Efficient Key Agreement and Nodes Authentication Scheme for Body Sensor Networks

Jawaid Iqbal
Department of Information Technology
Hazara University
Mansehra, Pakistan

Arif Iqbal Umar
Department of Information Technology
Hazara University
Mansehra, Pakistan

Noor ul Amin
Department of Information Technology
Hazara University
Mansehra, Pakistan

Nizamud Din
Department of Computer Science
IQRA National University
Peshawar, Pakistan

***Abstract*—Technological evolvement of Wireless Sensor Networks (WSNs) gave birth to an attractive research area for health monitoring called Body Sensor Network (BSN). In BSN tiny sensor nodes sense physiological data of patients under medical health care and transmit this data to Base Station (BS) and then forward to Medical Server (MS). BSN is exposed to security threats due to vulnerable wireless channel. Protection of human physiological data against adversaries is a major addressable issue while keeping constrained resources of BSN under consideration. Our proposed scheme consists of three stages. In first stage deployment of initial secret key by the ward Medical Officer (MO), in second stage secure key exchange and node authentication, in third stage secure data communication are performed. We have compared our proposed scheme with three existing schemes. Our scheme is efficient in computation cost, communication overhead and storage as compared to existing schemes while providing enough security against the adversaries.**

Keywords—Body sensor network; hash function; node authentication; key agreement; session key

I. Introduction

The WSN applications in various fields like natural disasters, habitat monitoring, battle field, and other emergency services got the attention of the researchers [1], and WSN evolved to BSN for medical applications. In 1996 T.G. Zimmerman proposed the idea of Wireless Body Sensor Networks (WBSNs) for the first time. These networks were initially called Wireless Personal Area Network (WPANs). A typical sensor node's hardware consist on processor and memory, wireless communication stack, analog to digital converter and sensing [2]. BSN network comprised of low power, low processing, small size, light weight body sensors deployed on patient body which constantly monitor Electroencephalogram (EEG), respiratory rate, heart rate, Blood Pressure (BP) through by sensing then forward the real time sensed patient data to BS outside the body for onward transmitting to MS. After receiving patient data by MS, the ward physician gives feedback for the patient health care [3].The bandwidth for transmission in BSN is 10Kbps to 10Mbps [2]. BSN being challenging area of research have a number of research directions such as its security, energy, memory and data management. We accept the challenge of secure and authentic transmission of patient physiological data to the legal user (MO) of the network while keeping adversary attacks and overall efficiency of BSN. For secure communication between communicating parties it is essential to confidentially share secret keys. Our proposed scheme addresses the efficient key management and authentication to encounter the possible attacks on the system and reduce the human life risk. The three stages scheme is proposed where in first stage the ward MO deploy initial master secret keys M_{sk} in BSN equipments and stores the IDs of all sensor nodes in BS for further establishing secure link, in second stage legal nodes are authenticated and secure keys are established for the transmission of the next stage data, in third stage secure transmission of physiological data is performed. We compare the efficiency of our scheme with existing schemes and obtained results show that our proposed scheme is efficient in communication overhead, computation cost and storage requirement while provide protection against the attackers.

The rest of the paper is organized in sections. In Section II "Related Work" the background and related security schemes are critically discussed. In Section III "Network Model", Section IV "Radio Model", Section V "Attack Model", Section VI "Proposed Protocol", Section VII "Security Analysis", Section VIII "Performance Analysis" and Section IX "Conclusion" are elaborated.

II. Related Work

In scheme [4], [5] the proposed protocols sensor association and key management have considered while in [4] public key based authentication is used for the secure association of sensor nodes with the controller, however sensor with patient authentication is not considered that leads to security lapse and an illegal node may join the network and pick the patient data. Association between sensor nodes and controller is tedious and high in computation cost. In [5] group keys establishment and authentication is performed by group device pairing where for obtaining group keys each sensor has

to perform n + 3 times Modular Exponentiations (M-Exp) operations and n represents total of sensors in BSN which over burden the short resources sensor nodes and the communication overhead and computation cost of this scheme is quite high. In scheme [6], node to node authentication and key agreement is performed and Diffie-Hellman (DH) protocol is initially applied for the establishment of the secret key which is vulnerable to man in the middle attack. In this scheme, membership broad casting to all sensor nodes leads to high communication and memory overhead. The problem with [7] is that each received packet on each node is decrypted and hash function is applied which clearly increase computational cost and can't suitable for BSN environment. Scheme [1] is suitable for WSN but bulky for BSN as RSA public cryptosystem is used. In scheme [8], a hybrid approach is used where RSA is used for key agreement and symmetric cipher for session data transmission. As RSA is a public cryptosystem using 1024 bit key which is infeasible for the resource constrained sensor nodes and has high computation cost similarly it lacks node authentication. In [9] ECC is used for Key agreement instead of RSA which somehow reduced computation cost and memory requirement as ECC use 160 bits key but still costly due to hybrid (asymmetric and symmetric) approach and no mechanism for node authentication. Scheme [10] uses biometric technique for key agreement using electrocardiogram. The generated session key is used for secure transmission of patient data between sensors and base station. The keys generated through electrocardiogram are long and random. Identical ECG signals generate non linkable keys. Although this scheme provides security but obtaining two signals from accurate similar random biological signals is hard [11]. In scheme [12] asymmetric cryptosystem is used for key establishment and rekeying by utilizing DHECC and RSA. Specific routing algorithm is used for efficiency purposes. However, this scheme has unavoidable problems of high computation cost and storage requirement due to PKC, RSA and DHECC and inconvenient for tiny sensor nodes of BSN. Scheme [13] uses smart card and password based user authentication for patients' health care with two stages of registration and login and authentication. Before to access BSN each user has to be registered with the gateway first and then the gateway issue smart card to the system user which is used for accessing patient data. Smart card contains login information to network. After authentication a session for information communication is generated between communicating parties. This technique suffers from security flaws. In scheme [14] a preloaded secret key is shared amongst all node of the network. Then another secret session key for a specific session is generated by the cryptographic protocol. This scheme can be used for a large dynamic nature network. In proposed scheme [15] asymmetric mechanism is applied for sharing secret key amongst nodes. Then that key is used for the session data transmission securely using symmetric cryptosystem. This seems to be hybrid scheme where public key infrastructure is used for key establishment and symmetric for secure communication. This scheme is expensive in computational cost while using asymmetric technique for key establishment. Scheme [16] introduced a WBANs security suite; IAMKeys technique for WBAN key management and KEMESIS for inter-sensors transmission, random keys generation and ensuring security by eliminating exchange of keys between body sensors. Inter sensor communication over burden network overhead. To avoid inter sensors communication over all network overhead can be reduced. In scheme [17] AES based encryption which is supported by CC2420 where all nodes involved in communication receive share secret key through by a specific server. MAC, CCM and CBC are used for encryption and authentication. This is a platform dependency scheme. In scheme [18] generation of 128 bits key is performed using IPI and time difference is calculated by the peaks of the ECG/PPG. Hamming distance error correction scheme is used. The limitation of the scheme is that by a minute difference in calculating IPI at sensor error correction code should be applied for balancing keys. Calculating of IPI values require enough time which slows down the BSN. In scheme [19] SCK and ECC is used for authentication using pair of keys. Sensor nodes are loaded with confidential data through KDC for this identity of each sensor. Various parameters of EEC are used for association of every patient in BSN. Association patients and sensors is very difficult so the scheme is impractical for large hospitals with hundreds of patients. In scheme [20] pair of keys is established using ECC amongst sensors and BS. Patients of BSN are authenticated using biometric device attached to every sensor node. Attachment of biometric device leads to more energy consumption and memory requirement of the sensor. In scheme [21], a three tier architecture is presented for health care application i.e. patients authentication through by biometric, ECC for key agreement and symmetric encryption for confidential session data transmission with integrity. Each sensor is connected with a small scanner for finger print for ID of patients. This is a secure scheme but expensive with respect to computation cost and energy overhead.

III. Network Model

The network model comprises of low power sensors, base station and medical server. Low power biosensor nodes are deployed on patient body for sensing vital signs data. This data is forwarded to a device called BS or Access Point (AP) which acts as a controller. All BSN sensors access the base station directly to avoid inter sensor communication and reduce the BSN traffic. Base station is resourceful equipment with no limits of storage, processing and energy. BS forward health status received from sensing sensors to medical server. MS stores health status record which is received by the ward physician for speedy treatment. For interoperability Zigbee/802.15.6 standards are preferred to be used and all nodes are accessible at maximum up to two hopes. Fig. 1 represents the architecture of BSNs.

Fig. 1. BSNs architecture for patients in a ward of medical centre.

IV. RADIO MODEL

We would prefer to use first order radio model for the estimation of energy consumption by transmitting patient data wirelessly in BSN. The basic parameters of the model are $\boldsymbol{E_t}$ for energy transmission, $\boldsymbol{l}$ packet length and $\boldsymbol{d}$ transmission distance**.** Equation (1) for data transmission [22]:

$$\mathbf{E_t}(\boldsymbol{l},\boldsymbol{d}) = \begin{cases} \boldsymbol{l}\mathbf{E_{elec}} + \boldsymbol{l}\,\boldsymbol{\varepsilon_{fs}}\ \boldsymbol{d}^2, \boldsymbol{d} < \boldsymbol{d_0} \\ \boldsymbol{l}\mathbf{E_{elec}} + \boldsymbol{l}\,\boldsymbol{\varepsilon_{mp}}\ \boldsymbol{d}^4, \boldsymbol{d} \geq \boldsymbol{d_0} \end{cases} \quad (1)$$

Where $\mathbf{E_t}(\boldsymbol{l},\boldsymbol{d})$ is the ratio of consumed power by a sensor node in data transmission, power consumed is directly proportional to the packet length $\boldsymbol{l}$ and $\boldsymbol{d}^2$ distance. Power consumption depends upon the communication distance, long distance more energy consumption and short distance less energy consumption.

$$\mathbf{E_r}(\boldsymbol{l}) = \boldsymbol{l}\mathbf{E_{elec}} \quad (2)$$

Equation (2) is used to measure the consumed energy on patient data receiving where $\mathbf{E_r}(\boldsymbol{l})$ Energy required for receiving data by a sensor node, $\boldsymbol{l}$ is packet length and $\mathbf{E_{elec}}$ Energy consumption per bit as:

$$\boldsymbol{E_{elec}} = 50nJ/bit$$
$$\boldsymbol{d_0} = 100\text{m}$$

The distance in our scheme $\boldsymbol{d} < \boldsymbol{d_0}$ so we use free space model $\boldsymbol{\varepsilon} = \boldsymbol{\varepsilon_{fs}}$ =10 pJ/bit/m^2 . $_{\mathbf{fs}}$ is the free space model amplifier energy factor.

V. ATTACK MODEL

It is assumed that the BSN equipment are in reach of the attacker and may launch attacks like replay, eavesdropping, masquerading etc. BSN communicate patient physiological data which are the top personal secrets of the patient and should be protected from illegal use to safe the human life risk. For this purpose a cost effective and secure technique should be developed to tackle these issues. Preloading of initial secrets keys by the ward physician has to be done securely. Legal and illegal nodes should be differentiated through nodes authentication to protect the network from unauthorized access of patents personal diseases information and avoid masquerading attack. Secure exchange of secret keys for the session data communication is the requirement of our proposed scheme. As asymmetric cryptosystem is costly so we would prefer to use symmetric cryptosystem for the confidential communication of the patient data and avoid eavesdropping, chosen cipher and plain text attacks.

VI. PROPOSED SCHEME

Our proposed scheme comprised on three stages, deployment stage, node authentication stage and secure data communication stage. The notations used throughout this paper are listed in Table 1.

A. Deployment Stage

Deployment stage is the first stage in which initially required information are loaded to BSN devices. The corresponding ward MO generates a master secret key M_{sk} and deploys that key on MS, BS and sensor nodes.

TABLE I. NOTATION GUIDE

Symbols	Description
P_i	Patient in ward
s_i	Sensor node
PRNG	Pseudo Random Number Generator
R	random number
S_K	Session key
nonce	Number used once
ID	Identification number of sensor
DES	Data encryption standard
M_k	Master secret key
h / hi'	One-way hash function
C_i	Cipher text
E_k/D_k	Encryption / Decryption with key k

Unique IDs of the sensor nodes having M_{sk} are stored in BS and all relevant sensor nodes are deployed on patient body for monitoring health status of patients.

B. Node Authentication Stage

Node authentication is important in a situation where two or more biosensor nodes want to authenticate each other's identity or BS want to authenticate the identity of a legal node in a data communication networks. In this stage, biosensor nodes S_i send encrypted data to BS for authentication. BS decrypts the received data and authenticates biosensor nodes S_i . If authentication granted node will start secure communication using session key otherwise node is black listed and isolated from the network.

ALGORITHM.1. Key Agreement and Authentication

1. *Preload Patient Master secret key $\mathcal{M}_{SK}$ on BS and Biosensor*
2. *Biosensor*
   a. Generate random number (*R*) called pre session key S_K
   b. *Generate* nonce
   c. *Computes* $C = \mathcal{E}_{\mathcal{M}_{SK}}(Nonce \parallel s_k \parallel ID)$
   d. *Sends* C *to BS*
3. *Base Station*
   a. *Computes*$(Nonce \parallel s_k \parallel ID) = \mathcal{D}_{\mathcal{M}_{SK}}(C)$
   b. *If* $ID = pre\ store\ ID\ so$ Grant Authentication
      Else
   c. Blacklist the biosensor
   d. If Grant Authentication
   e. *Computes* $C = \mathcal{E}_{\mathcal{M}_{SK}}(S_K)$
   f. *Sends* C *to MS and MO*
4. *Medical Server and Medical Officer*
   a. *Computes* $S_K = \mathcal{D}_{\mathcal{M}_{SK}}(C)$
5. *Base Station*
   a. $C = E_{SK}(Nonce + 1)$
   b. *Sends* C *to Biosensor*
6. *Biosensor*
   a. $(Nonce + 1) = \mathcal{D}_{SK}(C)$

End

Authentication is required to ensure that only authorized nodes can join the network. Each sensor node has a default Pseudo Random Number Generator (PRNG) which generates a random number R called session key S_K and then generate $nonce$. Sensor node concatenate $nonce$, session key S_K, its own unique ID and encrypt on pre loaded master secret key M_{sk} then transmit to BS. At other end BS decrypt the received information by master secret key M_{sk} compare the received sensor node ID with its pre stored ID if matched, node is legal and authentication is granted and otherwise the node is from intruder and black listed. After a node is authenticated BS increment the received $nonce$ by 1 then encrypt it using session key S_K and sends to corresponding sensor node which decrypt the received message by its own S_K. Moreover, BS encrypts the session keys of authenticated nodes using M_{sk} and forward to MS and MO for onward secure communication. The overall scenario of proposed scheme is presented in Fig. 2.

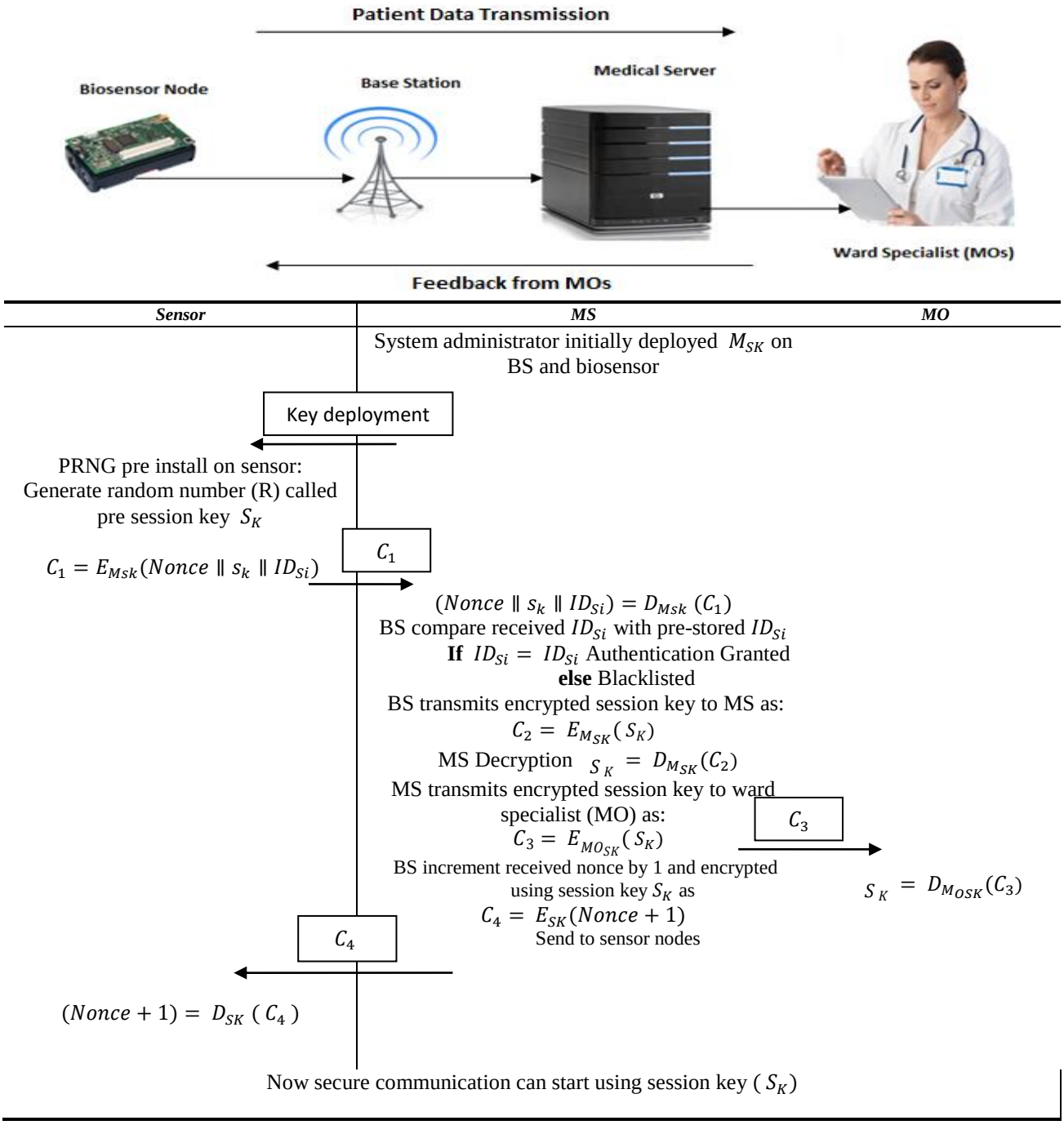

Fig. 2. Over all scenarios of proposed scheme.

C. Secure Data Communication Stage

Secure communication of the sensed physiological data of vital signs is performed inside the ward of a hospital so the range of BSN in our proposed scheme is limited to a ward. Sensor nodes deployed on patients are directly connected with BS and the sensed patient data is forwarded to MS for quick response of the physician. Each node has its own Session key S_K and all these keys are also stored on BS and MS as in stage 2 which are further used for secure communication as when a message patient vital signs data packet is required to be sent to MO by a sensor node. This data packet will be encrypted by the session key S_K of that node and will be transmitted to medical server through BS. Similarly the integrity of patient data is gained by hash collision resistive Message Digest (MD5) as hash of patient data h(patient data) is taken and hash value h_i is obtained then to obtain secure C_i, patient data and h_i is encrypted by session key S_K and C_i is transmitted to MS through BS. Now MS decrypt the received C_i by S_K , h_i and patient data is obtained if hi'(hash taken of received patient data by MS) is compared with h_i if found same then the received message is original and not changed otherwise changed by the attacker.

ALGORITHM.2. *Secure Data Communication*

A. Sensor Node

I. For each sensor node $s_i \in P_i$

{

a. $h_i = h(Patient\ data)$

b. Computes $c_i = \mathrm{E}_{sk}(\{Patient\ data\}, h_i)$

c. Sends c_i to MS through BS

}

II. End for

D. Medical Server

I. For each biosensor node $s_i \in P_i$

{

d. $(\{Patient\ data\}, h_i) = \mathrm{D}_{sk}\ (c_i)$

e. $h_i = h(Patient\ data)$

f. Computes $h_i' = h(Patient\ data)$

g. Accept if $h_i' = h_i$ hold

h. otherwise reject

}

End for

Security is depending upon two major parts. One as data security and the second is data privacy. In data security we study how data can be securely transmitted and stored and the second part only authorized users can access the patient personal information. In below Fig. 3 is represented the flow chart of secure data communication.

VII. Security Analysis

The analysis to validate security features of our proposed scheme is represented here. Our proposed scheme provides the essentials security requirements of authentication, confidentiality and integrity.

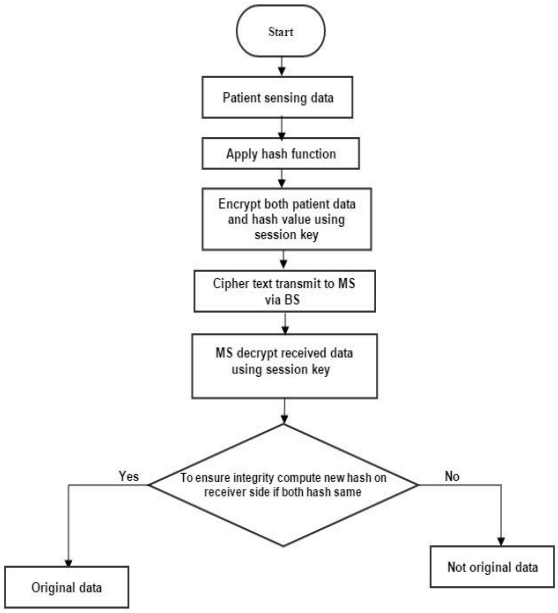

Fig. 3. Flow chart for secure data transmission.

A. Node Authentication

Upon receiving the request from a node for becoming the part of the network BS compare the ID of that sensor node with its pre installed IDs, if both of the IDs i.e. the received ID and the pre-stored ID are matched then that sensor node is authenticated otherwise rejected and thrown out from network by black listing that ID.

B. Data Confidentiality

In our proposed scheme, Master secret key is used for confidentially and sharing the session key (s_k). Session key is used to make sure vital signs data transmission of patients between sensor nodes with base station and medical server. Confidentiality of patient is maintained through DES cipher which encrypt the sensed session data before to be communicated to the BS and MS so that to protect this personal data from the illegal reading .MS forward it to MO for quick health care.

C. Patient Data Integrity

Data integrity is that feature of our scheme which obstructs the alteration of the patient precious personal data from illegal use for any bad intention. Integrity in our scheme is achieved using hash collision resistive Message Digest (MD5) in such a way that the received hash h_i is compared with computed hash (hi') is similar then data is safe and not changed otherwise incorrect data is received.

D. Scalability

Scalability is the property of our proposed scheme as whenever a sensor node is required to be added to the network or a sensor is to be removed from the network or a sensor is needed to be changed due to low battery power or any other fault by any of these activities the normal functionality of the network is not affected.

VIII. Performance Analysis

Performance analysis of our proposed scheme and two existing schemes with respect to computational cost, communication overhead, storage and energy consumption in term of efficiency is given below.

A. Computational cost

No expensive and major operations like ECPM and M-Exp are involved in our proposed scheme. In designed scheme [12], four ECPM and two M-Exp operations and in scheme [8] two M-Exp are used. Graph in Fig. 4 shows that our scheme is 90.99 % efficient in computation cost as compare to [12], 89.67 % as compare to [8] and 69.98 % as compare to [23]. In our scheme we implement the experiment done in [24] on MICA2 sensor that is operational with low power ATmega128 8-bit micro-controller at 7.3728 MHz, 128 KB nonvolatile memory (ROM) and 4 KB volatile memory (RAM). One major operation ECPM uses 0.81s using 160 bits elliptic curve [25] and RSA 1024 bits M-Exp takes 22 seconds [26]. DES encryption and decryption execution time [27] is same which 4.543859 seconds. We calculate the computation cost of our scheme in comparison with the [8], [12] on the basis of the results of [23], [24], [26]-[28].

According to scheme [28] the 3rd generation MICA2 needs 2.66s for pairing computation. The computational time of our proposed scheme is negligible as compared with others existing schemes [8], [12] because we used symmetric algorithm for encryption and decryption as well as our scheme is more suitable for resource constraint environment of BSN. One ECPM operation consumes 19.1Mj and one pairing computation operation consumes 62.73mJ energy [24], [28]. Our scheme have no major operation so energy consumption as compared to others existing schemes is negligible.

TABLE II. Associated Parameter and Data Size Involved in Data Communication

Associated Parameters	Data Size
RSA Key	1024 bits
ECC Key	160 bits
DES Session Key	64 bits
Master Secret Key	128 bits
Sensor ID	48 bits
nonce	16 bits

Comparison of Computation Cost of existing and proposed

1) Computation cost of our proposed scheme is compared with scheme [8] as:

Computation cost efficiency:

$$\frac{(2*22)s-(4.543859)\,s}{(2*22)s}\% = 89.67\ \%$$

2) Computation cost of our proposed scheme is compared with scheme [12] as:

Computation cost efficiency:

$$\frac{(2*22+4*1.61)s-(4.543859)\,s}{(2*22+4*1.61)s}\% = 90.99\ \%$$

3) Computation cost of our proposed scheme is compared with scheme [23] as:

Computation cost efficiency:

$$\frac{(2*30.67+1(14.62))s-(4.543859)\,s}{(2*30.67+1(14.62))s}\% = 69.98\ \%$$

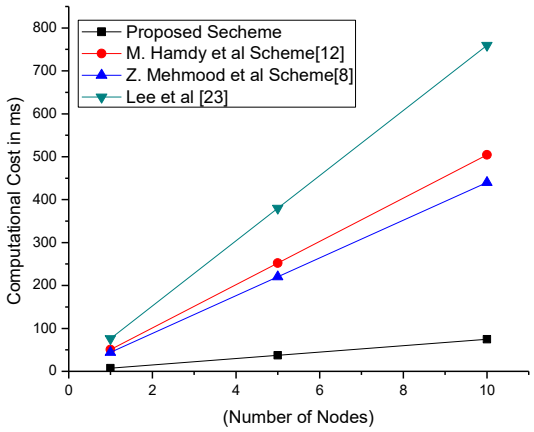

Fig. 4. Computational cost comparison.

B. Communication Overhead

The proposed scheme communication overhead as compared with other existing schemes [8], [12], [23] and the computed values are shown in Tables 3, 4 and 5 and then design graph according to these computed values which are shown in Fig. 5.

Communication overhead of our proposed scheme with schemes [8], [12], [23] is represented in Fig. 5 where our scheme shows 84.2% as compared to scheme [8], 85.7% efficiency than scheme [12] and 78.57% than [23].

TABLE III. Communication Overhead Comparison with Z. Mehmood Et Al.

Scheme	Communication Overhead	Communication Overhead Reduction in Percent
Z. Mehmood et al. [8]	(1024+192)bits	$\frac{1216-192}{1216}\%$ = 84.2 %
Proposed	(128+16+48) bits	

TABLE IV. Communication Overhead Comparison with M. Hamdy Et Al.

Scheme	Communication Overhead	Communication Overhead Reduction in Percent
M. Hamdy et al. [12]	(1024+320)bits	$\frac{1344-192}{1344}\%$ = 85.7 %
Proposed	(128+16+48) bits	

TABLE V. Communication Overhead Comparison with Lee Et Al.

Scheme	Communication Overhead	Communication Overhead Reduction in Percent
Lee et al. [23]	2(160+160+128)bits	$\frac{896-192}{896}\%$ = 78.57 %
Proposed	(128+16+48) bits	

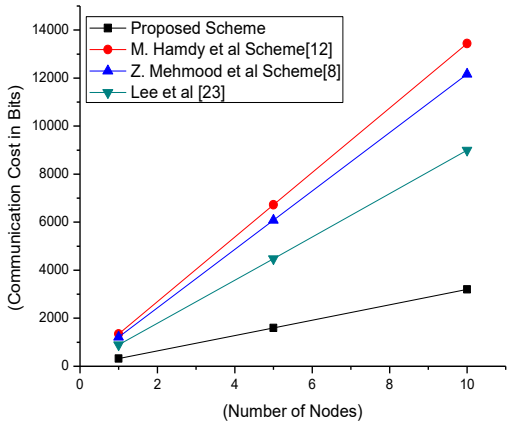

Fig. 5. Communication overhead comparison.

C. Memory Requirement for Key Storage

The proposed scheme memory for key storage as compared with other existing schemes [8], [12], [23] and the computed values are shown in Tables 6, 7 and 8 and then design graph according to these computed values which is shown in Fig. 6.

The NIST standard key size for algorithms AES, DES, RSA, ECC is given in Table 2. Fig. 6 represent analysis of memory requirement our proposed scheme with schemes [8], [12], [23]. Our proposed scheme reduces 75% as compare to scheme [8], 80% memory requirements as compare to scheme [12] and 28.57 than [23].

TABLE VI. STORAGE COMPARISON OF PROPOSED SCHEME AND Z. MEHMOOD ET AL.

Schemes	Key stored	Approximate key size in bits	Percent reduction in memory storage
Z. Mehmood et al. [8]	k_{pi}, k_{Cj}, e_{gw}	128+128 +1024	$\frac{1280-320}{1280}$% = 75%
Proposed	M_{sk}, $S_{k,}$ ID, *nonce*	128+128+48+16	

TABLE VII. STORAGE COMPARISON OF PROPOSED SCHEME AND M. HAMDY ET AL.

Schemes	Key stored	Approximate key size in bits	Percent reduction in memory storage
M. Hamdy et al. [12]	d_{si}, p_{si}, e, k_{pi}, k_{Cj},	160+160+ 1024+128+ 128	$\frac{1600-320}{1600}$% = 80%
Proposed	M_{sk},s_k, ID, *nonce*	128+128+48+16	

TABLE VIII. STORAGE COMPARISON OF PROPOSED SCHEME AND LEE ET AL

Schemes	Key stored	Approximate key size in bits	Percent reduction in memory storage
Lee et al. [23]	k_{pi}, k_{Cj}, e_{gw}	160+160+128	$\frac{448-320}{448}$% = 28.57%
Proposed	M_{sk}, $S_{k,}$ ID, *nonce*	128+128+48+16	

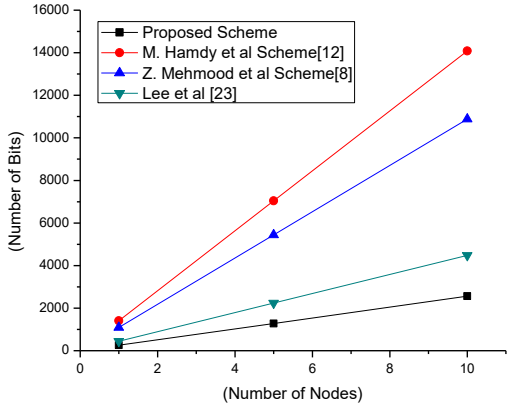

Fig. 6. Memory requirement for key storage.

D. Key Agreement and Authentication Delay

The delay in authentication and key agreement of the proposed scheme in comparison with existing schemes [8], [12], [23] is shown in graph Fig. 7 where the delay of our proposed scheme is very less and negligible.

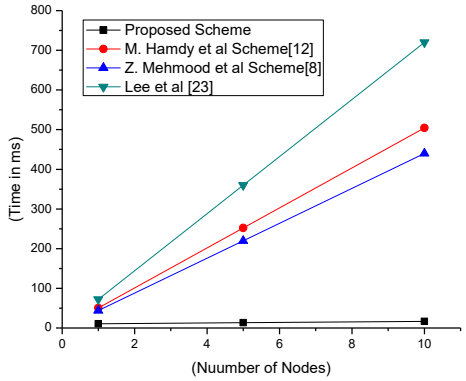

Fig. 7. Key agreement and authentication delay.

E. Energy Consumption for Authentication and key Agreement

The communication distance of our proposed scheme is less than 100 meters as per the standard size of the ward as the distance in our scheme $\mathbf{d} < \boldsymbol{d_0}$ so we use free space model

$\varepsilon = \varepsilon_{fs}$ =10 pJ/bit/m^2 where ε_{fs} is the amplifier energy factor of the free space model. Graph in Fig. 8 shows that our scheme is quite better than the existing schemes [8], [12], [23].

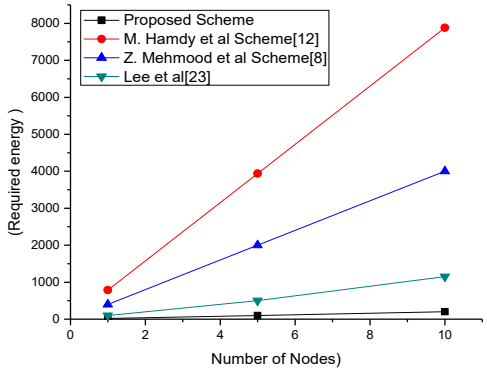

Fig. 8. Energy consumption for authentication and key agreement.

IX. Conclusion

In this paper, an efficient key agreement and nodes authentication scheme is presented which is compared with other solutions to prove the efficiency of our proposed scheme. Our proposed three stages solution not only protects patient data from unauthorized elements but also overcome the weaknesses of the existing schemes and thus proves its suitability for the resource constrained environment of BSNs. The comparison of the existing three schemes and our scheme has shown that our scheme leads in efficiency as 90.99% in computation cost as compared to M. Hamdy et al., 89.67% as compare to Z. Mehmood et al. and 69.98% as compared to Lee et al. 85.7% in communication overhead than M. Hamdy et al., 84.2% than Z. Mehmood et al. and 78.57% than Lee et al. in storage, 80% than M. Hamdy et al., 75% than Z. Mehmood et al. and 28.57% than Lee et al.

References

[1]. Sahana and I. S. Misra, “Implementation of RSA security protocol for sensor network security: Design and network lifetime analysis,” 2011 2nd Int. Conf. Wirel. Commun. Veh. Technol. Inf. Theory Aerosp. Electron. Syst. Technol. (Wireless VITAE), pp. 1–5, 2011.

[2]. K. S. K. Jingwei Liu, “Hybrid security mechanisms for wireless body area networks,” 2010 Second Int. Conf. Ubiquitous Futur. Networks, pp. 98–103, 2010.

[3]. P. M. Khan, A. Husain and K. S. Kwak, “Medical Applications of Wireless Body Area Networks,” Int. J. Digit. Content Technol. its Appl., vol. 3, no. 3, pp. 185–193, 2009.

[4]. S. L. Keoh, E. Lupu, and M. Sloman, “Securing body sensor networks: Sensor association and key management,” 7th Annu. IEEE Int. Conf. Pervasive Comput. Commun. PerCom 2009, 2009.

[5]. M. Li, S. Yu, W. Lou, and K. Ren, “Group device pairing based secure sensor association and key management for body area networks,” Proc. - IEEE INFOCOM, pp. 1–9, 2010.

[6]. S. L. Keoh, “Efficient Group Key Management and Authentication for Body Sensor Networks,” 2011 IEEE Int. Conf. Commun., pp. 1–6, 2011.

[7]. D. He, S. Chan, Y. Zhang, and H. Yang, “Lightweight and confidential data discovery and dissemination for wireless body area networks,” IEEE J. Biomed. Heal. Informatics, vol. 18, no. 2, pp. 440–448, 2014.

[8]. Z. Mehmood, Nizamuddin, S. Ashraf Ch., W. Nasar, and A. Ghani, “An efficient key agreement with rekeying for secured body sensor networks,” 2012 2nd Int. Conf. Digit. Inf. Process. Commun. ICDIPC 2012, pp. 164–167, 2012.

[9]. N. U. Amin, M. Asad, and S. A. Chaudhry, “An authenticated key agreement with rekeying for secured body sensor networks based on hybrid cryptosystem,” Proc. 2012 9th IEEE Int. Conf. Networking, Sens. Control, pp. 118–121, 2012.

[10]. G. Wu, L. Yao, B. Liu, K. Yao, and J. Wang, “A biometric key establishment protocol for body area networks,” Int. J. Distrib. Sens. Networks, vol. 2011, 2011.

[11]. X. H. Le, M. Khalid, R. Sankar, and S. Lee, “An Efficient Mutual Authentication and Access Control Scheme for Wireless Sensor Networks in Healthcare,” J. Networks, vol. 6, no. 3, pp. 355–364, 2011.

[12]. M. H. Eldefrawy, M. K. Khan, and K. Alghathbar, “A key agreement algorithm with rekeying for wireless sensor networks using public key cryptography,” Anti-Counterfeiting Secur. Identif. Commun. (ASID), 2010 Int. Conf., pp. 1–6, 2010.

[13]. P. Kumar, S. G. Lee, and H. J. Lee, “A user authentication for healthcare application using wireless medical sensor networks,” Proc.- 2011 IEEE Int. Conf. HPCC 2011 - 2011 IEEE Int. Work. FTDCS 2011 -Workshops 2011 Int. Conf. UIC 2011- Work. 2011 Int. Conf. ATC 2011, vol. 1, pp. 647–652, 2011.

[14]. D. Liu, P. Ning, and R. Li, “Establishing pairwise keys in distributed sensor networks,” ACM Trans. Inf. Syst. Secur., vol. 8, no. 1, pp. 41–77, 2005.

[15]. A. Boukerche and Y. Ren, “The design of a secure key management system for mobile ad hoc networks,” 2008 33rd IEEE Conf. Local Comput. Networks, pp. 320–327, 2008.

[16]. R. Sampangi, S. Dey, S. Urs, and S. Sampalli, “a Security Suite for Wireless Body Area Networks,” Int. J. Netw. Secur. Its Appl., vol. 4, no. 1, pp. 97–116, 2012.

[17]. M. Meingast, T. Roosta, and S. Sastry, “Security and privacy issues with health care information technology.,” Conf. Proc. IEEE Eng. Med. Biol. Soc., vol. 1, pp. 5453–5458, 2006.

[18]. C. C. Y. Poon, Y. T. Zhang, and S. Di Bao, “A novel biometrics method to secure wireless body area sensor networks for telemedicine and M-health,” IEEE Commun. Mag., vol. 44, no. April, pp. 73–81, 2006.

[19]. C. Jiang, B. Li, and H. Xu, “An Efficient Scheme for User Authentication in Wireless Sensor Networks,” 21st Int. Conf. Adv. Inf. Netw. Appl. Work., pp. 438–442, 2007.

[20]. K. Malasri and L. Wang, “Addressing security in medical sensor networks,” Proc. 1st ACM SIGMOBILE Int. Work. Syst. Netw. Support Healthc. Assist. living Environ. - Heal. ’07, p. 7, 2007.

[21]. K. Malasri and L. Wang, “Design and implementation of a secure wireless mote-based medical sensor network,” Sensors, vol. 9, pp. 6273–6297, 2009.

[22]. F. N. Wu, I. H. Li, and I. E. Liao, “A Traffic Load-Aware Energy Efficient Protocol for Wireless Sensor Networks,” vol. 2008, pp. 10–12, 2008.

[23]. Lee, Y. S., Alasaarela, E., & Lee, H. J, "An Efficient Encryption Scheme using Elliptic Curve Cryptography (ECC) with Symmetric Algorithm for Healthcare System," Int. J. Sec and Its Applica, vol.8, no. 3, pp.63-70.

[24]. N. Gura, A. Patel, A. Wander, H. Eberle, and S. C. Shantz, “Comparing elliptic curve cryptography and RSA on 8-bit CPUs,” in *Cryptographic Hardware and Embedded Systems* (Lecture Notes in Computer Science), vol. 3156. New York, NY, USA: Springer-Verlag, 2004, pp. 119–132.

[25]. Li, Fagen, and Pan Xiong. "Practical secure communication for integrating wireless sensor networks into the internet of things." *Sensors Journal, IEEE*13, no. 10, 2013, pp.3677-3684.

[26]. N. Gura, A. Patel, A. Wander, H. Eberle, and S. C. Shantz, “Comparing elliptic curve cryptography and RSA on 8-bit CPUs,” Lect. notes Comput. Sci., pp. 119–132, 2004.

[27]. S. Singh, S. K. Maakar, and S. Kumar, “A Performance Analysis of DES and RSA Cryptography,” Int. J. Emerg. Trends Technol. Comput. Sci., vol. 2, no. 3, pp. 418–423, 2013.

[28]. P. Szczechowiak, A. Kargl, M. Scott, and M. Collier, “On the application of pairing based cryptography to wireless sensor networks,” in *Proc.2nd ACM Conf. Wireless Netw. Security*, Zurich, Switzerland, 2012, pp. 1–12.