AN EFFICIENT SECURE ID-BASED FOR SECURING MULTIPLE PATIENTS' USING ECIES PRIVACY IN WIRELESS BODY SENSOR NETWORK

Bhagirath bhalawi,
Research Scholar
Samrat Ashok Technological Institute
Vidisha (M.P.)464001 India
shri.kashikunj2@gmail.com

Ramratan Ahirwal
Assistant professor
Samrat Ashok Technological Institute
Vidisha (M.P.)464001 India
ram2004_ahirwal2004@rediffmail.com

Yogendra Kumar Jain
Head of the Department (CSE)
Samrat Ashok Technological Institute
Vidisha (M.P.)464001 India
ykjain_p@yahoo.co.in

***Abstract*— 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, analyse 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.**

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.

Keywords

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

I. INTRODUCTION

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.

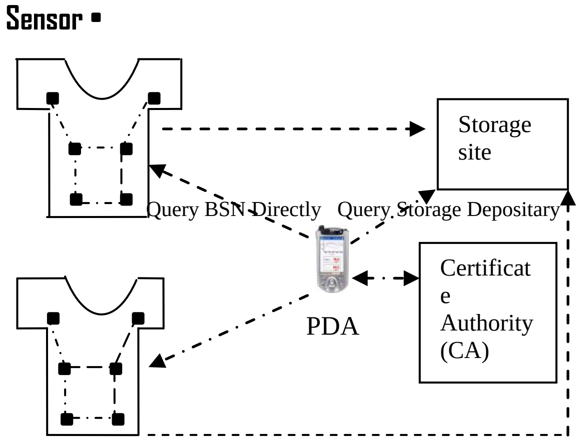


Figure 1: A Body Sensor Network They usually consist of a *processing unit* with limited computational power and limited memory, *sensors* (including specific conditioning circuitry), a *communication device* (usually radio transceivers or alternatively optical), and a power source usually in the form 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.

II. BACKGROUND

The wireless body sensor network makes it possible to track over any patient at any time, although in this security plays an important role such that the unauthorised users can't access the data. Hence the elliptic curve cryptography is implemented to make the patients data secure. Although the ECC is one of the more secure technique to encrypt the data but here we have proposed the Elliptic curve integrated encryption scheme standard to secure multiple patient's record. The idea is to use multiple sensors in multiple patients where the sensors notes different reading and collect over to the storage site.

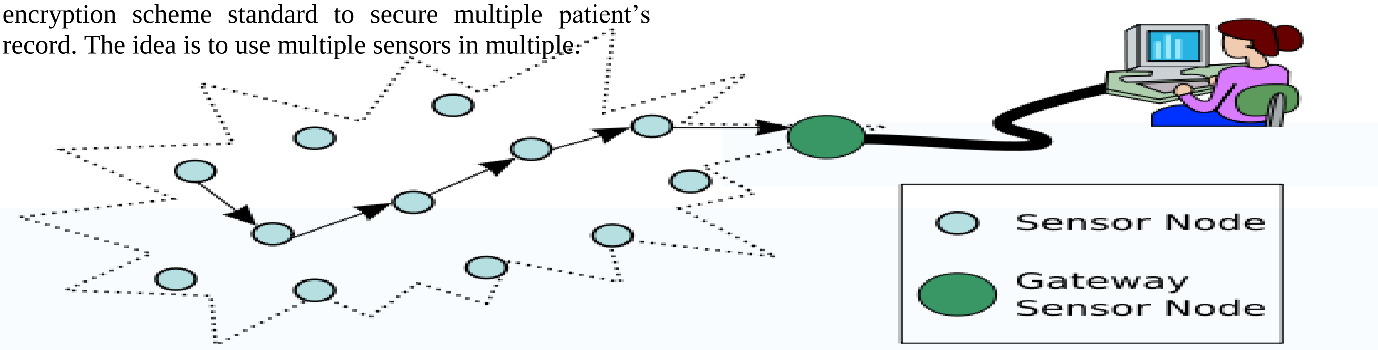


Figure1.1: Typical Multiple patient Wireless Sensor Network Architecture

III. 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, 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.

IV. PROPOSED SCHEME

To setup ECC, we first select a particular elliptic curve E over GF (p), where p is a big prime number. We also denote P as the base point of E and q as the order of P, where q is also a big prime. We then pick a secret key x, and the corresponding public key y, where y = x · P, and a Message Authentication Code hash function. Finally, we have the secret key x and public parameters (y, P, p, q, h (.)).

Encrypting a message m using public key y as EccEncrypt(m, y). The resulting ciphertext is denoted by c. The decryption of ciphertext c using the secret key x is given as EccDecrypt(c, x).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.

ECIES is a public key encryption algorithm like ECDSA there is assumed to be a set of domain parameters (K,E,q,h,G), but to these we also add a choice of symmetric encryption/decryption functions which we shall denote k(m) and Dk(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 a xor-based encryption algorithm the output needs to be as long as the message is 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. The recipient is assumed to have a long-term public /private key pair (Y,x) where

Y = [x] G

Algorithm1: EciesEncrypt(m, y)

```
1: Generate a random number 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)
5: Compute the MAC on the ciphertext, r ⇓MAC k2(C).
6. Return (U,c,r)
```

Algorithm2: EciesDecrypt(c, x)

```
1: T ⇓ [r] U
2: (K1||K2) ⇓ KD(T,l)
3: Decrypt the message m ⇓ Dk1(c)
4: if r ≠ MAC k2(c) then output "invalid ciphertext"
5: output m
```

Algorithm 3: Encrypt (m, str)

```
1. Determine string str using agreed upon syntax
2.Generate public key Ystr where
Ystr = …. yi
3. Execute EccEncrypt(m, Ystr) to obtain c
```

Algorithm 4: Decrypt(c, str)

```
After authorization and Key generation
Doctor executes EciesDecrypt(c, Xstr) 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

```
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
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
     V. Doctor execute the EciesDecrypt (ci , Xstr)
     VI. Doctor accept the patient data
     VII. End if
     VIII. End For
```

V. SECURITY ANALYSIS

In previous work [10], all flag and all data are to be encrypted but in our protocol only sensor generated values are encrypted. Flags are not encrypted

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 =

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

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

VI. Result Comparison

A comparison between existing protocol and Proposed (our) protocol is now given below:

Basic of comparison	Existing protocol	Proposed Protocol
Encryption and Decryption of flag	YES	NO
Tuples in the record of patient which are transmitted	ALL	Requested ones only
Channel Bandwidth to be reserved	O(N) where N is no. of tuples in recoed of patient.	O(e) Where e is expected number of tuples requested at a time where e<=N
Energy Consumption for encryption	O(D+F) where D is size of data in the record and f is size of flag	O(D)
Encryption consumed for decryption	O(D+F) where D is size of data in the record and F is size of flag	O(D*e/N) where e/N<=1
Time required for Encryption	O(D+F)	O(D)
Time required for Decryption	O(D+F)	O(D*e/N)

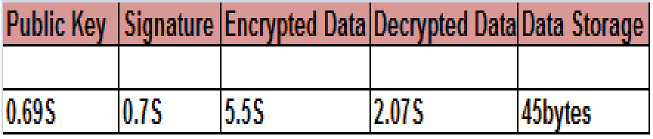
A. Public key: The key generated when the sensors starts reading from the patient.

B. Signature: The sensors when reads the data and encrypted that data using signatures so that data can't be access eavesdropped and the signatures when matched can be decrypted.

C. 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.

D. 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.

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



Public Key	Signature	Encrypted Data	Decrypted Data	Data Storage
0.69S	0.7S	5.5S	2.07S	45bytes

Figure2: Analysis on different parameters

As shown in the fig. 2 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.

Storage (bytes)	ECC-IBE	ECIES
2500	50	N*50
5000	100	N*100
10000	200	N*200
25000	500	N*500
50000	1000	N*1000

Figure 2.1: Key Required Vs Storage Size in Byte

Where 'N' is the number of patients

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 fig. 2.1 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.

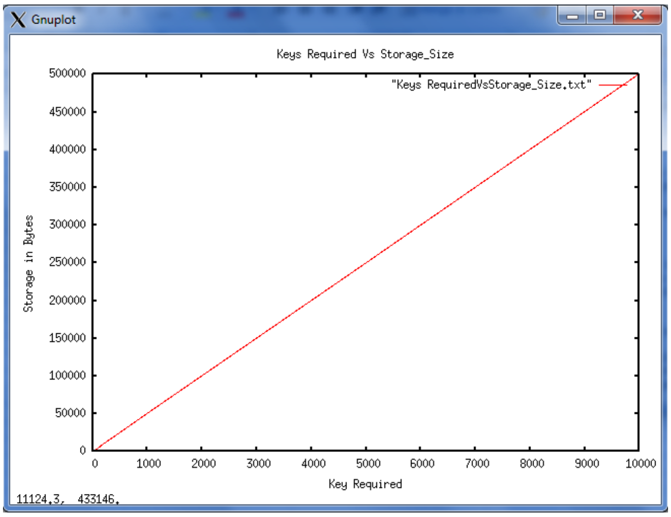


Figure 2.3: Key Required Vs Storage Size in Byte

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 fig. 2.3 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.

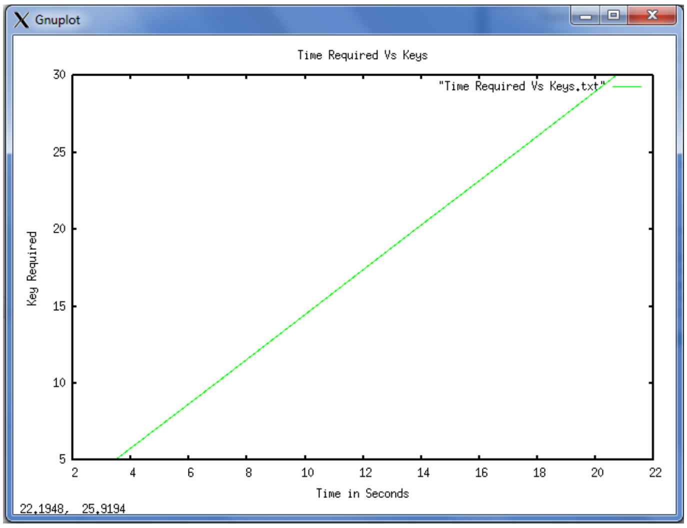


Figure 2.4: Times Required Vs Key Required Result Analysis

The fig. 2.4 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.

VII. Conclusion

This paper has presented the working of a system of compact, wearable, wireless body sensing devices implanted in the human body. 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 and decryption, required bandwidth of channel and energy consumption of sensor can be achieved.

In this thesis, IBE has been used with Elliptic Curve Integrated Encryption Scheme (ECIES) which makes strong public key cryptography system for the purpose of data encryption and decryption.

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

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

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

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

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

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

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

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

[17] 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.

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

[19] 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.

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

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

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

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

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

.