Journal of Computer Science 2012, 8 (11), 1780-1787
ISSN 1549-3636
© 2012 Science Publications
doi:10.3844/jcssp.2012.1780.1787 Published Online 8 (11) 2012 (http://www.thescipub.com/jcs.toc)

A Secure Key Management Technique for Wireless Body Area Networks

[1]Venkatasubramanian Sivaprasatham and [2]Jothi Venkateswaran

[1]Department of Information Technology, Nizwa College of Technology, Oman
[2]Department of Computer Science, Presidency College, Chennai, Tamil Nadu, India

Received 2012-07-02, Revised 2012-08-29; Accepted 2012-09-04

ABSTRACT

In Wireless Body Area Networks (WBAN), the key factors to be considered for transmission of confidential data are security and privacy as it is mostly having applications in emergency medical response systems. The lack of security may lead to loss of data privacy resulting in an adversary to bring in bogus data or altering the legal ones. Hence in this study, a secure key management technique for WBAN is proposed. The proposed architecture consists of a set of WBANs connected to the master server via backend server using authentication channel. Initially, backend server and master server use a shared symmetric key. When a node wants to join a network, it forwards a request message protected by the Message Authentication Code (MAC) to the master server via the backend server. The master server verifies the MAC and generates message key and master key for the node and sends it to backend server. The backend server encrypts the message key with the master key and sends it to the node that initiates the joining process. After all nodes receive key information from the master server, the Base Server (BS) schedules a re-keying period to refresh the master key. By simulation results, it is shown that the proposed technique is more authenticated. The proposed approach offers data confidentiality and integrity in WBANs.

Keywords: Message Authentication Code (MAC), Wireless Body Area Networks (WBAN), Base Server (BS), BAN Network Controller (BNC), BAN Nodes (BNs)

1. INTRODUCTION

1.1. Wireless Body Area Network (WBAN)

Zimmerman (1996) established the concept of WBAN which is otherwise defined as Wireless Personal Area Network (WPAN) (Li *et al*., 2010). WBAN is the network that permits the combination of smart, small scale, minimum power, aggressive/discreet sensor nodes which monitors body activities and neighboring environment. Every intelligent node in the network has potential to forward the information to the base station after processing to obtain the diagnosis and prescription (Ullah *et al*., 2009). The application of WBANs is concerned with medical field and it also upholds consumer electronics applications concurrently (Khan *et al*., 2009).

The features of WBAN are listed below (Li *et al*., 2010):

- It is a miniature wireless network for communicating within 3 m gap
- The speed at which the data is transmitted varies from 10 Kbps to 10 Mbps
- The star topology is the fundamental arrangement considered in WBANs and BAN Nodes (BNs) communicate with BAN Network Controller (BNC) alone
- BNs possess restricted power, calculation and communication capabilities
- Energy efficient security mechanism is required with reduced overhead and also the requirement such as data integrity, authentication and encryption should be fulfilled
- The network surrounds the body closely for implanting its communication system
- BAN mainly detects, collects and transmits the biomedical information

Corresponding Author: Venkatasubramanian Sivaprasatham, Department of Information Technology, Nizwa College of Technology, Oman

The key issues to be accounted while designing WBAN are Power limitation and short RF transmission range, Mobility, Minimum and time-dependant quality of wireless links and Network size (Nabi *et al*., 2010).

1.2. Security Risks in WBANs

The susceptible nature of wireless channels results in a wide range of security threats distracting the WBAN's progress (Saleem *et al*., 2011). Depending on the network layers, the attacks over WBAN are categorized into following classes:

- Physical layer attacks
- Data link layer attacks
- Network layer attacks
- Transport layer attacks

1.3. Fundamental Security Requirements in a WBAN

This section presents the fundamental security requirements of WBANs (Saleem *et al*., 2009), such as:

- Data Confidentiality
- Data Authentication
- Data Integrity
- Data Freshness.
- Secure Management
- Availability

1.4. Proposed Work

To avoid compromised attacks on preloaded keys and reduce the overhead, a new secure key management mechanism for WBAN is proposed in this study.

1.5. Related Work

Tan *et al.* (2009) have developed a lightweight Identity-Based Encryption (IBELite) suitable for sensors in a BSN. Their protocol balances security and privacy with accessibility. However the proposed system can release n secret keys. When we try to release (n+1) th secret key then the master key is vulnerable to compromise.

Venkatasubramanian and Gupta (2010) have presented a novel scheme for securing inter-sensor communication in BSNs called Physiological Value based Security (PVS). Their scheme distributes the key along with the message by hiding it using physiological values.

The proposed security method, however, can be used only when the entire sensor measures the same IPI signals as physiological values which are very difficult. It has more effects of topographic specificity, which has the potential to eliminate key distribution completely.

Mohanavalli and Anand (2011) have presented an architecture which continuously monitors the patients at home using BSN. Their scheme facilitates senior citizens, patients with chronic illness and patients who need to be remotely monitored in the comfort of their homes, but this work does not consider end to end security as they use basic authentication techniques.

Sharma and Bansal (2011) have examined impersonate attacks in WBAN. They proposed this technique to guarantee whether wireless sensors in a WBAN are transmitting and receiving data from authorized or authentic sources. They utilized digital certificates to overcome Impersonate Attacks.

Raazi and Lee (2009) have proposed a distributed key management scheme for WBAN. The keys they used initially for personal server and sensor nodes are preloaded keys, so they can be compromised by adversaries. If initial keys are compromised, then further security operations are useless.

2. MATERIALS AND METHODS

2.1. Secure Key Management Technique

2.1.1. Overview

In this study, a new secure key management mechanism for WBAN is proposed. The proposed architecture consists of a set of WBANs connected to the backend server. The backend server relay the biometric information measured by the sensor node to the master server through the internet. All sensor nodes will discover the master server by using a node id. The master server will then generate a unique secret key for each node. When a node wants to join a network, it forwards a request message protected by the MAC to the master server via the backend server. The master server verifies the MAC and generates a message key and a master key for the node and sends it to backend server. The backend server encrypts message key with master key and sends it to the sensor node that initiates the joining process. After all nodes receive key information from master server, the BS schedules re-keying period to refresh the master key.

2.2. Proposed Architecture

Our proposed architecture consists of a set of WBANs, Backend Server (BS) and Master Server (MS).

In **Fig. 1** a WBAN network consists of few sensor devices deployed on a human body which are connected to a Backend Server (BS). The BSs of various WBANs are connected to a Master Server (MS).

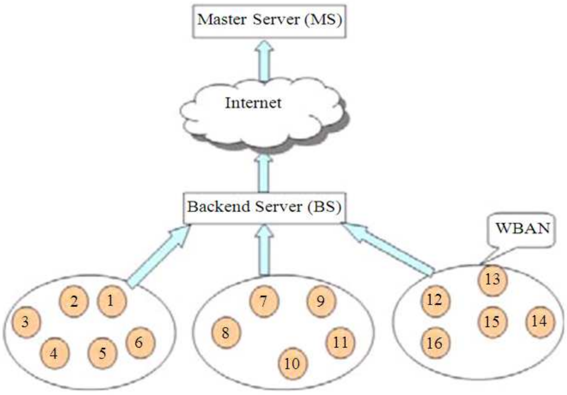

Fig. 1. System architecture

2.3. Backend Server (BS)

The Backend Server (BS) uses three types of keys which are described as follows:

Message Key (K_{msg}) = It is used for communicating with backend server and other nodes

Master Key (K_{mas}) = It is used for refreshing the message key by scheduling the re-keying intervals

Secret key (K_{sec}) = It is shared with the master server and this key is unique for each node

2.4. Private Authentication Channel Creation

The techniques described below are used to create a secure out-of-band channel.

2.5. Manual Authentication Technique

This technique enables wireless devices and authenticates them through wireless channel for assisting manual data transmission among devices. The manual data transfer involves the operator’s actions such as replication of the data output from one device to the other device, comparison of output of two devices, entering similar data into both the devices. This process does not necessitate the user to enter long strings of digits. In general, the user has to enter (or compare) approximately 32 binary digits (Gehrmann *et al*., 2004).

2.6. Distance Bounding Protocols

This protocol merges physical and cryptographic properties and allows the host to estimate the upper-bound distance which demands to be inside the transmission range. The estimation of upper bound distance considers the metrics such as Received Signal Strength (RSS), Angle of Arrival (AoA) or Time of Flight (ToF). For securing the distance bounding protocols, the time of flight is taken into consideration (Singelee and Preneel, 2007).

2.7. Symmetric Key Generation

For any message transmitted in the network, encryption and authentication are required. Initially, sensor nodes SN_i share a symmetric key with MS.

The symmetric key $K_{sy}^{SN_i}$ for a sensor node SN_i is generated as follows Equations 1-4:

$$K_{sy}^{SN_i} = \lambda k_{sec}(SN_i) \quad (1)$$

where, λ = pseudo random function. K_{sec} (SN_i) = secret key of the sensor node After successful authentication, the Master Server (MS) supplies a unique master key (K_{sec}) to each SN_i. K_{sec} holds two sub-keys such as the encryption key (k_e) and the Message Authentication Code (MAC) key (k_{mac}):

$$K_M = k_e + K_{mac} \quad (2)$$

$$SN_i \xleftarrow{K_{sec}} MS \quad (3)$$

When SN_i wants to transmit the data to MS, the data is encrypted by the k_e and signed by the MAC key K_{mac} before transmission. The format is as follows:

$$SN_i \to MS : \{d \mid t_s\}_{ke,} \, mac(K_{mac}\{d \mid t_s\}_{ke}) \quad (4)$$

where, D is the data, Ts is the timestamp during data transmission and mac (K, d) represents the computation of the message authentication code of message d with key K.

When MS receives the data from any node, a verifies the data and then decrypts it. The secured communication is ensured among the node and MS by the encryption key and MAC key (Wang *et al*., 2007).

2.8. Initialization

Each Sensor Node (SN) is initialized with security by MS prior to joining the WBAN. In this phase, MS and BS use a shared symmetric key. This is performed with the help of private and authenticate out-of band channel. The creation of private and authenticate channel is based on the physical characteristics of the sensor nodes.

Using this technique, the data can be sent through the channel confidentially such that data integrity and authenticity are also protected. The backend server performs like gateway and it is a private authentic channel which provides secure communication between WBAN nodes and master server Initialize the sensor node SN_i.

The steps involved in the transfer of the data through the secure out-of-band channel are as follows.

SNi sends its ID to the Master Server (MS):

$$SN_i \xrightarrow{ID} MS$$

This can be performed in an explicit manner. However the ID of SNi can be known implicitly due to certain properties of the out-of-band channel.

MS generates a random secret key K_{sec} and forwards it to SN_i:

$$SN_i \xleftarrow{K_{sec}} MS$$

Both SN_i and MS stores K_{sec} in their memory.

It is to be noted that each SN_i is assigned with a unique secret key K_{sec}. Also it is assigned with a unique Counter (C) with initial value as 0 (CTR→0) and stored in the sensor's buffer. The counter values helps in preventing replay attacks and guarantees consistency. Each time the counter is accessed, the value is incremented by 1.

2.9. Node Joining

The new nodes are added to the network during the following circumstances.

- Deployment of new nodes for monitoring certain biometrics
- Malfunctioning of a node device

The Node joining process is described using the following algorithm.

Algorithm 1.

SN_i forwards a Join Request (JREQ) to the BS:

$$SN_i \xleftarrow{JREQ} BS$$

JREQ is protected by MAC generated by K_{sec} by the joining SN_i:

$$JREQ : MAC\_K_{sec}$$

BS forwards the JREQ to MS:

$$BS \xrightarrow{JREQ} MS$$

MS verifies the MAC and generates initial message key K_{msg} and master key K_{mas} for the node and forwards them to BS:

$$MS \xrightarrow{K_{msg}+K_{mas}} BS$$

BS encrypts K_{msg} with K_{mas} and sends it to SN_i

$$BS \xrightarrow{EK_{mas}\{K_{msg}\}} SN_i$$

2.10. Re-Keying

When SN_i receives key information from the MS, BS schedules re-keying period to refresh the master key. The BS broadcasts the re-keying period along with the new updated K_{msg}, encrypted by K_{mas} to the SN_i:

$$BS \xrightarrow{EK_{mas}\{K_{msg}\}} SN_i$$

During the re-keying period, SNi sends a rekeying request (RE_REQ) message to MS through the BS:

$$SN_i \xrightarrow{RE\_REQ} BS(\text{Authentication channel}) \xrightarrow{RE\_REQ} MS$$

MS updates a new master key K'_{mas} and forwards this K'_{mas} encrypted by Ksec to all the respective SN_i:

$$MS \xrightarrow{Ek'mas\{K_{msg}\}} SN_i$$

Proposed Algorithm:

Step 1: The proposed architecture is constructed that includes a set of WBANs, Backend Server (BS) and Master Server (MS). A WBAN network consists of few sensor devices deployed on a human body which are connected to a Backend Server (BS)

Step 2: The backend server and master server agree on a shared symmetric key. All the sensor nodes will discover the master server by using a node id, now master server will generate the unique secret key k_{sec} for each node

Step 3: When a node wants to join a network, it will send a request REQ to the backend server. The REQ is protected by Message Authentication Code (MAC), generated by the unique secret key k_{sec} by the joining node

Step 4: Upon receiving the REQ message, the backend server forwards the REQ to the master server

Step 5: The master server verifies the MAC and generates initial message key k_{msg} and master key k_{mas} for the node and forwards them to backend server

Step 6: The backend server encrypts k_{msg} with k_{mas} and sends it to the sensor nodes

Step 7: After all nodes receive key information from master server, the BS schedules rekeying period to refresh the master key

3. RESULTS AND DISCUSSION

3.1. Simulation Parameters

To simulate the proposed Secure Key Management Technique (SKM), NS2 Network Simulator is used. A network area of 50×50 m is considered. The IEEE 802.15.4 (Shelby and Bormann, 2011) is used as MAC layer since it provides reliable communication for the devices. For all types of communications, it provides access to the physical channel. It also supports security features. The IEEE 802.15.4 specification uses Physical layer (PHY) options based on Direct Sequence Spread Spectrum (DSSS) which uses the frame structure for low-duty-cycle low power operation containing a 32-bit preamble frame length.

The Exponential traffic is used for transmission and UDP is as transport protocol between source and sink. **Table 1** summarizes the simulation parameters used.

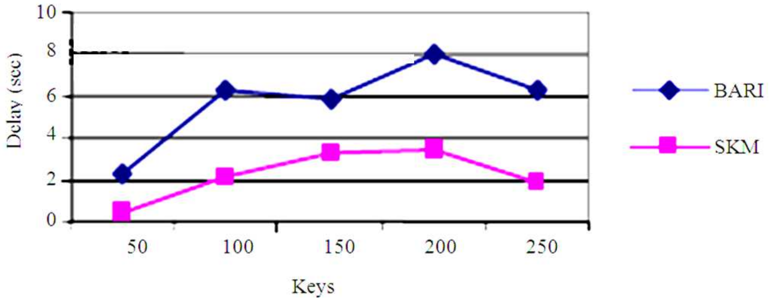

Fig. 2. Keys Vs delay

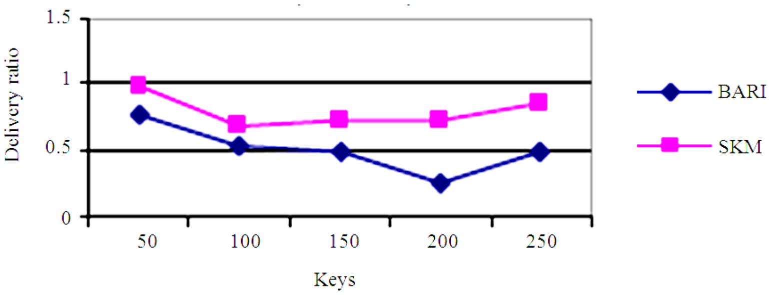

Fig. 3. Keys Vs delivery ratio

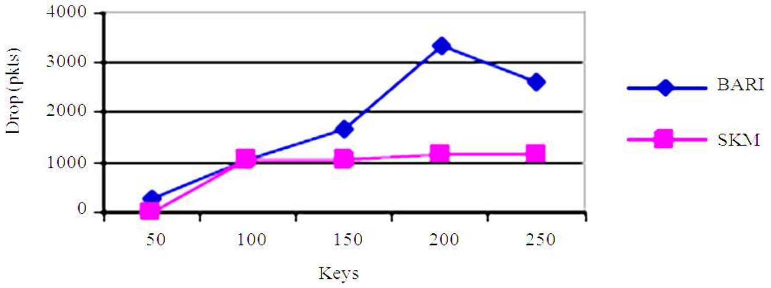

Fig. 4. Keys Vs drop

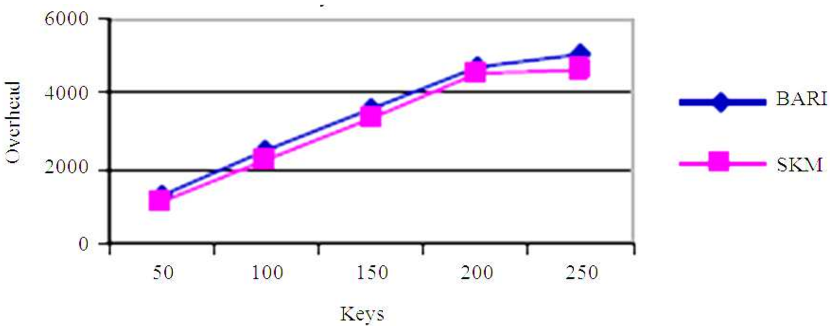

Fig. 5. Keys Vs overhead

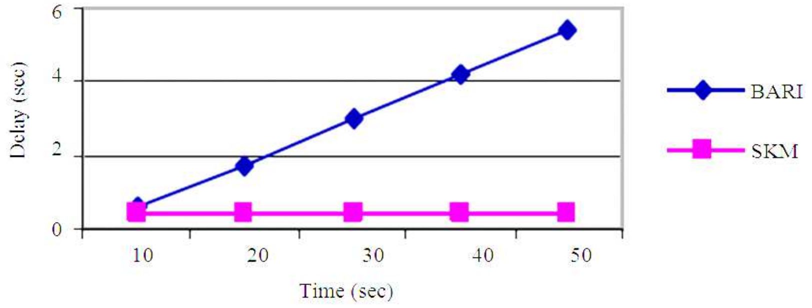

Fig. 6. Time Vs delay

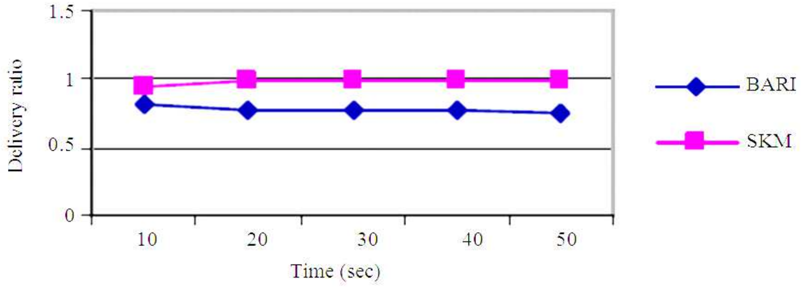

Fig. 7. Time Vs delivery ratio

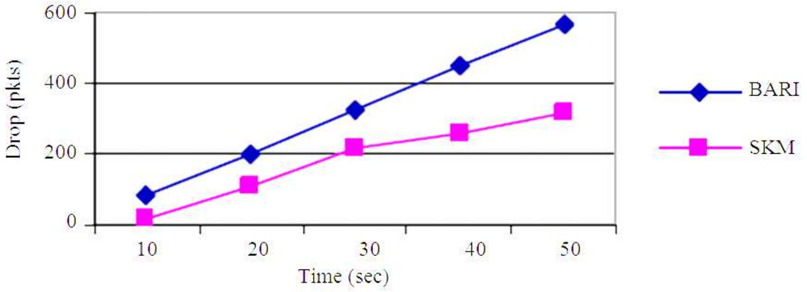

Fig. 8. Time Vs Drop

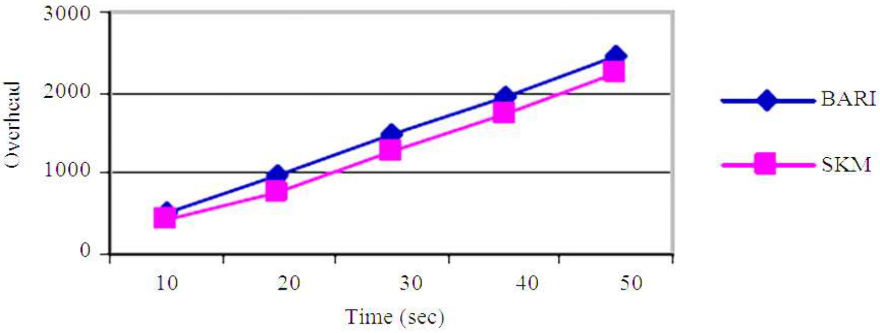

Fig. 9. Time Vs Overhead

Table 1. Simulation parameters

Total nodes	22
Area size	50×50
MAC protocol	IEEE 802.15.4
Simulation time	25 sec
Transmission range	25m
Routing protocol	SKM
Traffic source	Exponential
Packet size	512
No. of keys	50, 100, 150, 200 and 250Kb.
Simulation time	10,20,30,40 and 50 sec.

3.2. Performance Metrics

The BARI (Raazi and Lee, 2009) scheme is considered for performance comparison with SKM. The performance is evaluated based on the following metrics: Average end-to-end delay, Average Packet Delivery ratio and packet drop.

3.3. Varying the Keys

Initially the number of keys is varied from 50-250.

Figure 2 shows that the average end-to-end delay of our proposed SKM protocol is less than the existing BARI scheme. **Figure 3** gives the delivery ratio for both the schemes and it is high for the proposed SKM protocol than the existing BARI scheme. The result of **Fig. 4** shows that the packet drop of our proposed SKM protocol is less than the existing BARI scheme. From **Fig. 5**, we can see that the overhead of our proposed SKM is lower than the existing BARI scheme.

The average end-to-end delay is represented in **Fig. 6**. It shows that proposed SKM technique has less delay than the existing BARI scheme. **Figure 7 and 8** show the result of packet delivery ratio and packet drop, respectively. We can observe that the delivery ratio is high and packet drop is less for SKM technique when compared to BARI scheme. From **Fig. 9**, we can see that the overhead of our proposed SKM is lower than the existing BARI scheme.

4. CONCLUSION

A secure key management technique for WBAN is proposed in this study. The proposed architecture contains a set of WBANs connected to the backend server. The backend server relay the biometric information measured by the sensor node to the master server through the internet. The proposed technique uses shared symmetric key between the backend and master servers in order to ensure authentication of the backend server. The proposed technique is simulated in NS2 and compared with the BARI scheme. The performance is evaluated based on Average end-to-end delay, average packet delivery ratio, packet drop and overhead. Simulation results are in favor of the proposed technique which show improved packet delivery ratio with reduced delay and overhead.

5. REFERENCES

Gehrmann, C., C.J. Mitchell and K. Nyberg, 2004. Manual authentication for wireless devices. Cryptobytes, 7: 29-37.

Khan, P., M.A. Hussain and K.S. Kwak, 2009. Medical applications of wireless body area networks. Int. J. Digital Content Technol. Appli.

Li, C., J. Li, B. Zhen, H.B. Li and R. Kohno, 2010. Hybrid unified-slot access protocol for wireless body area networks. Int. J. Wireless Inform. Networks, 17: 150-161. DOI: 10.1007/s10776-010-0120-2

Mohanavalli, S.S. and S. Anand, 2011. Security architecture for at-home medical care using body sensor network. Int. J. Ad-hoc, Sensor, Ubiquitous Comput., 2: 60-69.

Nabi, M., T. Basten, M. Geilen, M. Blagojevic and T. Hendriks, 2010. A robust protocol stack for multi-hop wireless body area networks with transmit power adaptation. Proceedings of the 5th International Conference on Body Area Networks, (BAN' 10), ACM Press, New York, USA., pp: 77-83. DOI: 10.1145/2221924.2221941

Raazi, S.M.K.U.R. and H. Lee, 2009. BARI: A distributed key management approach for wireless body area networks. IEEE International Conference on Computational Intelligence and Security, Dec. 11-14, IEEE Xplore Press, Beijing, pp: 324-329. DOI: 10.1109/CIS.2009.186

Saleem, S., S. Ullah and H.S. Yoo, 2009. On the security issues in wireless body area networks. Int. J. JDCTA, 3: 178-184. DOI: 10.4156/jdcta.vol3.issue3.22

Saleem, S., S. Ullah and K.S. Kwak, 2011. A study of IEEE 802.15.4 security frame work for wireless body area networks. Sensors, 11: 1383-1395.

Sharma, N. and E.M. Bansal, 2011. Preventing impersonate attacks using digital certificates in WBAN. Int. J. Adv. Engin. Sci. Technol., 9: 31-35.

Shelby, Z. and C. Bormann, 2011. 6LoWPAN: The Wireless Embedded Internet. 2nd Edn., John Wiley and Sons, ISBN-10: 1119965349, pp: 244.

Singelee, D. and B. Preneel, 2007. Key establishment using secure distance bounding protocols. Proceedings of the 4th annual international Conference on Mobile and Ubiquitous Systems: Networking and Services, Aug. 6-10, ACM Press, USA., pp: 1-6. DOI: 10.1109/MOBIQ.2007.4451066

Singelee, D., B. Latr, B. Braem, M. Peeters and M.D. Soete, 2010. A secure low delay protocol for multihop wireless body area network. Ad Hoc Sensor 8 Wireless Netw., 9: 953-72.

Tan, C.C., H. Wang, S. Zhong and Q. Li, 2009. IBE-Lite: A light weight identity based cryptography for wireless body area networks. IEEE Trans. Inform. Technol. Biomed., 13: 926-932. DOI: 10.1109/TITB.2009.2033055

Ullah, S., B. Shen, S.M.R. Islam, P. Khanemail and S. Saleem *et al*., 2009. A study of MAC protocols for WBANs. Rev. Literature Arts Am., 10: 128-145. DOI: 10.3390/s100100128

Venkatasubramanian, K.K. and S.K.S. Gupta, 2010. Physiological value-based efficient usable security solutions for body sensor networks. ACM Trans. Sensor Net. DOI: 10.1145/1777406.1777410

Wang, Y., B. Ramamurthy and X. Zou, 2007. KeyRev: An efficient key revocation scheme for wireless sensor networks. IEEE International Conference on Communications, Jun. 24-28, IEEE Xplore Press, Glasgow, pp: 1260-1265. DOI: 10.1109/ICC.2007.213

Zimmerman, T.G., 1996. Personal area networks: Near-field intrabody communication. IBM Syst. J., 35: 609-617.