Print ISSN: 0974-2115
www.jchps.com Journal of Chemical and Pharmaceutical Sciences

Design of a Secure System for Reading Patient's Data Using Medical Sensor Networks

Radhika Rani Chintala*, Madava Rama Narasinga Rao, Somu Venkateswarlu
Department of CSE, K L University, Vaddeswaram, Guntur.
***Corresponding author: E-Mail: radhikarani_cse@kluniversity.in, Tel: 098 48 56 0009**

ABSTRACT

Wireless sensor networks (WSN) are an important technology that can directly be used in electronic – healthcare, which is useful to collect and process the data of a patient, and then recommend/provide the patient with safe/proper pharmaceutical medication, by using wearable and tiny bio-sensor devices. The data collected from a patient is very important and must be securely protected from attacks. But there are many challenges which are to be dealt with, in the WSN devices because of the constraints in the resources which are very tiny. Even there is very huge in the security and privacy that is to be provided practically. In the present paper, a new security system has been proposed that can be effectively used in the e-health care applications using Medical sensor networks (MSN). The present paper proposes a system that is using a mechanism that is updating key based on hash-chain and a special signature technique which is proxy protected. This system is advantageous as it is useful and helpful in achieving efficient transmission which is secure also. A data access control system that has fine grained mechanism is also proposed in this paper. This system is useful for low powered nodes as it employs symmetric key encoding and/or decoding and hash operations.

KEY WORDS: Medical Sensor Networks, Pharmaceutical medication, Bio sensors, Security.

1. INTRODUCTION

Now a day as the popularity of MSNs is increasing day by day, the technology is also changing at the same pace. As a result, the wearable & portable biosensor devices are developing at the same rate. The communication technologies which are wireless enabled and medical sensor systems (MSNs) which are wireless based have risen as a promising procedure as the method for looking for healthcare at various areas viz., home, clinic or huge medicinal offices (Lorincz, 2004; Choi, 2012). Now there is no need to measure patient's parameters directly. Measuring different parameters of the patients is also possible remotely without any external disturbances with non-stop continuity using MSNs. After that the prepared information will be exchanged to restorative databases. This medicinal data is shared among and got to, for further analysis, by different clients, for example, healthcare staff, scientists, government organizations, insurance agencies, and patient's relatives too. Through thusly, healthcare processes, for example, clinical conclusion and crisis restorative reaction, will be encouraged and facilitated, in this way significantly expanding the effectiveness of medicinal services.

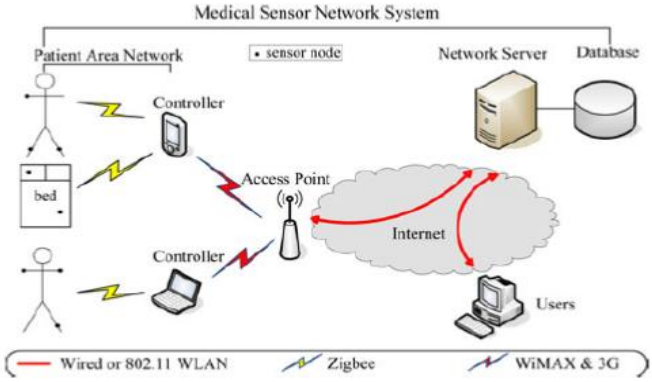

Figure.1. Architecture of a typical medical sensor network

Fig.1, shows sample Medical Sensor Network's (MSN) architecture. More number of Patient Area Networks (PAN) can be covered typically by a large-scale MSN. Every one of the PAN is equipped with few bio-sensor nodes and a generally a medium or small processing unit is also contained in the PAN. (e.g., tablet PC, smart phone or desktop computer), which is generally called by the name controller. In the PAN, portable or easily implantable bio-sensor nodes are fixed to a patient for continuously monitoring the patient health condition and also for recording the patient health details like Personal Health Data (PHD). Thus, recorded data is sent to the controller for further processing. The controller will establish communication link with remotely located server and will inform the PHD to it. The authorized users (e.g. Doctors) can execute the pre-written programs to access the PHD from the server or can command the bio-sensors of an identified patient area network. Point to be noted here is that the biosensor nodes will be communicating only with controller node, but will never communicate with the authorized users. Because the bio-sensor nodes may not be able to identify the users, whose number may be in thousands in many cases.

The PHD thus collected is private information belonging to a particular patient. This PHD will play a crucial and viral role in diagnosing a patient medically and to treat the patient accordingly. Hence it is quite essential to take every care regarding who is accessing this PHD and it is necessary to see that only the concerned doctor is accessing this data for further treatment. This not only gives medical security to the patient but also safeguards the patient's security (Lorincz, 2004).

Keeping all the above one has to design and implement safest and most secure MSN in the medical field. While designing such a system the below listed problems have to be faced by the designer:

- The system that is going to be designed is for the usage of Medical field which requires utmost security. Hence all types of security concerns have to be implemented.
- The portable bio-sensors used in the patient body are having very less battery power, their processing power, internal storage capacity and speed for data transfer are very less in fact. Keeping all these data one has to design the security parameters. Or else the total system may fail to function.
- The size of the bio-sensor nodes is tiny. As a result, there is every possibility that these may be lost easily or patient might lose them easily.
- These bio-sensor nodes may be stolen easily and hence they can be manipulated.

To address the above issues, some contributions have been made in this paper. They are:

- The security loop holes and performance problems of the prevailing security systems in MSNs have been identified.
- The main parameters of the medical sensor nodes have been identified. Then the requirements of highly secured & easy to use system of MSNs have been presented. By keeping in view the special characteristics of MSN, *a robust mobile and portable adversary* is introduced.
- The proposed highly secured and easy to use system for MSN, apart from enabling a key mgmt. that is easy for usage, the proposed system will provide access control that is fine grained. In addition, the conceptual analysis of the proposed system has shown that the requirement of security can easily be met by it.

2. RELATED WORK

As on date, though there is severe need and requirement of a best secure and easy to use system in medical field, there is no such system available for patient data transmission and PAN access control mechanism.

In the recent past, a network architecture (Malasri and Wang, 2007), called "Sensor Network for Assessment of Patients" (SNAP) was proposed for dealing with security issues confronted with sensor network for checking the wellbeing of the network remotely. It is identified that SNAP does not manage client verification for the therapeutic information. The gathered information from a biosensor are communicated in a plain and simple text to the controller. In this way, enemy has the possibility to undoubtedly adjust the therapeutic information & additionally infuse dirtied medicinal information into the system. A few researchers (Rajasekaran, 2012; Wang, 2011), use physiological signs of the patient to empower bio-sensors to concur on a symmetric (shared) cryptographic key in genuine way. In any case, they request that every biosensor can quantify exactly the original physiological parameter; this supposition is prohibitive and makes the same strategy not reasonable.

In line with public key cryptography, for ensuring the security of the sensor networks (Malasri and Wang, 2009; Keoh, 2011; Tan, 2009; Le, 2011), which are wireless, few new protocols have been proposed. The authors (Malasri and Wang, 2009) proposed utilization of ECC - Elliptic-Curve Cryptography to put together symmetric keys in between the base station & sensor nodes. Additionally, an innovative authentication mechanism and group key management was also described. But, they're inefficient in computation. They can't fulfill the rigid delay requirements in WSNs & are susceptible to Denial of Service attacks.

Likewise, a lightweight personality based cryptography having the name as IBE-Lite been thrown light upon (Tan, 2009). It equalizes security and protection with availability. Be that as it may, it is watched that taking after are security shortcomings and effectiveness issues in IBE-Lite.

- ECC is used for encrypting all the medical data that is not effective for Medical Sensor Networks (MSNs).
- False medicinal information could be infused or regarded as honest to goodness because of the absence of hub verification.
- Node replication attacks cannot be resisted by IBE-Lite.
- The main key of every PAN comprises of 'N' secret keys, which the patient selects who is ready for diagnosis. Every specialist doctor utilizes the secret key in order to unravel those messages that are mixed and received from the sensor node. After a doctor communicates 'N' customer requests to goal PAN, he can create the main key of that network PAN. In this way, for ensuring IBE-Lite's security, the quantity of customer inquiries must be compelled. Le (2011), exhibited a shared validation and get the opportunity to control protocol that relies upon ECC. A study has proved that the arrangement described just above is helpless against data spillage problems (Kumar and Lee, 2012).

Several researchers have worked on security in MANETs and Generic WSNs (He, 2011; 2009; Zhao, 2012). The results of these works are not specifically pertinent in MSNs because of the remarkable, testing, operational and security prerequisites of MSNs. For example, the authors He (2011), acquainted an innovative method with guarantee dispersed protection saving control of access that is based on the ring mark system.

Public Key Management methodology has been explained in (He, 2009), here it is possible to generate and store securely few of the encrypted keys, offline, at identified nodes. For keeping away from shortcomings of public key cryptography, it is also possible to use identity-based cryptography as a part of different zones of securing MANETs (Zhao, 2012). Unfortunately, as portrayed some time recently, arrangements depending on public key cryptography aren't straightforwardly appropriate.

MSN Characteristics: Sensor networks used in medical field are different from Ad hoc networks and wireless sensor networks in the following aspects (Choi, 2012).

Data Transfer Rate: Ad hoc Networks and WSNs will continuously monitor the events which generally will occur at different intervals. Whereas the events monitored by the medical sensor networks, viz., human being's physiological activities, occur periodically. Thus, relatively stable rates are exhibited by the data streams of those applications. All the device nodes are lightly synchronized time clocks despite the usage of secure time scheme that is synchronized.

Mobility: All the sensor nodes are implanted in the body of the patient and hence the movement of the nodes is zero. Even the movements of controllers from the nodes is also relatively zero or very less.

Efficiency: The signals which are sensed by the sensor nodes are efficiently received and processed by the biosensors and the result is the physiological information of the patient. The batteries fitted in the bio sensors will consume very low power as the power consumption by the bio sensors is very less.

Network Model: The biosensor nodes implanted in the patient, forming the MSN, have limited resources viz., memory capacity, processing speed and processor's processing capacity and power back up. Because of the limitations in the resources, it will be difficult to run Public Key Cryptography like algorithms on these nodes, as these algorithms will consume more energy and are very expensive computationally. The server of the network that is fitted with resistance free material to store the material that is keyed in. The data rates at which the MSN is working, the time is divided into some fixed values for collecting the data from the biosensor in each and every round.

The nodes which are having bio-sensor may be placed in and around the patient. The data transmission range for effective communication from these bio sensors is larger than 3 mtrs. Hence all the nodes having sensors in a Patient Area Network can communicate directly with the controller.

Adversary Model: The outside aggressors can leave messages by staying in the correspondence channel, listen stealthily messages, modify and inject fashioned messages, or the out dated messages can be replayed. Insider aggressors may exchange off different controllers, biosensor hubs, and framework hubs to secure their key materials & data.

Keeping in view of the remarkable elements of MSN, an effective mobile adversary is brought to MSNs (Ma and Tsudik, 2010). Mobility is the basic component that isolates the present model from foe models. Considerably, the enemy can exchange off discrete biosensors' subsets in discrete time slots. The exchanged off nodes' subset may be gathered or adjoining, that is, at the same time traded off hubs can be spread all over the MSN. While controlling biosensor center, the enemy obtains status of node and key materials information, examines all memory or stockpiling, and may listen the entire communication of the exchanged off node. Two inspirations a portable enemy may demonstrate are there.

- The biosensors are kept in and around the patient. These biosensors may easily be detected and identified by the outsides viz., patient himself or the medical department persons. Thus, the opponent for being not detected will roam in and around the sensor network.
- Detecting the patient movement and following the patient is, thus, very difficult for the adversary. Gradually opponent may lose the control on those biosensor hubs.

Secure System's Requirements: Here, several criteria for MSNs have been presented which are desirable in a light weight and secure system.

Lightweight: Each PAN regularly incorporates sensor nodes with low level architecture, which rely on upon battery charge (Lorincz, 2004; Chaitanya and Venkateswarlu, 2015). Moreover, crisis circumstances inside a MSN require the capacity for quick therapeutic response without debilitating security capacities.

Securely controlling the access to data: Getting the control must be upheld for the PHD in the entire MSN to guarantee that personal data won't be acquired by unapproved clients. More to the point, secured framework ought to give diverse benefits to various system clients.

Scalability: The proposed system has must be able to work in the large networks environment also, where there are good number of PANs with too many number of MSNs and large number of users (Lorincz, 2004).

Flexibility: In MSNs, the get to strategy should absolutely be characterized by both human health services units and by the patients themselves. For example, on-request approval to take in PHD may be furnished with briefly to any one specialist, not contacted regularly every time, a restorative crisis happens. Clearly, powerlessness or inertness in adjusting the get to guidelines may undermine a patient's life (Lorincz, 2004).
Confidentiality: Data confidentiality ought to be safe from node/controller compromise attacks.
Assurance on the integrity of the Data: In MSNs, the data related to patient are highly important. The modified data may lead to dangerous decisions. Hence data integrity is to be protected continuously.
Forward secrecy: Even in the case that an enemy obtains the vital information that is required from the node, decrypting the already encrypted data is not possible.
Backward secrecy: In the case an enemy has taken over the control on a compromised node, it is not possible for the enemy to decrypt the data that it has obtained from the compromised node.

3. PROPOSED SYSTEM

Fundamental concept: Fundamental idea of the system that is proposed by the authors in this paper is described as follows.

After customer's registration process with the server is completed, he's permitted to raise requests for accessing the assembled PHD or monitor those biosensors as demonstrated by his advantage. To accomplish the goal, PSW - Proxy Protected Signature by Warrant is conveyed to the structure (Shao, 2009). This technique is truly an exceptional advanced mark. One can discover two sorts of individuals. The first one gives the proxy one a warrant that indicates personality of the proxy one, the character of the first one. The termination time of allocation of marking force, and so forth. The proxy signer creates proxy marks just with original signature key disseminated by first signer. Authenticators approve intermediary marks just with people in general key of the first underwriter and concentrate on the legitimateness of the warrant.

For applying PSW method in proposed structure, the procedure is described below. The MSN server acts as first signer and MSN user acts as proxy signers. After the registration is completed, server gives few proxy signature keys to the user after he enters MSN. The primary component can in this way be legitimately used to create signature on a summon. Along these lines, affirmed customers make legitimate charges just with intermediary signature keys composed by server. The legitimacy of every request might be affirmed by server through open keys. In this way, server will control unapproved commands. Verification tables need not be stored on a biosensor as the proposed structure requires only lightweight cryptographic operations. Subsequently, the storage and computational need on a biosensor is reduced.

An important quantity of PSW plans have already been described in the previous works. Many of them feel the ill after effects of some security shortcomings, and a sizable portion of these aren't sufficiently efficient for biosensors. After a cautious assessment, it is available that Shao's PSW method (Shao, 2003), is very advantageous for the proposed reason. Irrespective of its efficiency, it's watched that the plan has a design shortcoming. This shortcoming has made the proposed protocol to fail. Subsequently, to confirm that the protocol that is proposed works, an achievable approach has been suggested to be in this kind of shortcoming.

The proposed system has four phases.

- Phase-1: Initialization of the system.
- Phase- 2: Users joining the system.
- Phase-3: Using the system regularly (secure data collected from biosensor node is communicated to network server through the controller).
- Phase-4: Issue of commands by users

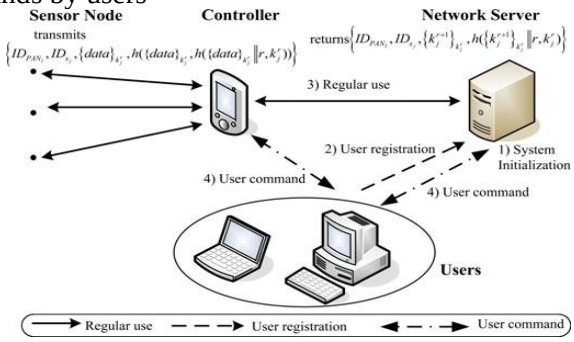

Figure.2. Flows of security information in the proposed system

Structure of the proposed System: The Phase-1: Initialization of the system: The following steps have been executed by the network server during the initialization phase. The notations used throughout are enlisted in Table.1.

- Select any two random prime numerals '*p'* and '*q'* randomly (in such a fashion that $(p-1)/2$ and $(q-1)/2$ are also prime numerals). Now calculate the public modulus defined as $n = p*q$. After that server selects public one - way hash function $h(\ )$ for example SHA-1.
- Select a set of integer numbers '*e'* and '*d'* which satisfies the property $e \cdot d \equiv 1 \pmod{\varphi(n)}$ and let one of the two numbers '*d'* be a very big positive integer number. $\Phi(n) = (p-1)(q-1)$ is Euler's totient function and '*e'* must certainly be larger compared to the output of the $h(\ )$. Thus, on the basis of the RS & A algorithm, the network server will create the private and public keys as $PK_{tns} = \{n, e\}$ and $SK_{tns} = d$.

Table.1. Notations

Notation	Description
U_i	User number i
S_j	Sensor node number j
r	Round index
SK_{tns}	Network server's private key
PK_{tns}	Network server's public key
$(X)_K$	Encrypting message X with a symmetric key K
, or ||	Concatenation operator
ID_A	The identity of an entity A
h(.)	A public one-way collision-resistant hash function
h(X,K)	Keyed hash function with a session key K for message X

- For each PAN, viz., PAN_l, the server securely distributes the unique primary key k_{0j} with each biosensor, say s_j, and stores the value *(IDPANl, IDsj,* $k^o j$). Here ID_{sj} may be the identity of the node s_j while *IDPANl* may be the identity of the PAN *PANl*. The maximum quantity of the bio-sensor nodes in a PAN is altogether are under 40; in this manner, the bit length of IDsj is put to 8. There are two appropriate methods for primary key distribution: trusted server method & key pre-distribution method. Trusted-server method arranges the key in between and every node and system server by relying on a trusted-server. Since MSN contains an infrastructure that is reliable, this method is appropriate in MSN's.

The following way, in which key data was disseminated to every hub just before arrangement, has been generally utilized in bunches of nonexclusive WSNs. Contrasted with WSNs which are nonspecific, this procedure is more attainable for MSNs. Connected with MSN's size that is altogether little more than typical WSN, this plan has less influence over the effectiveness necessities, for example, adaptability. Whichever of these two plans can be utilized, the principal dispersion plan is simply executed in the machine start stage, its little impact on the multifaceted nature of the proposed framework. Additionally, the parameter *PKtns* is stacked to the controller of each PAN in front of the system sending.

Phase- 2: Users joining the system: The user U_i must enroll with the server before issuing a summons to MSN. In the wake of checking his enlistment data, the system server assigns a character, say ID_{Ui}, for him. Expect that along every client character is 2B, in which case the gadget can bolster 65,536 system clients. At that point, the system server finds an intermediary signature key υ_i for client U_i which is given by

$$\upsilon i \equiv [h(mw)]^{-d} \pmod{n}. \qquad (1)$$

Where n = general population modulus characterized before. The license mw record IDU_i, the personality of the system server and an individual benefit like the characters of PANs that client U_i is permitted to get into, and substantial times of assignment.

Watch that condition (1) includes secluded exponentiation with an unfavorable type, which might be done by calculating multiplicative inverse u of h(mw) mod (n) utilizing the augmented Euclidean algorithm.

$$\upsilon i^e h(mw) \equiv 1 \pmod{n}. \qquad (2)$$

Because $\upsilon i \equiv ud \pmod{n}$,

$$u \equiv \upsilon i^e \pmod{n},\ u \equiv h(mw)-1 \pmod{n},\ \upsilon i^e \pmod{n} \equiv h(mw)-1 \pmod{n}.$$

Phase-3: Using system Regularly: After a gadget start stage, the MSN is prepared for customary utilize. For effortlessness, in the following PAN PAN_l is considered for instance. At the determination of individual round r greater than or equal to zero, the whole data that hub s_j communicates to system server via controller is

$$IDPANl, IDsj, \{data\}k^r j, h(\{data\}k^r j \ \|r, krj) \qquad (3)$$

Here data could be the one that is collected by node S*j* during r^{th} round, and {IDP ANl, IDsj} denotes the origin address of the message. From then on, node S*j* generates a secret and exclusive key by $kr+1j = h(krj)$, and promptly erases $k^r j$ from the memory. In wireless networks transmission of data is an expensive operation; transmitting at least one bit over a wireless channel requires at the minimum Thousand (1000) times more power than the usual one 32-bit data calculation (Barr and Asanovi, 2006). For decreasing the transmission overheads, for equation (3), $h(\ )$ is safe hash function with shortened yield. In view of the constraint of the capacity asset on every

controller, the controller must present the gathered information to the system server for all the changeless records. After getting the message, the system server recovers the common key $k^r j$ in accordance with the got data *{IDP ANl,IDsj}*. Along these lines, the system server may utilize the critical key krj to check the realness of the sender, and the freshness and uprightness of the data & get unit information of data. Consequently, system server processes the following key $kr+1j = h(krj)$, and then replaces $k^r j$ of the tuple *IDP ANl, IDsj, krj* with $k^{r+1}j$.

From equation (3), we are able to note that the key used for encrypting PHD for every single transaction is seldom reused. This reduces the severe problem of attacks resulting in key discovery. It leaves the foe, the main genuine choice of beast drive assaults. Since keys are hash values, lexicon assaults don't have any significant bearing. With a satisfactory measure of hash qualities, for example, 160 bits in conjunction with an effective encryption calculation, it will without a doubt be extremely difficult to enemy for spliting keys.

Phase-4: Issue of commands by users: After receiving proxy signature keys, if an individual, *Ui*, who is ready to execute an instruction, has to develop the instruction *Que* and after that it imprints a trademark sign on the *Que* as explained below:

- Identify an integer number randomly 'z' such that $z \in [1, n]$ & then calculate $\beta = ze$ (modulo (n)).
- Then calculate $\delta = h(Que\_\beta)$ and $y = z \times vi\delta \pmod{n}$.
- *Ui* communicates *{Que, mw, y, δ}* to the server.

After acquiring signature message *{Que, mw, y, δ}*, the controller checks it and executes the subsequent equations.

Verify if the timestamp Ti utilized in Que is inside some admissible range contrasted and prevailing time. If the effect can result in undesirable, then the signed message may be excluded. Else, server pays consideration around authenticity with warrant m_w as well as the charge Que. As an illustration, much like the substantial times during the designation field. Server can verify if the main advantage of the customer has lapsed. One more case is usually that the server verifies if or not the charge Que is in and around the extent of customer benefit, because of the concise explanation of warrant m_w. Just when they are valid, the check method goes toward the subsequent stride.

Compute $\beta^* = y^e h(mw)^\delta \pmod{n}$. Verify if $h(Que || \beta^*) = \delta$.

Since $vei = h(mw) - 1 \pmod{n}$; $\beta^* = z^e v^{\delta e_i} h(mw)^\delta = z^e = \beta$ (modulo (n))

In the event that all confirmation methods depicted already pass, the server trusts the charge Que, warrant m_w which are obtained from an approved client having vital benefits. A client may associate by means of server, specifically for simplicity of observing patient. Charges given from client may actuate the biosensors implanted on patient or modify their testing recurrence. These charges can be sent by system server towards determined bio sensor. Then again, if system client communicates a get to order, the network server gives back the subsequent PHD to client. For the purpose of security, client may build up a session key using server by some key exchange techniques and utilize this session key for guaranteeing secrecy, uprightness, and brilliance of PH data communication.

4. CONCLUSION

Several security challenges faced by sensor networks used in the pharmaceutical field and in Medical diagnosis field have been identified in this paper. These challenges have been identified while monitoring the health conditions of a patient remotely and/or wirelessly. A lightweight and innovative system for transmitting the patient data securely and for controlling the pharmaceutical system in MSNs has been proposed by the authors in the present paper. Usage of tiny and wearable bio sensors on the patient body for collecting the vital and important patient information remotely has also been discussed in this paper.

REFERENCES

Barr K.C and Asanovi K, Energy aware lossless data compression, ACM Trans. Comput. Syst, 24 (3), 2006, 250–291.

Chaitanya K and Venkateswarlu S, Detection of black and Grey Attacks in MANETs based on ACK based Approach, Journal of Theoretical and Applied Information Technology (JATIT), 2015.

Choi J, Ahmed B, Gutierrez-Osuna R, Development and evaluation of an ambulatory stress monitor based on wearable sensors, IEEE Trans. Inf. Technol. Biomed, 16 (2), 2012, 279–286.

Daojing He, Sammy Chan, Shaohua Tang, A Novel and Lightweight System to Secure Wireless Medical Sensor Networks, IEEE journal of biomedical and health informatics, 18 (1), 2014, 316-326.

He D, Bu J, Zhu S, Chan S, and Chen C, Distributed access control with privacy support in wireless sensor networks, IEEE Trans. Wireless Commun, 10 (10), 2011, 3472–3481.

He W, Huang Y, Sathyam R, Nahrstedt K, and Lee W, SMOCK, A scalable method of cryptographic key management for mission-critical wireless ad-hoc networks, IEEE Trans. Inf. Forensics Security, 4 (1), 2009, 140–150.

Keoh S, Efficient group key management and authentication for body sensor networks, in Proc. IEEE Int. Conf. Commun, 2011, 1–6.

Kumar P and Lee H.J, Security issues in healthcare applications using wireless medical sensor networks, A survey, sensor, 12, 2012, 55–91.

Le X, Khalid M, Sankar R, and Lee S, An efficient mutual authentication and access control scheme for wireless sensor network in healthcare, J. Networks, 6 (3), 2011, 355–364.

Lorincz K, Malan D, Fulford-Jones T, Nawoj A, Clavel A, Shnayder V, Mainland G, Moulton S, and Welsh M, Sensor networks for emergency response, Challenges and opportunities, IEEE Pervas. Comput, 3 (4), 2004, 16–23.

Ma D and Tsudik G, Security and privacy in emerging wireless networks, IEEE Wireless Commun, 17 (5), 2010, 12–21.

Malasri K and Wang L, Addressing security in medical sensor networks, in Proc, ACM Health Net, 2007, 7–12.

Malasri K and Wang L, Design and implementation of a secure wireless mote-based medical sensor network, Sensors, 9 (8), 2009, 6273–6297.

Rajasekaran R, Manjula V, Kishore V and Sridhar T, Jayakumar C, An efficient and secure key agreement scheme using physiological signals in body area networks, in Proc. Int. Conf. Advances Comput. Commun. Informat, 2012, 1143–1147.

Shao Z, Provably secure proxy-protected signature schemes based on RSA, Comput, Electr, Eng, 35 (3), 2009, 497-505.

Shao Z, Proxy signature schemes based on factoring, Inf. Process. Lett, 85 (3), 2003, 137–143.

Tan C.C, Wang H, Zhong S, and Li Q, IBE-lite, A lightweight identity based cryptography for body sensor networks, IEEE Trans. Inf. Technol. Biomed, 13 (6), 2009, 926–932.

Wang H, Fang H, Xing L, and Chen M, An integrated biometric based security framework using wavelet-domain HMM in wireless body area networks (WBAN), in Proc. IEEE Int. Conf. Commun, 2011, 1–5.

Zhao S, Aggarwal A, Frost R, and Bai X, A survey of applications of identity-based cryptography in mobile Ad-hoc networks, IEEE Commun. Surveys Tutorials, 14 (2), 2012, 380–400.