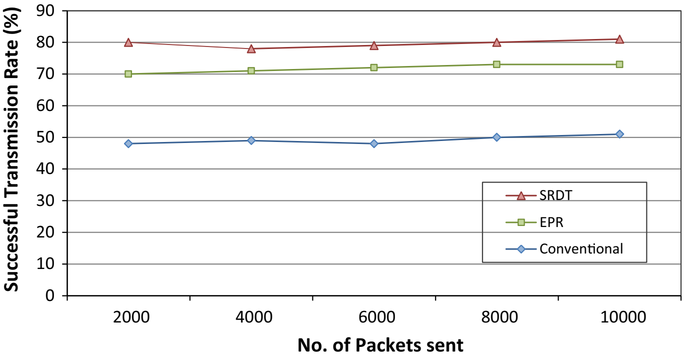

Fig. 9 Throughput

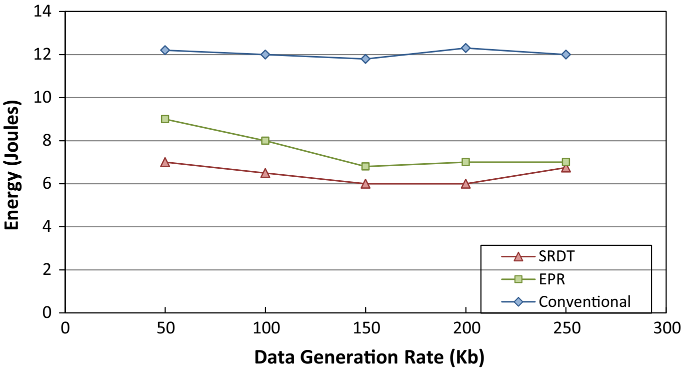

Fig. 10 Data generation rate versus energy

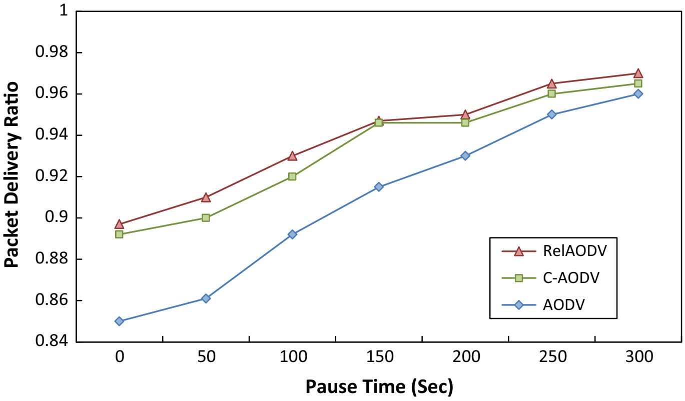

Fig. 11 Pause time versus packet delivery ratio

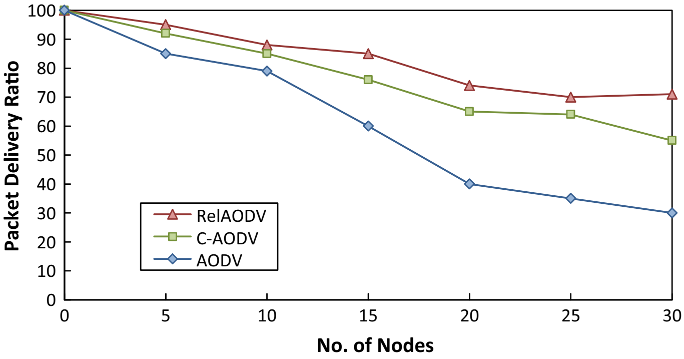

Fig. 12 No. of nodes versus packet delivery ratio

message are hard to break. Critical messages go through an extra encryption for authentication. For a WBAN with its sensors storing limited battery power, the main factor of concern is energy consumption. The energy consumed by critical messages and non-critical messages are compared in Fig. 14. Though the energy consumed by critical messages is significantly more than the energy consumed by non-critical messages, since critical messages are less common it does not lead to energy degradation.

9 Conclusions and Future Work

Patient-related data stored in the WBAN play a critical role in medical diagnosis and treatment. Hence it is essential to ensure the security of these data. The SRDT system addresses the most important security requirements of confidentiality and authentication and also improves upon transmission reliability compared to the existing protocols. In this paper we proposed the classification of nodes as direct and relay nodes to help in saving battery power and to reliably route packets to the coordinator. We also proposed the classification of messages into critical and non-critical information to bestow more intelligence to the sensor nodes. Finally we enhanced the AODV routing protocol and proposed

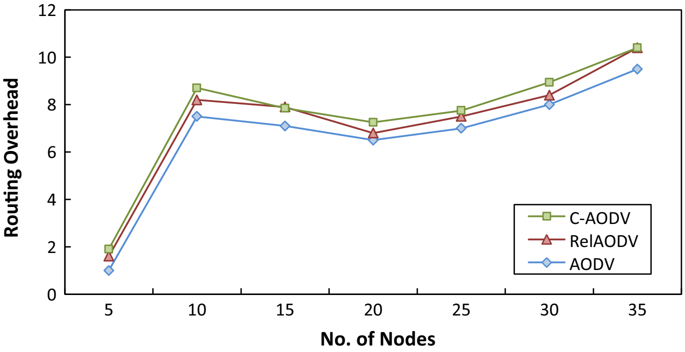

Fig. 13 No. of nodes versus routing overhead

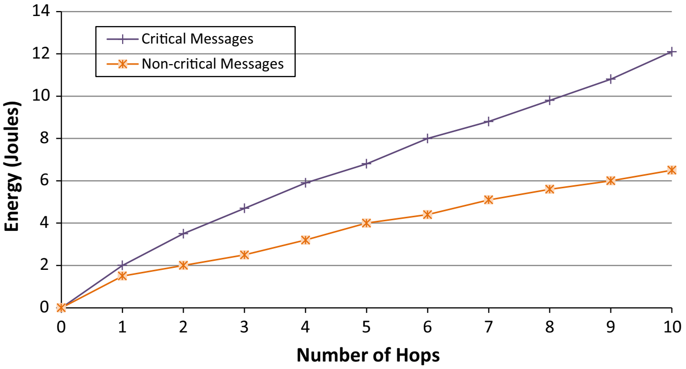

Fig. 14 Energy consumed by critical versus non-critical messages

RelAODV for better reliably in routing packets. SRDT has yielded better results in terms of packet drop ratio, packet delivery ratio and better management of transmission power improving the overall reliability of the system.

WBAN routing is always from a source sensor to a coordinator. The destination does not change and the number of sensors is also very less. Moreover, movement is mostly due to postural mobility. In future we plan to exploit the above said features of a WBAN and improve the SRDT system. The proposed system provides some amount of intelligence to the sensor nodes. Yet, more intelligent sensors that decide the authority to be reported in case of specific problems or suggesting possible diagnostics to the doctor by analyzing the sensor data improve the system and its acceptance rate among the patients.

References

1. Crosby, G. V., Ghosh, T., Murimi, R., & Chin, C. A. (2012). Wireless body area networks for healthcare: a survey. *International Journal of Ad hoc, Sensor & Ubiquitous Computing (IJASUC), 3*(3), 1–26.
2. Yilmaz, T., Foster, R., & Hao, Y. (2010). Detecting vital signs with wearable wireless sensors. *Sensors, 10*(12), 10837–10862.
3. Marinkovic, S. J., Popovici, E. M., Spagnol, C., Faul, S., & Marnane, W. P. (2009). Energy-efficient low duty cycle MAC protocol for wireless body area networks. *IEEE Transactions on Information Technology in Biomedicine, 13*(6), 915–925.
4. Birari, V. M., Wadhai, V. M., & Helonde, J. B. (2012). Mobility management in wireless body area network for patient monitoring system. In *IJCA proceedings on international conference in computational intelligence (ICCIA 2012)*, ICCIA(7).
5. Li, H.-B., Takahashi, T., Toyoda, M., Katayama, N., Mori, Y., & Kohno, R. (2008). An experimental system enabling WBAN data delivery via satellite communication links. In *IEEE international symposium on wireless communication systems. 2008. ISWCS'08* (pp. 354–358). IEEE.
6. Huang, C., Liu, M., & Cheng, S. (2010). WRAP: A weighted random value protocol for multiuser wireless body area network. In *2010 IEEE 11th international symposium on spread spectrum techniques and applications* (pp. 116–119).
7. Iyengar, S., Durresi, A., Paruchuri, V., & Kannan, R. (2005). Data integrity protocol for sensor networks. *International Journal of Distributed Sensor Networks, 1*(2), 205–214.
8. Saleem, S., Ullah, S., & Kwak, K. S. (2011). A study of IEEE 802.15. 4 security framework for wireless body area networks. *Sensors, 11*(2), 1383–1395.
9. Sampangi, R. V., Dey, S., Urs, S. R., & Sampalli, S. (2012). A security suite for wireless body area networks. arXiv preprint arXiv:1202.2171.

10. Mana, M., Feham, M., & Bensaber, B. A. (2011). Trust key management scheme for wireless body area networks. *IJ Network Security, 12*(2), 75–83.
11. Liu, J., & Kwak, K. S. (2010) Hybrid security mechanisms for wireless body area networks. In *2010 Second international conference on ubiquitous and future networks (ICUFN)* (pp. 98–103). IEEE.
12. Raazi, S.-R., Lee, S., Lee, Y.-K., & Lee, H. (2009). BARI: A distributed key management approach for wireless body area networks. In *CIS'09. International conference on computational intelligence and security, 2009* (Vol. 2, pp. 324–329). IEEE.
13. Barua, M., Alam, M. S., Liang, X., & Shen, X. (2011) Secure and quality of service assurance scheduling scheme for wban with application to ehealth. In *Wireless Communications and Networking Conference (WCNC), 2011 IEEE*, 2011 (pp. 1102–1106). IEEE.
14. Lee, R.-G., Chen, K.-C., Lai, C.-C., Chiang, S.-S., Liu, H.-S., & Wei, M.-S. (2007). A backup routing with wireless sensor network for bridge monitoring system. *Measurement, 40*(1), 55–63.
15. Liang, X., Li, X., Shen, Q., Lu, R., Lin, X., Shen, X., et al. (2012). Exploiting prediction to enable secure and reliable routing in wireless body area networks. In *INFOCOM, 2012 Proceedings IEEE*, (pp. 388–396). IEEE.
16. Zhu, X., Han, S., Huang, P.-C., Mok, A. K., & Chen, D. (2011). Mbstar: A real-time communication protocol for wireless body area networks. In *2011 23rd Euromicro conference on real-time systems (ECRTS)* (pp. 57–66). IEEE.
17. Razzaque, M. A., Hong, C. S., & Lee, S. (2011). Data-centric multiobjective QoS-aware routing protocol for body sensor networks. *Sensors, 11*(1), 917–937.
18. Khan, Z. A., Sivakumar, S., Phillips, W., & Aslam, N. (2014). A new patient monitoring framework and energy-aware peering routing protocol (epr) for body area network communication. *Journal of Ambient Intelligence and Humanized Computing, 5*(3), 409–423.
19. Natarajan, A., Motani, M., de Silva, B., Yap, K.-K., & Chua, K. C. (2007) Investigating network architectures for body sensor networks. In *Proceedings of the 1st ACM SIGMOBILE international workshop on systems and networking support for healthcare and assisted living environments* (pp. 19–24). ACM.
20. Adleman, L. M., Rivest, R. L., & Shamir, A. (1983). *Cryptographic communications system and method*. Google Patents.
21. Perkins, C. E., & Bhagwat, P. (1994). Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers. In *ACM SIGCOMM computer communication review* (Vol. 24, pp. 234–244). ACM.
22. Perkins, C., Belding-Royer, E., & Das, S. (2003). *RFC 3561-ad hoc on-demand distance vector (AODV) routing. Internet RFCs* (pp. 1–38).
23. Eastlake, D., & Jones, P. (2001). *US secure hash algorithm 1 (SHA1)*. RFC 3174, September.
24. Manfredi, S. (2012). Reliable and energy-efficient cooperative routing algorithm for wireless monitoring systems. *Wireless Sensor Systems, IET, 2*(2), 128–135.

Dr. Kanaga Suba Raja is working as an Associate Professor in the Department of Information Technology in Easwari Engineering College. He obtained his Ph.D. degree in Computer Science in 2013 from Manonmaniam Sundaranar University, Tirunelveli. He has about 10 years of teaching and research experience. He has successfully guided many graduate and under-graduate students for their research projects. He has several papers published in International journals and conferences to his credit. His current research interests are wireless body area networks, ad hoc and sensor networks and mobile and ubiquitous computing.

Usha Kiruthika is a research scholar in the department of Computer Technology in Madras Institute of Technology, Chennai. She completed her bachelor's degree in Information Technology at Crescent Engineering College, Chennai and her master's degree in Computer Science and Engineering at SSN College of Engineering, Chennai. She is currently pursuing her Ph.D. in the area of cloud computing. Her research interests are automated negotiation, service level agreement (SLA) management in cloud, grid computing and ad hoc and sensor networks.