Implementation of Aggregate Signcryption in Unattended Medical WSNs using Micaz

Faezeh S. BABAMIR [1]

Abstract

Healthcare applications are promising fields for wireless sensor networks called wireless medical sensor networks. The main issues in wireless medical sensor networks are reliable communication, patient mobility and security of sensed physiological data. In order to mobile patient monitoring, disconnected or unattended setting of wireless medical sensor networks is considered. The disconnected property causes periodic or offline data delivery of information. Moreover, medical sensors nodes should retain data for long time while they have limited battery and capacity. These challenges provide attacker to threat security of sensed data without being detected. In this paper, we propose an efficient aggregate signcryption technique to provide simultaneously confidentiality, integrity (by encrypting) and authenticating (by signing) for collected data. Moreover, the aggregation property reduces communication and space overhead as well as signcryption provides time efficiency by applying mostly linear operators. We further, compare our technique with the nest alternative works in the literature to show the efficiency and resilience against various attacks.

Keywords: unattended wireless medical sensor networks, confidentiality, integrity, authenticity, space overhead.

[1] *Electronic Engineering, Istanbul Technical University, Turkey*

1. INTRODUCTION

Wireless Sensor Networks (WSNs) are emerging technologies which are recently attracts many researchers. A wireless sensor is a small, low power and low capacity unit of a network that can be implemented in large scale environments. These networks have many applications such as military, water monitoring, healthcare and etc. in this paper; we consider healthcare application with a disconnected WSN. Moreover, we consider disconnected or Unattended Wireless Medical Sensor Network (UWMS). Generally, a wireless medical sensors maybe wearable, implantable or potable and also can be integrated in various kind of motes including Mica2, Micaz and Telos [1]. Unattended WMSNs are deployed on patient body to closely monitor physiological patient conditions, providing a patient has locomotion and is not always in the access of doctor or caregiver. In other words, the patient would be periodically present to log his physiological data. These physiological data should be 1-confidential: because patient health data are generally held under the legal obligations as well as should be available just for doctors or caregivers. Moreover, data eavesdropping by an adversary causes breaching the patient privacy.

2-authentication: data authorization in UWMSNs is a must for every medical sensor to verify by a trusted receiver e.g. doctor. 3-Integrity: the system should have integrity to guarantee that physiological data is not altered. Data modification in WNSNs is very dangerous, since it can mislead the doctor and threats the patient life.

To achieve confidentiality and authenticity traditionally, encryption and *then* signature (message authenticated code) are often combined. The traditional way is infeasible with the disadvantages: (1) heavy overheads; (2) lack of security. Zheng proposed a novel concept named *signcryption* to perform the encryption and signature in a single simoltaneous primitive [2]. Zheng's conception is unpractical for increasingly popular ubiquitous communications. Bao and Deng improved it and gave a signcryption that can be verified publicly in 1998 [3].

In this paper, we propose a new aggregate signcryption to achieve more functionalities. Moreover, since this technique includes some efficient order functions such as addition, Elliptic Curve Cryptography (ECC) multiplication (one of the main advantages of ECC is small key size [4]. A 224-bit key in ECC is considered to be secure as a 2048 key in RSA [5]. the broadcast cost significantly is reduced. Also, we apply aggregation mechnism to decrease and compress amount of data. First advantage exceeds the lifetime of networks, while second advatage, helps either sender and receiver to run the proposed technique in efficient time and space orders.

This paper is organized as follows. Section 2 reviews related work, followed by Section 3 which introduces our environment assumptions and definitions. Then, Section 4 provides our proposed aggregate signcryption. In section 6, we explain the implementation our practical technique. Section 7 describes proof of security. Section 6 sketches our technique compared to another work. Finally, Section 8 presents our conclusions and future work.

2. RELATED WORKS

The property that ensures us will be computationally infeasible for an adversary to recover past secret keys of a compromised node if she knows the current value of the key is forward security. On the other hand, backward security guarantees that knowledge of current key cannot be used to disclose any information about future ones.

Muhammad et al. in [6] proposed BARI+ which is distributed key management protocol based on biometric. This wireless body area network (WBAN) is managed by four keys including, communications key, administrative key, basic key and secret key. Huang et al. [7] proposed a secure access. They used a wearable sensor system (WSS) to monitor the vital signals of patient. WSS uses an Advance Encryption Standard (AES) based authentication (i.e. CBC-MAC) as well as encryption scheme. A public key based key establishment protocol is used to establish the secure key. Haque et al. [8] proposed a public key based infrastructure for patient monitoring system using WSN. This scheme is composed of three main components: patient (PT), healthcare system (HSS) and secure base stations (SBSs). A pair-wise shared key and bilateral key handshaking method are applied to the established secure communications between three components. Also, this proposed scheme provides data confidentiality by encryption and decryption.

Contribution: To the best of our knowledge, this paper is the first to identify the problem of data security in UWMSNs, using *signcryption technique*. Using aggregation concept, communication and memory overheads are significantly reduced. Also, we use unknown receiver *secret key* to hide receiver nature. Moreover, the total mission of our scheme is efficiently gathering and transmitting data in which receiver remain anonymous. Finally, our research opens up new directions and identifies challenges in the context of UWMSN security.

3. DEFFINITIONS AND NETWORK ASSUMPTIONS

3.1. Bilinear pairing

Let G_1 be an additive cyclic group generated by g, with prime order *q(=113)*, and G_2 be a multiplicative cyclic group of the same order q with the set. A bilinear pairing is a map $e: G_1 \times G_1 \rightarrow G_2$ with the following properties. For any $P, Q, R \in G$ and $a, b \in Z_q^*$:

- Bilinearity: $e(P+Q, R) = e(P, R)\, e(Q, R)$ and $e(P, Q+R) = e(P, Q) e(P, R)$. In particular, $e(aP, bQ) = e(P, Q)^{ab} = e(P, abQ) = e(abP, Q)$.
- Non-degeneracy: $e(P, P) \neq I_{G_2}$, where I_{G_2} is the identity element of G_2.

3.2. Related Computational Assumptions

In this section, we review the assumptions related to bilinear maps that are relevant to the protocol we discuss.

- Bilinear Diffie-Hellman Problem (BDHP): Given $g, ag, bg, cg \in G_1^4$ for unknown $a, b, c \in Z_q^*$, the BDH problem in G_1 is to compute $e(g, g)^{abc}$.
- Computational Diffie-Hellman Problem (CDHP): Given $A = ag \in G_1$ for unknown $a \in Z_q^*$, the CDH problem in G_1 is finding a.

3.3. Network assumptions

Suppose some UWNS which consists of N sensors and a sink. Sink have to visit the network periodically. Moreover, sensors collect data during *collection intervals,* each of which is divided into *v round*. At the end of each equal round, the collected data will be signcrypted and further at the end of each equal interval, all signcryptions will be aggregated to one unit of data to send. These signcryption are threat by an adversary denoted as ***A*** during an interval. ***A*** is curious or aims to prevent receiving data to the sink or more over, changes the data to deceive sink. In this paper, we propose a new scheme to defend curious adversary by encrypting, changing data by signing and even deleting them by alerting sink to supply deleted data via other neighbor sensors. Below, we describe the condition of the adversary:

- Compromise power: We envision a powerful mobile adversary. We assume that ***A*** is capable of compromising at most *k* out of *n* sensors within a particular time interval (0 <*k* <*n/2)*. This subset of compromised sensors is not clustered or contiguous. Furthermore, in every interval, ***A*** can migrate and compromise a different subset till occupies the whole of network.
- Limited erasure capacity: Between any two successive sink visits, ***A*** can erase no more than a given number of measurements from the network. Otherwise, this raises an alarm on the sink and contradicts ***A***'s goal of remaining undetected.

Defense awareness: ***A*** is fully aware of any scheme or algorithm that any sensor uses to defense.

4. THE PROPOSED IDENTITY BASED AGGREGATE SIGNCRYPTION

The new Identity Based Aggregate Signcryption scheme for unattended WSNs consists of algorithms *Setup, KeyGen, Signcrypt, Aggregate-Signcrypt, Unsigncrypt,* and *Aggregate-Unsigncrypt* which are explained as below. Suppose identity *ID* signcrypts messages m_i and finally aggregates them. Note that the signature of our scheme is inspired from [9].

- **Setup:** Let *d* be a security parameter of the system. We define an Elliptic Curve *E* on a finite field $GF(2^v)$ where *v* is a prime power number. Let G_1 be an additive cyclic subgroup of the group of EC points (included infinity point O_E) with *g* and *q* as generator and prime order of G_1respectively.Also we let G_2 be a multiplicative group with prime order $q\,Z_q^*$. We define a function $f(x) = \log_p(x)$ where $x, f(x), p \in Z_q^*$ Let *e* be a "Bilinear Map" (BM) defined by $G_1 \times G_1 \to G_2$ that $e(g,g) = p$. Let H_i be the following hash functions:

  $H_1 : G_1 \times \{0,1\}^* \to Z_q^*$, $H_2 : G_2 \times G_2 \times \{0,1\}^* \to G_1$,

  $H_3 : G_1 \times G_1 \times \{0,1\}^* \to Z_q^*$,

  $H_4 : G_1 \times \{0,1\}^* \to \{0,1\}^{|ID|+|m|+|q|}$

  Where |ID| and |m| are the length of *ID* and message *m* respectively. Let ID_B is the identity of receiver and the Master private key *"Msk"* be $x \in Z_q^*$ and the master public key $X = xg$. Therefore, the public parameter is:

"Params" = <G_1, G_2, X, g, e, H>, $Msk = x$

- **KeyGen*(ID)*:** To generate a partial secret key for identity *ID*, the *KeyGen* selects $r \in Z_q^*$ at random, computes:

$R \leftarrow rgx^{-1}$, $s \leftarrow rx^{-1} + xH_1(R, ID) \bmod q$,

We call $H' = H_1(R, ID)$. The sensor partial private key is (R, s). A correctly generated secret key should fulfill $sg = R + XH'$ (1).

- **Signcrypt(m_i, *ID*, ID_B, *(R, s)*, *j*):** Signcrypt algorithm inputs a message, sender identity *ID*, receiver identity ID_B, sender partial private key and interval number. Let $Y_i = gy_i^{-1}$ .For every message, we have:

(y_i, K)=*StartRoundKey(i, j, ID, (R,s))*,

y_{i+1}= *MessageKey-Generator* (y_i, *ID, (R,s))*,

$Z_i \leftarrow y_i + sH_3(Y_i, R, m_i) \bmod q$,

$C_i = P[i \| m_i \| Y_{i+1}]XOR[H_4(Ry_i^{-1}, ID)]$

The signcryption of message m_i is

$\delta_i = < C_i, Z_i, K >$.

- **Aggregate-signcrypt(σ_i, *ID*):** On receiving *n* individual signcryptions $\delta_i = < C_i, Z_i, K >$, where $i=1$ to n(all K are the same) and identity *ID* as sender. The output is the aggregation <K, Z_{agg}>.

$Z_{agg} = \sum_{i=1}^{n} Z_i$, $\delta_{agg} = < K, \{C_i\}_{i=1}^{n}, Z_{agg} >$

- **Aggregate-Unsigncrypt(σ_i, *ID*, *(R, s)*, *j*):** The receiver executes the algorithm with $\delta_{agg} = < K, \{C_i\}_{i=1}^{n}, Z_{agg} >$, sender identity *ID*, its partial private key and interval number *j*. This algorithm outputs $m_i, \forall i$ for every valid message otherwise it outputs *false*.At the begining of the interval *j,* thesensor computes Y_1= *MessageKey- Discoverer(K, ID, (R,s),j)*. Then for every message, we have:

$i \| m_i \| Y_{i+1} \leftarrow [C_i]XOR[H_4(rY_i, ID)]$,

$h_i \leftarrow H_3(Y_i, R, m_i)$,

To verify the aggregate signcryption δ_{agg} for message m_i and identity *ID*, the verifier should computes h_i for $m_i, \forall i$.

Verification:

if $e(gZ_{agg}, g^{-1}) = \prod(e(Y_i^{-1}, g)e(g^{-1}h_i, R + XH'))$ then pass output *(m_i)* corresponding to *ID*, else output *"Invalid"*.

Correctness:

$$e(gZ_{agg}, g^{-1}) = e(g\sum(y_i + sh_i), g^{-1}) = e(\sum gy_i, g^{-1})e(\sum gsh_i, g^{-1}) = e(\sum Y_i^{-1}, g)e(\sum h_i g^{-1}, gs) = \prod e(Y_i^{-1}, g)e(h_i g^{-1}, R + XH')$$

- *MessageKey -Generator (y_i, ID, (R,s)):* This function input the current round key, *ID* and its partial private key and outputs a key $y_{i+1} \in Z_q^*$ for the next round.

$$y_{i+1} \leftarrow PRNG(y_i) \bmod q$$

- *MessageKey-Discoverer(K, ID, (R,s), j):* This function inputs seed *K*, *ID,* its partial private key and interval number. It outputs a key rY_1 for receiver.

$$w = e(K,X) = e(y_1 H_2(s,j,ID_B),xg) = e(g,g)^{y_1 x_j x} = p^{y_1 x_j x}$$
$$rY_1 = \frac{H_2(s,j,ID_B)(r)}{f(w)} = \frac{x_j gr}{\log_p(p^{y_1 x_j x})} = \frac{x_j gr}{y_1 x_j x} = \frac{R}{y_1}$$

- *StartRoundKey(i, j, ID, (R,s)):* This function input the current round key number, interval number, sender *ID* and its partial private key and outputs a key $y_1 \in Z_q^*$ and corresponding seed $K \in G_1$. At the beginning of the interval, (i.e. $i=1$). This function selects a random key $y_1 \in Z_q^*$ to compute:

$$K = y_1 H_2(s,j,ID_B) = x_j Y_1, x_j \in Z_q^*$$

Otherwise ($i \neq 1$), the function outputs current (y_i, *K)* located in the sensor memory.

5. PROOF OF SECURITY

In this section, we present two probability analysis proofs.

The identity based aggregate signcryption scheme is ($\varepsilon, t, q_k, q_s, q_h$)-secure against IND-IBAS-CCA2 adversary ***A*** under adaptive chosen identity and adaptive chosen ciphertext attack in the random oracle model if Elliptic Bilinear Diffie Hellman Problem (EC-BDHP) assumption holds in G_1.

$$\varepsilon' = (1 - \frac{q_s(q_s + q_2 + q_3)}{q})(1 - \frac{q_u}{q})(\frac{1}{q_1})\varepsilon \qquad (1)$$

$$t' = t + O[(q_k + q_s + q_u)E_m + q_u E_e] \qquad (2)$$

And q_1, q_2, q_3, q_k, q_s, q_u and q are the number of H_1, H_2, H_3, *KeyGen, Signcryption* and *Unsigncryption* queries respectively. E_m and E_e is the time for multiplication and bilinear pairing operations respectively.

Probability analysis proof: ***C*** only fails in providing a consistent simulation because one of the following independent events happens:

- E1: ***A*** does not choose to be challenged on *ID**.
- E2: ***A*** makes key extraction query on challenged *ID**.
- E3: ***C*** aborts in a Signcryption query because of a collision on H_2 and H_3.
- E4: ***C*** rejects a valid ciphertext at some point.

5.1. Confidentiality

We have $\Pr[\sim E_1] = \frac{1}{q_q}$ and $\sim E_1$ implies $\sim E_2$. Also $\Pr[\sim E_3]$ is:

$$(1-\frac{q_s}{q})^{q_s+q_2+q_3} \geq 1-\frac{q_s(q_s+q_2+q_3)}{q}$$

Considering $\Pr[\sim E_4] = \frac{q_u}{q_q}$, the overall successful probability $\Pr[\sim E_1 \wedge \sim E_3 \wedge \sim E_4]$ is at least equation 1.

The time complexity of the algorithm is dominated by the multiplication in the KeyGen, Signcryption and Unsigncryption queries and bilinear pairing in just Unsigncryption query which is equal to equation 2.

5.2. Unforgeability

The identity based aggregate signcryption scheme is $(\varepsilon, t, q_k, q_s, q_h)$-secure against EFU-IBAS-CMA2 adversary ***A*** under adaptive chosen identity and adaptive chosen ciphertext attack in the random oracle model if Elliptic Curve Discrete Logarithm Problem (EC-DLP) is hard in G_1.

Probability Analysis Proof: This is similar to the one in Theorem 1. In addition, there is a rewind here, with successful probability $\varepsilon = q_3$. Combine together, the overall successful probability is at least:

$$(1-\frac{q_s(q_s+q_2+q_3)}{q})(1-\frac{q_u}{q})(\frac{1}{q_3 q_1})\varepsilon^2$$

6. IMPLEMENTATION

In this section, an overview of the implementation in the single-hop setting is presented. This implementation is like [9] because the signcryption of our scheme is very similar.

6.1. Basic setting

In this simulation, the system parameter *Params* generated by the base station, is embedded in each sensor node when they are deployed. Like the case for general WSNs, the base station is powerful enough to perform computationally intensive cryptographic operations, unlike the sensor nodes, that have limited resources in terms of computation, memory and battery power.

The sensor nodes used are MicaZ 3, developed by Crossbow Technology. Its RF transceiver complies with IEEE 802.15.4/ZigBee, and the 8-bit microcontroller is Atmel ATmega128L, a major energy consumer. Also a PC (Dell Dimension 9150 3.0 GHz CPU, 1GB RAM) is considered as a base station. The utilized programming languages are like [9]: nesC, C and Java. The base operating system for the MicaZ platform is TinyOS 2.0. In addition, elliptic curve cryptography due to the small key size and low computational overhead are employed. We specifically used an ECC library developed by Siemens AG 4 with 160-bit key size. we split the signcryption packets into two phases instead of single phase is that the "*K*" part of our signcryption will be the same for all signcryptions produced from a particular sensor node; hence it will save communication overhead by sending *K* once at the very beginning of the communications.

6.2. Energy Consumption Model

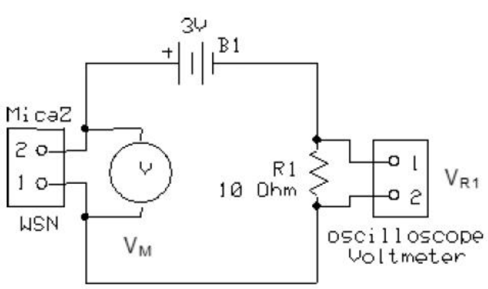

Figure 1: Power supply circuit for estimating energy consumption of MicaZ

Since the actual energy consumed when running our codes in MicaZ cannot be calculated just based on its internal impedance, there is no way to estimate the impedance of logic gates. Hence, the energy consumption of MicaZ is measured indirectly. Figure 1 shows the power supply built for estimating the energy consumption for our scheme. The circuit is powered by two Sanyo AA size NiMH rechargeable batteries, with fully charged and voltage level is at 2.97V. The reason that a resistor *R*1 is added to the circuit instead of just connected to an Ammeter in series of the circuit is because to capture the current changes in the circuit and the period of changes at the same time. With this setup, we are able to measure the current flow into MicaZ indirectly by measuring the voltage drop, *VR*1, in the resistor *R*1 using HP54520 oscilloscope. After we had the current information, we measure the total voltage drop across Micaz, *VM*, by using Fluke 87 voltmeter connected in parallel with MicaZ. By now, we are able to calculate the total power of the circuit in any instance. In order to get the energy consumption, we need the timing information. MicaZ is programmed to execute our scheme periodically. With this, the oscilloscope is able to capture the computation time as the voltage across *R*1 and *VR*1 will change across MicaZ during the computation of our scheme.

7. COMPARISON

In this section, we present the performance analysis of our scheme (IBAS) compared to the FssAgg schemes [10] (best known alternatives). In Table I, advantages and disadvantages of these schemes are presented. $|\sigma|$, $|sk|$, $|pk|$ are bit length of signature/signcryption, private key and public key of given scheme, respectively. In tables II, ‘S’, ‘V’, ‘AS’, ‘AU’ mean Signing, Verifying, Aggregate Signcryption and Aggregate Unsigncryption respectively.

Our scheme is storage/bandwidth efficient and complements each other in terms of their storage overhead. Table II compares IBAS and FssAgg schemes about storage and communication overheads. Upon receiver opinion, IBAS, which require only single key storage, is the most storage efficient schemes. FssAgg and FssAgg-BLS (which is resourceful to address such UWMSN applications) schemes require linear and quadratic order storage respectively. Upon a sensor’s perspective, all schemes require constant storage. Also aggregation property makes only a constant transmission overhead. Note that the aggregation also causes “all-or-nothing” property that provides the resilience against the truncation attacks [10]

TABLE I. COMPARISON OF IBAS AND FSSAGG

	IBAS	FssAgg			
		BLS	***AR***	***BM***	***MAC***
Data Confidentiality	✓	X	X	X	X
Public Verifiablity	✓	✓	✓	✓	X
Unbounded Time Period	✓	X	X	X	X
Forward-Secure Confidentiality	✓	X	X	X	X
Backward-Secure Confidentiality	✓	X	X	X	X
Flexible Delivery Schedule	✓	✓	✓	✓	✓
Signer Storage Efficient	✓	✓	✓	✓	X
Receiver Storage Efficient	✓	X	✓	✓	✓
Immediate Verification	✓	✓	✓	✓	✓

TABLE II. ORDER COMPARISON OF IBAS AND HASSAFS

	IBAS	**FssAgg**			
		BLS	***AR***	***BM***	***MAC***
S/AS	O(1)(|H|+|sk|+|pk|)	(Exp+H)l	(3x.Sqr+x/2Muln)l	(x.Sqr+x/2Muln)l	(3H)l
V/AU	O(1)|sk|	(PR+H)l	x(L+l)Sqr+(lx/2)Muln	L.Sqr+(2l+l.x)Muln |	(3H)l

8. CONCLUSION

We further studied the security issue in unattended wireless medical sensor networks with identity-based aggregate signcryption scheme. This proposed scheme is different with the scheme proposed by other techniques in WSNs [10, 11, 12, 13, 14]. Our scheme is proven secure with respect to its IND-CCA2 and EUF-CMA security formal and probability security. These are the strongest security notions for message confidentiality and authentication respectively. In addition, our scheme is efficient time and space order, i.e. both sender and receiver need least time and space overheads to make secure system. In future works, we are supposed to improve our work by applying Homomorphic property. Applying this property, sensors are able to make secure connections through the network. In future, we are supposed to study other cryptographic hard problems to reduce linearly time order as well as equipped our scheme with some high applicable property called homographic. This property helps network to securely and efficiently transmit data.

9. REFERENCES

[1] P. Kumar, H. Jea Lee, "Security issues in healthcare applications using wireless medical sensor networks: a survey", in journal of sensors, vol. 12, pp. 55-91, 2012.

[2] Y. Zheng, "Digital signcryption or how to achieve cost (signature & encryption) << cost(signature) + cost(encryption)," *In: Kaliski Jr. B.S. ed. Advances in Cryptology–CRYPTO'1997. LNCS1294*,

Heidelberg: Springer-Verlag,1997, 165-179

[3] F. Bao, RH. Deng, "A signcryption scheme with signature directly verifiable by public key," *In: Imai H., Zheng Y. ed. Public Key Cryptography'98, LNCS 1431*, Heidelberg: Springer-Verlag,1998, 55-59

[4] A. S. S. Mateus, C. B. Margi, M. A. Simplicio, C. C. F. P. Geovandro and B. T. de Oliveira, "Implementation of data survival in unattended wireless sensor network using cryptography", *in proceeding of IEEE conference on Local Computer Networks (LCN), 2010, USA, pp. 961-967.*

[5] C. H. Lim and H. S. Hwang, "Fast implementation of elliptic curve algorithm in GF(p^n), " *in public key cryptography series, lecture notes in computer science,* vol. 1751, springer, 2000, pp.405-421.

[6] K.R.R.S. Muhammad, H. Lee, S. Lee, Y.K. Lee, "BARI+: A Biometric Based Distributed Key Management Approach for Wireless Body Area Networks" *in journal of Sensors, vol. 10, pp. 3911-3933, 2010.*

[7] Y. M. Huang, M.Y. Hsieh, H.C. Hung, J.H. Park, "Pervasive, Secure Access to a Hierarchical Sensor-Based Healthcare Monitoring Architecture in Wireless Heterogeneous Networks," *IEEE J. Select. Areas Commun., vol. 27, pp. 400-411, 2009.*

[8] M.M. Haque, A.S.K. Pathan, C.S. Hong, "Securing u-Healthcare Sensor Networks Using Public Key Based Scheme," *In Proceedings of 10th International Conference of Advance Communication Technology, Pyeongchang, Korea, 19–22 February 2008; pp. 1108-1111.*

[9] J. K. Liu, J. Beak, J.Zhou, Y. Yang and J. W. Wong, "Efficient online/offline identity based signature for wireless sensor network," *International journal of security,* vol. 9, issue. 4, pp. 287-296, 2010.

[10] D. Ma and G. Tsudik "Extended abstract: Forward-secure sequential aggregate authentication," *in proceeding of IEEE symposium on security and privacy (S&P),* Oakland, CA, USA, May 2007, pp. 86-91.

[11] D. Ma, "Practical forward secure sequential aggregate signatures, " *in*

proceeding of the 3rd ACM symposium on information, computer and communications security (ASIACCS'08), ACM, NY, USA, 2008, pp. 341-352.

[12] D. Ma and G. Tsudik, "A new approach to secure logging," *ACM transaction on storage (TOS),* vol. 5, no. 1, 2009, pp. 1-21.

[13] Faezeh S. Babamir, Z. Eslami, *"Data Security in Unattended Wireless Sensor Networks through Signcryption",* KSII Transactions on Internet and information systems, 2012, 9, 287-296.

[14] Faezeh S. Babamir, A. Norouzi *"Achieving key privacy and invisibility for unattended wireless sensor networks in healthcare",* The Computer journal, Oxford journal, doi: 10.1093/comjnl/bxt046.