International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868
Foundation of Computer Science FCS, New York, USA
Volume 2– No.6, May 2012 – www.ijais.org

An Efficient Protocol for Securing Multiple Patient's Privacy in Wireless Body Sensor Network using ECIES

Ramratan Ahirwal
Computer Science & Engineering
Samrat Ashok Technological Institute
Vidisha (M.P.) 464001, India

Bhagirath Bhalawi
Computer Science & Engineering
Samrat Ashok Technological Institute
Vidisha (M.P.) 464001, India

ABSTRACT

In medical applications the wireless body sensor network makes it possible to track over any patient at any time, although in this area security plays an important role such that the unauthorized users can't access the data. Although the ECC is one of the more secure technique to encrypt the data. Hence the elliptic curve cryptographic techniques used to make the patient's data secure.. In this paper Elliptic Curve Integrated Encryption Scheme (ECIES) is introduced which makes strong public key cryptographic system for the purpose of data encryption and decryption. Integrated Encryption Scheme is a public key encryption based on ECC. It is designed to be semantically secure in the presence of an adversary capable of launching chosen-plaintext and chosen ciphertext attacks. The ECIES provides a more secure way of encryption as compared to the existing security algorithms using MAC and hashing. In our scheme we can access multiple data reading from sensors and integrate them at the storage site.

Keywords

Elliptic Curve Cryptography, Elliptic Curve Integrated Encryption Scheme, Private Key Generator, Secret Key, Sensor Node. Depositary

1. INTRODUCTION

Body Sensor Networks (also known as bodynets or Body Area Networks) have the potential to revolutionize healthcare monitoring. These networks are comprised of wearable devices with attached sensors that can measure various physiological and environmental signals. Bodynet devices communicate wirelessly with networked gateways (mobile phones, computers and PDAs) which store, analyze and communicate vital information in real-time. A Bodynet can be designed to immediately alert emergency personnel to a critical situation like a heart attack or a debilitating fall. Bodynets can also help physicians catch warning signs of a disease earlier or remotely monitor the progress of a recovering surgery patient.

A Wireless Sensor Network (WSN) is a wireless network consisting of spatially distributed autonomous devices using sensors to cooperatively monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants, at different locations. The development of wireless sensor networks was originally motivated by military applications such as battlefield surveillance. However, wireless sensor networks are now used in many civilian application areas, including environment and habitat monitoring, healthcare applications, home automation, and traffic control.

In addition to one or more sensors, each node in a sensor network is typically equipped with a radio transceiver or other wireless communications device, a small microcontroller, and an energy source, usually a battery. The envisaged size of a single sensor node can vary from shoebox-sized nodes down to devices the size of grain of dust although functioning 'motes' of genuine microscopic dimensions have yet to be created. The cost of sensor nodes is similarly variable, ranging from hundreds of dollars to a few cents, depending on the size of the sensor network and the complexity required of individual sensor nodes. Size and cost constraints on sensor nodes result in corresponding constraints on resources such as energy, memory, computational speed and bandwidth. Sensor nodes can be imagined as small computers, extremely basic in terms of their interfaces and their components.

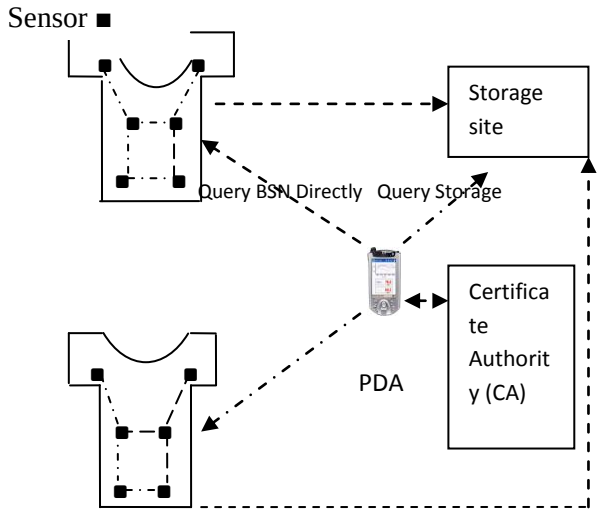


Figure 1: A Body Sensor Network

They usually consist of a processing unit with limited computational power and limited memory, sensors (including specific conditioning circuitry), a communication device (usually radio transceivers or alternatively optical), and a power source usually in the form of a battery. The base stations are one or more distinguished components of the WSN with much more computational, energy and communication resources. They act as a gateway between sensor nodes and the end user. A sensor is any device that generates a signal based on its environment. Sensors are either built into the node or are connected via an input port.

Figure 1 show inertial sensor board attached to Tmote Sky. The Tmote Sky contains 16 input pins that allow hardware designers to attach sensing devices. The sensor board also contains a charging circuit and voltage regulators for the attached Lithium Ion battery.

ECIES is an advance technique of IBE (identity based encryption) that used in symmetric or asymmetric based scheme. IBE scheme, For example, Alice may want to encrypt a message for the doctor in charge on Monday. Alice can independently generated a public key using the strings "Monday" and "doctor" to encrypt her data without further contact with the trusted party. To decrypt the message, a doctor will have to convince the trusted party that he is a doctor in charge on Monday. The same doctor working on Tuesday cannot decrypt messages encrypted using the string "Tuesday" and "doctor" even if he knows the secret key from Monday. The simple example cannot be easily accomplished without using IBE. Alice can try to generate many public/secret key pairs, one for each occasion. However, Alice will have to store the secret key created with the trusted party each time a new public/secret key pair is generated. Otherwise, the trusted party cannot derive the secret key on its own. This is inefficient.

Another possible alternative is for Alice to include some instructions with each of her message, and encrypt everything with the trusted parties' public key. When a doctor receives an encrypted message, the doctor will forward it to the trusted party. The trusted party can decrypt can obtain Alice's instructions. The trusted party will release the message to the doctor only if he meets Alice's instructions. This solution is also inefficient since a BSN may generate many pieces of data, each of which has to be forwarded to the trusted party for decryption. Using IBE, the doctor only needs to be given a single secret key once.

The reminder of the paper is organized as fallows. In section 2 reviews of Shrng Zhong, Qun Li's protocol and with its drawback. In section 3 we Introduce our efficient and secure ID-based user & doctor authentication scheme , and we discuss the security analysis in section 5, compare the performance and efficiency of the propose scheme with other related scheme in section 6. And finally concludes the paper in section 7.

2. BACKGROUND

The Elliptic curve with identity based encryption technique provides the security of single data over the network, but here we have proposed the Elliptic curve integrated encryption scheme standard to secure multiple patient's record. The elliptic curve integrated encryption system (ECIES) is the standard elliptic curve based encryption algorithm. It is called integrated, since it is a hybrid scheme that uses a public –key system to transport a session key for use by a symmetric cipher. The idea is to use multiple sensors in multiple patients, where the sensors notes different reading and collect over to the storage site.

A. Private Key Generation: The pkg generation show the fig.2.

Private Key generation is identity base encryption scheme. In our scheme we use private key generator to generate doctor private key with the help of patient identity and doctor identity that create doctor private key. When user has been authenticated by CA then the CA will allow the PKG to generate master private key as well as medical server will be allowed to provide the data to the user. The adversary cannot obtain data until he is authorized by CA. If the adversary can somehow obtain the flag and data from storage site, he cannot get public parameter necessary to decrypt the data unless CA gives him public parameters. This is not possible without authentication. To decrypt an IBE-encrypted message, in addition to the IBE public parameters, the recipient needs to obtain the private key that corresponds to the public key that the sender used. The IBE private key is obtained after successfully authenticating to a private key generator (PKG), a trusted third party that calculates private keys for users. The recipient then receives the IBE private key over a secure connection.

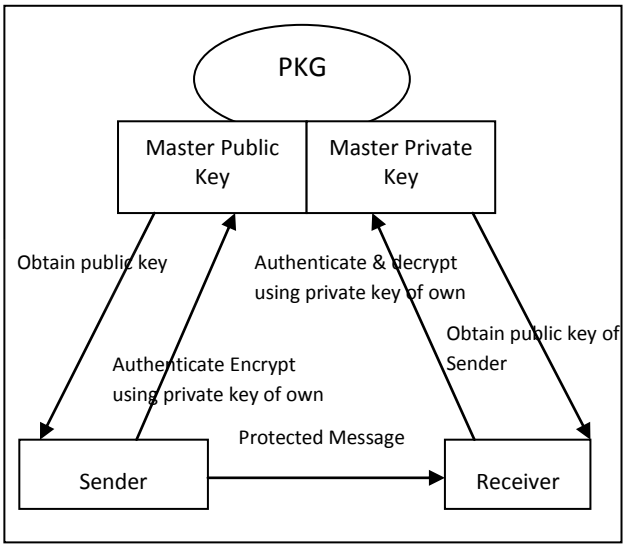


Fig.2 Private Key Generation

3. RELATED WORK

The motivation behind a BSN is to place low cost sensors directly on the patient for health care monitoring. With this in mind, we are implementing the security of the BSN data by which intruders or other unauthenticated person cannot access the data without permission of patient. In this regard there are various work on security has been implemented till now. For example Dan Boneh et.el in their research proposal "Identity-Based Encryption from the Weil Pairing" [2] propose a fully functional identity-based encryption scheme (IBE). The scheme has chosen ciphertext security in the random oracle model assuming a variant of the computational Difie-Hellman problem. They give precise definitions for secure identity based encryption schemes and give several applications for such systems.

In the 2003, S. Capkun, L. Buttyan [3] introduce in their research entitled "Self-organized public-key management for mobile ad hoc networks" to proposed a fully self-organized public-key management system that allows users to generate their public-private key pairs, to issue certificates, and to perform authentication regardless of the network partitions and without any centralized services. Furthermore, our approach does not require any trusted authority, not even in the system initialization phase.

Moreover in same year, H. Chan, A. Perrig, and D. Song [4] present a Random key pre-distribution scheme for sensor networks. In their scheme, it provides Key establishment in

sensor networks. They presented three new mechanisms for key establishment using the framework of pre-distributing a random set of keys to each node. First, in the q-composite keys scheme, we trade off the unlike lines of a large-scale network attack in order to significantly strengthen random key pre-distribution's strength against smaller-scale attacks. Second, in the multipath-reinforcement scheme, we show how to strengthen the security between any two nodes by leveraging the security of other links. Finally, they presented the random pair-wise keys scheme, which perfectly preserves the secrecy of the rest of the network. Any node is captured, and also enables node-to-node authentication and quorum-based revocation. Other than this proposal, several research prototypes have been developed [16, 24, 8, 17]. The use of identity-based cryptography (IBE) [23, 2, 5] for medical applications was also suggested by [20, 19], but our work presents practical implementation on actual sensors rather than a general architecture. Other applications of IBE include [12, 1, 10].

Sensor network security is a widely researched area [22, 11], with solutions focusing on key deployment [7, 13, 15, 4], public key cryptography [14, 21, 9] and management [6, 18, 3]. Unlike prior work, our security protocols incorporate identity-based cryptography primitives.

4. PROPOSED SCHEME

The elliptic curve integrated encryption system (ECIES) is the standard elliptic curve based on encryption algorithm. It is called integrated, since it is a hybrid scheme that uses a public key system to transport a session key for use by a symmetric cipher.

ECIES is a public-key encryption algorithm. In ECIES we assumed to be a set of domain parameters (K, E, q, h, G), but to these we also add a choice of symmetric encryption and decryption functions which we shall denote $E_k(m)$ and $D_k(c)$.The use of a symmetric encryption function makes it easy to encrypt long messages. In addition instead of a simple hash function we require two special types of hash function:

A message authentication code MACk(c).

MAC: {0.1} ^n * {0, 1} ^* → {0, 1} ^m

This acts precisely like a standard hash function except that it has a secret key passed to it as well as a message to be hashed.

A key derivation function KD (T, l)

KD E * N → {0, 1} ^*

A key derivation function acts precisely like a hash function except that output length could be quite large. The output is used as a key to encrypt a message hence if the key is to be used in an Ex-OR-based encryption algorithm the output needs to be as long as the message is being encrypted. The ECIES scheme works like a one-pass Diffie Hellman key transport, where one of the parties is using a fixed long term rather than an ephermal one. This is followed by symmetric encryption of the actual message. For example the combined length of the required MAC key and the required key for the symmetric encryption is given by l. In this paper we have proposed Elliptic curve Integrated Encryption Scheme which provides a better way of securing the patient's data as compared to the existing algorithm.

A. Algorithm

This algorithm can be applied to achieve multiple reading simultaneously at the same time and by using the identity of a particular patient the reading can be accessed. To setup ECC, we first select a particular elliptic curve E over GF (K), where k is a big prime number. We also denote G as the base point of E and q as the order of K, where q is also a big prime. We then pick a secret key x, and the corresponding public key y, where y = x ·G, and a Message Authentication Code hash function. Finally, we have the secret key x and public parameters (Y, K, k, q, h (.) G). Encrypting a message m using public key Y as EciesEncrypt (m, Y). The Elliptic curve integrated encryption standard technique consists of reading the data from the sensors which is then encrypted in the sensors using Algorithm 1.The Algorithm 2 is used to decrypt the data. The Algorithm 3 is used to encrypt the data using a public key i.e. the identity of the patient. The Algorithm 4 is used by the doctor to decrypt the data using the identity of the patient. The Algorithm 6 is used to provide a certificate for both the identity of the patient and the doctor so that the identities of both are stored as PKG in the storage site which is then used to verify the doctor and decrypt the reading. The resulting ciphertext is denoted by c. The decryption of ciphertext c using the secret key x is given as EciesDecrypt(c, x). The recipient is assumed to have a long-term public /private key pair (Y, x) where

$$Y = [x] G$$

Algorithm1: EciesEncrypt(m ,y)

ECIES Encryption	
INPUT:	Message m and public key
OUTPUT:	The ciphertext (U,c,r)
1.	Choose k € R(1…….q-1)
2.	U ← [k]G
3.	T ← [k]Y
4.	(k1‖k2) ← KD(T,l)
5.	Encrypt the message c ← Ek1(m)
6.	Compute the MAC on the ciphertext r ← MACk2(c)
7.	Output (U,c,r)

Each element of the ciphertext (U,c,r) is important:

U is needed to agree the ephermal Diffie Hellman key T.c is actual encryption of the message. r is used to avoid adaptive chosen ciphertext attacks. Notice that the data item U can be compressed to reduce bandwidth, since it is an elliptic curve point.

Algorithm2: EciesDecrypt(c, x)

ECIES Decryption	
INPUT:	Ciphertext (U,c,r) and a private key r.
OUTPUT:	The message m or an 'invalid ciphetext' message
1.	T ← [x]U
2.	(k1‖k2) ← KD(T,l)
3.	Decrypt the message m ← Dk1(c).
4.	if r ≠ MACk2(c) then output 'Invalid Ciphertext'.
5.	output m

Notice that the T computed in the decryption algorithm is the same as the T computed in the encryption algorithm since

Tdecryption = [r]U = [x][k]G = [k]([x]G) =

[k]Y=Tencryption

Algorithm 3: Encrypt (m, str)

Encrypt(m,public_key)
1. Determine the String str using agreed upom pattern
2. Generate public key Ystr.
3. Execute ECIES_Encryption(m, Ystr) to obtain c.

Algorithm 4: Decrypt(c, str)

Decrypt(U,c,r) where r is a private key
Doctor executes ECIESDecrypt(U,c,r) to obtain m

Algorithm 5: Sensor encrypting data

1. Derive the string str, that is also using as flag string. This string is a known bit string.
2. Calculate c =Encrypt(str, d)
3. Send (Flag, c) to storage site.

Algorithm 6: Doctor querying for data

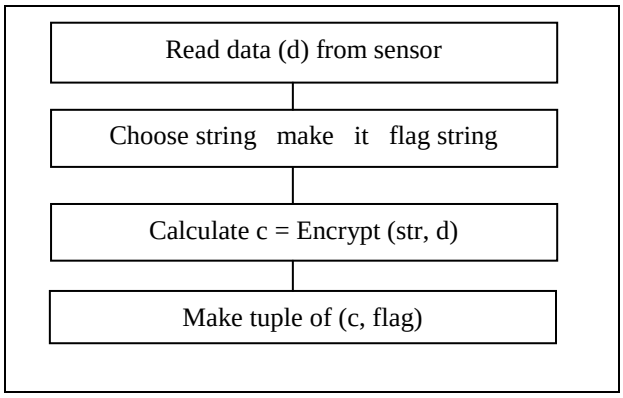
Doctor querying for data
1. Doctor send certificate (Doctor-Id) to CA and PKG (KMS) and Patient-Id with known str (flag string) for Authentication and key generation.
2. CA will check the authorization and Access Permission of Doctor based on policy
3. If "Authenticated" then
I. PKG runs Keygen(str) to derive Xstr
II. CA sends the Private key (Xstr) to doctor
1. 4. Doctor sends Patient-id and flag string to Storage Site. And then
I. For every (ci, flagi) i ∈ K for patient do
II. Storage site matches flagi string with flag string given by doctor
III. If flag string = = flagi then
IV. Storage site sends corresponding encrypted ci to doctor
I. Doctor execute the EciesDecrypt (ci , Xstr)
II. Doctor accept the patient data
III. End if
End For

The Notations

The notation use in proposed scheme and phases are describe below-

U	Public Key
X	Private Key
Y	Public Key
T	The ephermal Diffie Hellman key
L	Message Length
K	Shared secret Key with random prime number.
H(.)	One way Hash Function
‖	Concatenation
⊕	Bitwise XOR Operation
G	Base point with random big prime number
Ek1 (m)	Encrypted message
Dk1(c)	Decrypted ciphertext
MACk2(c)	Secure message authenticate code
K1	Diffie Hellman key
K2	Diffie Hellman key

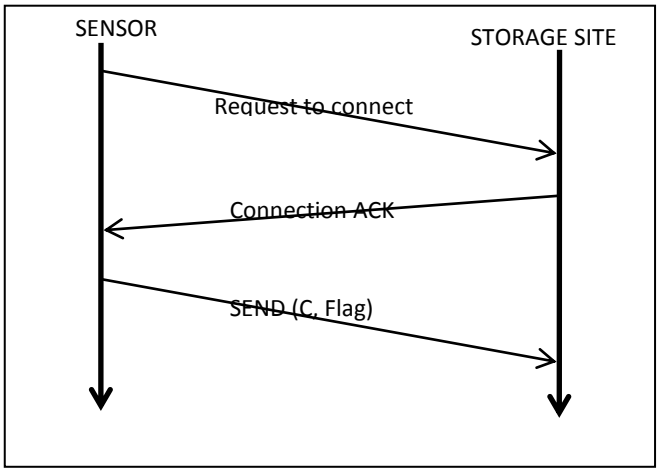
B. Flow Chart



C. Data collection

As the sensors from multiple patient's sense the data, each of these data will contain a string which is stored in the storage site. Let the sensor collect data d at event str with the flag that is the given bit string. The sensor executes Alg. 5 to encrypt its data. Following flowchart shows the block-diagram of data collection from sensor and encryption of that data. Tuple (c, Flag) is then stored in sensor memory. The flag is a commonly known bit-string several bits long. As shown in the above fig. is the flow of data from the sensors.

A doctor wishing to obtain data collected under some str will first contact the CA for permission. After the CA agrees, the PKG will run Keygen(str) to derive the corresponding secret key X_{str} needed to decrypt data. The doctor then contacts the storage site and retrieves the data as shown in Alg. 6. When the data is stored within the sensor, the role of the storage site will be executed by the sensor. Following block-diagram shows the pictorial presentation of doctor querying for data after the authenticating and getting the private key from CA and PKG respectively.



D. Data transfer

Periodically, each sensor in the BSN will transfer its data to the storage site. This is done by first aggregating all the data into a cell-phone like device that may be either PDA or it may be any built-in device within the body sensor network that is equipped with GSM service. The cell-phone then forwards the aggregated data to the storage site. Assuming that there are k tuples generated by the BSN, the cell-phone will forward the set {(c1, flag1). (ck, flagk)}. Alternatively, a sensor with enough storage capacity can opt to store the data within the sensor itself. In this case, there is no data transfer process. Following block diagram show the transmission of data from sensor to storage site.

E. Querying

A doctor wishing to obtain data collected under some str will first contact the CA for permission. After the CA agrees, the PKG will run Keygen(str) to derive the corresponding secret key X_{str} needed to decrypt data. The doctor then contacts the storage site and retrieves the data as shown in Alg. 6. When the data is stored within the sensor, the role of the storage site will be executed by the sensor. Following block-diagram shows the pictorial presentation of doctor querying for data after the authenticating and getting the private key from CA and PKG respectively. Since all the data is encrypted, the storage site checks the flag of each tuple in database and if the flag matches then storage site return a specific encrypted tuple to the doctor , instead, the storage site simply lets the doctor try to decrypt each tuple (c^i) belonging to the patient. The reason for returning specific c^i to the doctor instead returning all tuples is to improve efficiency of channel by reducing the traffic on the channel and hence it will save bandwidth of the channel.

5. SECURITY ANALYSIS

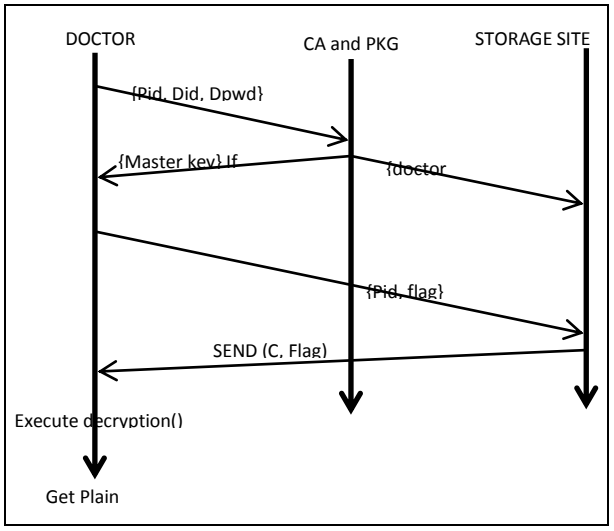
I. Analyses of Basic Primitives

Our Setup picks n secrets and n corresponding public keys. Knowing only one X_{str} and h(str), the doctor cannot determine the patient's master secret X since there are n unknown x_i. The doctors only able to determine X when he has in this possession n

Different secret keys $x_1$str… $x_n$str.

The use of X_{str} and Y_{str} as the private key and public key derived from string str does not violate the discrete logarithm property of ECIES where, given a $y = x \cdot P$, it is infeasible to determine x given y and P, since both are simply the result of addition of points. Also, both Encrypt and Decrypt are secure since both rely on well-established ECC encryption and decryption methods.

5.I.1. Analysis of Proposed Security Protocol



Privacy of the patient's data by encrypting all the information before forwarding the data to the storage site

Prevent unauthorized access to the patient's data. This is achieved by authentication of doctor. Also CA sends the private key X_{str} to doctor which cannot be used to decrypt any other cipher text, not encrypted using public key Y_{str}. Flexibility Patient is the only person who will register the doctor to access his/her data from the storage site by authenticating him to CA. The patient will register doctor-ID and Password with policy that is for how many days, the doctor is authentic to access his/her data. The process of specifying what doctor-id and password is can be programmed by the patient without additional permissions from the CA. A compromised sensor does not allow the adversary to obtain any useful data about a patient from the storage site since the sensor only stores the publicly known parameters.

Protected Storage site At most the adversary try obtains the cipher text with flag i.e. (c, flag) from storage site. Storage site cannot provide stored data without getting permission from central authority, since the central authority checks the authentication of any user that may be any authenticated user or even adversary. When user has been authenticated by CA then the CA will allow the PKG to generate master private key as well as medical server will be allowed to provide the data to the user. The adversary cannot obtain data until he is authorized by CA. If the adversary can somehow obtain the flag and data from storage site, he cannot get public parameter necessary to decrypt the data unless CA gives him public parameters. This is not possible without authentication.

II. Channel Bandwidth Analysis

In the earlier work performed by Tan, Wang, Zhong and Li in his work "Body Sensor Network Security" major drawback of above protocol is wastage of channel bandwidth between storage site and doctor for example if for different patient whose records are stored at the site, the maximum number of tuples in record of one patient is N, then the bandwidth reserved for data flow between storage site and doctor should be enough to allow this much data flow at a time. I.e. mathematically, if Xi = data size associated with one parameter then channel bandwidth needed to be reserved equal to

Where H= header length.

Xi = encrypted data size of tuple Ci.

According to our protocol, the reserved channel bandwidth is proportional to the average number of tuples transmitted per interaction between storage site and doctor. This means that if number of parameter that sensors generates requires an increase n times then the increase in channel bandwidth will be less than n times. Channel bandwidth required in our protocol is proportional to

N1, N2..... Nn are number of tuples

transmitted in 1st, 2nd and nth interaction.

III. Energy Consumption Analysis

In the earlier protocol [10] all the data and flag received by storage site were first encrypted and stored and when a doctor requires information about one patient then all the encrypted tuples related to that patient were sent to doctor in encrypted form. In our protocol, only the values generated by sensors are stored in encrypted form at the storage site and flag are not encrypted. When doctor requires information about particular patient, he first obtain access permission from CA, then he sends flag associated with the tuples related to patient but only those tuples which doctor presently requires but not all the tuples.

Table 1 : Analysis on different parameters

Public Key	Signature	Encrypted Data	Decrypted Data	Data Storage
0.69 sec.	0.7 sec.	5.5 Sec.	2.07 sec.	45 bytes

Thus our protocol saves encryption and decryption time due to the following changes compared to previous protocol: Flag are not encrypted as in earlier protocol. At a time all the tuples related to the patient is not sent. Only the tuples mentioned by means of flag are sent. Therefore less number of tuples will be decrypted by doctor's PDA.

Thus protocol saves the CPU time complexity in encryption and decryption process.

Therefore ratio indicated energy saved can be found as follows: Suppose data size to be encrypted = D bytes Flag size is = F bytes. Suppose energy consumed/byte of encryption = e mJ/B Then energy consumed in our scheme = D* e mJ. In previous protocol energy consumed = (D* e + F*e) mJ

Therefore the percentage of energy saved =

$$\frac{(F * e)\ mJ}{(D * e + F * e)\ mJ} X\ 100$$

$$\left\{\frac{F}{(F + D)}\right\} X\ 100\ \%$$

6. RESULT AND COMPARISON

Public key: The key generated when the sensors starts reading from the patient.

Signature: The sensors when reads the data and encrypted that data using signatures (verification of the sender and the receiver so that the unauthorised user can't access the data) so that data can't be access eavesdropped and the signatures when matched can be decrypted.

Encrypted data: The data which is not in actual form but can be converted into another form such that the even if the data is accessed can't understand by the others.

Decrypted Data: The data which is encrypted to provide a security to the data will be decrypted by the same technique used for encryption such that data is correct and readable.

Data storage: The memory required to store a single data from the patient in the sensor.

As shown in the table 1 that the proposed algorithm when implemented gives less time than the existing ECC technique, Also the proposed algorithm requires less storage in the sensor to store the data. Hence requires less storage.

The comparison between existing protocol and our protocol

Table 2: The comparison between existing protocol and our protocol

given below:

Parameters	Chiu C. Tan ECC using IBE	Our Algorithm(ECIES)
Public key	0.74 s	0.69s
Signature time	0.77 s	0.7s
Time to encrypt	5.0s	5.5s
Time to decrypt	1.12 s	2.07s
Storage	1.6 KB	45bytes

Table 2 : Key Required Vs Storage Size in Byte

Storage (Bytes)	2500	5000	10000	25000	50000
Keys	50	100	200	500	1000

As our proposed algorithm generates 'n' number of public keys and different on the number of public keys the sensors read that number of data. As shown in the table 3 that as the memory required to store the data will depends on the number of public keys and the storage will increase if the number of public keys generated will increase.

Table 3: Times Required Vs Key Required Result Analysis

Time(S)	3.45	6.9	10.35	13.8	17.25	20.7
Keys	5	10	15	20	25	30

The table 4 shows the time required to generate the public key, as our proposed algorithm generates 'n' number of public keys, so the time required for generating 'n' public keys will increase the time according to the number of public keys generated.

7. CONCLUSION

We presented alternative security and privacy technologies consider for use in our system architecture for an e-hospital environment. This paper has presented the working of a system of compact, wearable, wireless body sensing devices implanted in the human body. Patients have web access to the community services and provide their medical data using wireless sensor devices and/or web browser. Doctors access community services either remotely or from inside the hospital. The novel achievement is that we have proposed is the improvement in the existing protocol for data encryption, decryption and transfer between BSN, storage site and doctor with the need for high data rates.

In this proposal some saving of encryption, decryption and comprise the encrypted data, required bandwidth of channel and energy consumption of sensor can be achieved. Here we are trying to implement the light weight IBE technique to make the data secure using ECIES. The goal is to collect reading from multiple sensors from multiple patients and to make this data secure using encryption technique.

8. REFERENCES

[1] N. Asokan, K. Kostiainen, P. Ginzboorg, J. Ott, andC. Luo.Applicability of identity-based cryptography for disruption tolerant networking. In MobiOpp 2007.

[2] D. Boneh and M. Franklin. Identity-based encryption from the Weil pairing. In CRYPTO 2001.

[3] S. Capkun, L. Butty´an, and J.-P. Hubaux. Self organized public-key management for mobile ad hoc networks. IEEE TMC 2003.

[4] H. Chan, A. Perrig, and D. Song. Random key predistribution schemes for sensor networks. In IEEE SP 2003.

[5] C. Cocks. An identity based encryption scheme based on. quadratic residues. In LNCS 2260 (2001).

[6] W. Du, R. Wang, and P. Ning. An efficient scheme for authenticating public keys in sensor networks. In MobiHoc 2005.

[7] L. Eschenauer and V. D. Gligor. A key-management scheme for distributed sensor networks. In CCS 2002.

[8] R. Ganti, P. Jayachandran, and T. Abdelzaher. Satire:A software architecture for smart attire. In Mobisys 2006.

[9] J. Girao, D. Westhoff, E. Mykletun, and T. Araki.Tinypeds: Tiny persistent encrypted data storage in asynchronous wireless sensor networks. Ad Hoc Networks 2007.

[10] U. Hengartner and P. Steenkiste. Exploiting hierarchical identity-based encryption for access control to pervasive computing information. In SecureComm 2005.

[11] C. Karlof, N. Sastry, and D. Wagner. Tinysec: a link layer security architecture for wireless sensor networks. In SenSys 2004.

[12] A. Kate, G. Zaverucha, and U. Hengartner. Anonymity and security in delay tolerant networks. In SecureComm 2007.

[13] L. Lazos and R. Poovendran. Serloc: Secure range independent localization for wireless sensor networks. ACM TOSN 2005.

[14] A. Liu, P. Kampanakis, and P. Ning. Tinyecc: Elliptic curve cryptography for sensor networks (version 0.3). 2007.

[15] D. Liu and P. Ning. Establishing pairwise keys in distributed sensor networks. In CCS 2003.

[16] B. Lo and G. Z. Yang. Key technical challenges and current implementations of body sensor networks. In BSN 2005.

[17] D. Malan, T. Fulford-Jones, M. Welsh, andS. Moulton. Codeblue: An ad hoc sensor network infrastructure for emergency medical care. In BSN 2004.

[18] D. J. Malan, M. Welsh, and M. D. Smith. A public-key infrastructure for key distribution in tinyos based on elliptic curve cryptography. In SECON 2004.

[19] K. Malasri and L. Wang. Addressing security in medical sensor networks. In HealthNet 2007.

[20] M. Mont, P. Bramhall, and K. Harrison. A flexible role-based secure messaging service: exploiting IBE technology for privacy in health care. In International Workshop on Database and Expert Systems Applications 2003.

[21] E. Mykletun, J. Girao, and D. Westhoff. Public key based cryptoschemes for data concealment in wireless sensor networks. In ICC2006.

[22] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and J. D. Tygar. SPINS: Security protocols for sensor networks. In Mobicom 2001.

[23] A. Shamir. Identity-based cryptosystems and signature schemes. In CRYPTO 1984.

[24] L. Zhong, M. Sinclair, and R. Bittner. A phone centered body sensor network platform: cost, energy efficiency and user interface. In BSN 2006.