International Journal of Advance Research, IJOAR .org
Volume 1, Issue 11, November 2013, Online: ISSN 2320-9194

# SECURE COMMUNICATION FOR LAN AND WAN IN WIRELESS SENSOR NETWORKS INTO INTERNET OF THINGS

1M.Tharani 2 N.Senthilkumar
*1PG scholar , ECE department*
*Vivekanandha College of Engineering For Women*
*Mail id: tharanim53@gmail.com*
*2Associate Professor/ECE department Vivekanandha College of Engineering For Women Mail id: senthilsuguna@gmail.com*

## Abstract –

A secure channel between a sensor node and internet host is created, hence new security challenges arises and wireless sensor networks is integrated into internet of things. We use heterogeneous online/offline signcryption scheme so that secure communication is provided. We use bilinear diffie- hellman inversion problem in random oracle model, it provides indistinguishability against adaptive chosen ciphertext attacks and existential unforgeability against adaptive chosen messages attacks. This scheme has the following advantages: First, it achieves confidentiality, integrity, authentication, and non- repudiation in a logical single step. Second, it allows a sensor node in an identity-based cryptography to send a message to an Internet host in a public key infrastructure. Third, it splits the signcryption into two phases: i) offline phase; and ii) online phase. In offline phase heavy computations are carried out and in online phase light computations are done. This scheme is suitable to provide security solution for integrating WSN into the IoT. We use this scheme and perform an industrial application.

## Index Terms—

Wireless sensor network, Internet of things, security, signcryption, public key infrastructure, identity- based cryptography.

## I. INTRODUCTION

The Internet of Things (IoT) is a booming field that has received considerable attention from both academy and industry. The primary idea of IoT is permanent presence for variety of objects such as radio-frequency identification (RFID) tags, sensors, actuators, mobile phones, etc.-which, through unique addressing schemes, are able to view each other and collaborate with their neighbors to reach common goals[2]. Wireless sensor networks (WSNs) are ad hoc networks which consist of a large number of small sensor nodes with restricted resources and one or more base stations. Usually, sensor nodes consist of a processing unit with constrained computational power and limited capacity. [6]To guarantee unforgeability, integrity and confidentiality of communications, the traditional method is to digitally sign a message then followed by public key encryption. [1] On the other hand, the base station is a powerful trusted device that acts as an medium between the network user and the nodes.[1] WSNs have many applications, that includes military sensing and tracking, environment monitoring, target tracking, healthcare monitoring, and so on. The data received from the sensors through the base station can be read by users of WSN. If we wish to read the data from anywhere in the world, we need to integrate the WSNs into the Internet as part of the IoT. [6]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. [3]There are three methods to acheive this integration, front-end proxy solution, gateway solution and TCP/IP overlay solution. In the front-end proxy solution, the base station acts as an interface between the WSNs and the Internet. There is no direct connection between the Internet and a sensor node. The base station allows all incoming and outgoing information. In the gateway solution, the base station acts as an application layer gateway that translates the lower layer protocols from both

networks. In the TCP/IP overlay solution, sensor nodes communicate with each nodes using TCP/IP. The base station acts as a router that forwards the packets from and to the sensor nodes. In both gateway solution and TCP/IP overlay solution, the sensor nodes can communicate with the Internet hosts directly. However, new security challenges will appear, such as setup of a secure channel between a sensor node and an Internet host that supports end-to-end authentication and confidentiality services. The computational power and storage of a sensor node are always limited. [5] A new identity based signature (IBS) scheme without MapToPoint function in the random oracle model, which offers better performance than Other IBS schemes from pairings. This ensures a better security aid for communication. The internet of things is nothing but combination of sensors and connectivity.

[4]To support the authenticity of public keys in the public key cryptography, there are two main infrastructures called public key infrastructure (PKI) and identity-based cryptography (IBC) . In the PKI, a certificate authority (CA) issues a certificate which provides an unforgeable and trusted link between the public key and the identity of a user by the signature . The drawback of the PKI is that we need to manage certificates, including revocation, storage and distribution. In addition, we need to verify the validity of certificates before using them. On the other hand, the dependence on the PKG who can generate all users' secret keys inevitably causes the key escrow problem in the IBC. For the WSNs, IBC is the best choice because there is no certificates problem. However, Identity Based Cryptography is only suitable for small networks. For the Internet security, we need PKI technique.

### *A. Contribution*

The motivation of this paper is to setup a secure channel between a sensor node and an Internet host that supports end-to-end confidentiality, integrity, authentication and non-refusal services. In addition, we require that the IBC is used in the sensor node and that the PKI is used in the Internet host. We also require that the computational cost of sensor nodes is low. Our solution is heterogeneous online/offline signcryption (HOOSC). Concretely, we propose an efficient HOOSC scheme. We prove that the proposed scheme has the indistinguishability against adaptive chosen ciphertext attacks (IND-CCA2) under the bilinear Diffie-Hellman inversion problem (BDHIP) and existential unforgeability against adaptive chosen messages attacks (EUF-CMA) under the $q$ -strong Diffie-Hellman problem ($q$-SDHP) in the random oracle model. We have a computational problem called twin bilinear Diffie- Hellman inversion (BDHI) problem. But for our work bilinear Diffie-Hellman inversion is more suitable. Our scheme has the following characteristics: (i) It achieves confidentiality, integrity, authentication and non-refusal in a logical single step. (ii) It allows a sensor node in the IBC to send a message to an Internet host in the PKI. (iii) It splits the signcryption into two phases: offline phase and online phase. In the offline part, most heavy computations are done without the knowledge of a message. In the online stage, only light computations are done when a message is known.

### *B.Related Work*

Signcryption [5] is a new cryptographic primitive that fulfills both the functions of digital signature and public key encryption in a logical single step, at a cost significantly lower than that required by the traditional signature-then-encryption approach. That is, signcryption can simultaneously achieves confidentiality, integrity, authentication and non-refusal at a lower cost. The performance advantage of signcryption over the signature-then-encryption method makes signcryption useful in many applications, such as electronic commerce, mobile communications and smart cards.

In 2010, Sun and Li [7] proposed two heterogeneous signcryption schemes. The first scheme allows a sender in the PKI to send a message to a receiver in the IBC. The second scheme allows a sender in the IBC to send a message to a receiver in the PKI. But their schemes are only secure against outsider attacks (i.e. attacks made by an attacker who is neither the sender nor the receiver). Such signcryption schemes do not provide any kind of non-refusal function. The insider security means that (i) if a sender's secret key is exposed, an attacker is still not able to recover the message from the ciphertext and (ii) if a receiver's secret key is exposed, an attacker is still not able to forge a ciphertext. [6]Our new technique allows the offline information to be re-usable. It performs the signature generation procedure in two phases. [6]The first phase is performed offline (prior to the knowledge of the message to be signed) and the second phase is performed online (after knowing the message to be signed). In WSN, the offline phase can be executed at the base

station, while the online phase is to be executed in the WSN node. The online phase is typically very fast, and hence can be executed efficiently even on a weak processor, such as a node in WSN.

### *C.Organization*

We use heterogeneous offline/online scheme in our paper. We show the working of HOOSC scheme in exploratory section II. The formal model of HOOSC in section III. An efficient HOOSC scheme is proposed in section IV. We analyze the proposed scheme in section V. finally, the conclusion is given in section VI.

## II. EXPLORATORY

In this area, we discuss about the definitions of bilinear pairings:

Let $C_1$ be a cyclic additive group generated by P, whose order is a prime p, and $C_2$ be a cyclic multiplicative group of the same order p. A bilinear pairing is a map $e^{\wedge} : C_1 \times C_1 \rightarrow C_2$ with the following properties:

1) Bilinearity: $e\hat{}(a P, bQ) = e\hat{}( P, Q)^{ab}$ for all P. $Q \in C_1$,, $a,b \in Z^*_p$

2) Non-degeneracy: There exists $P, Q \in C_1$ such as $e\hat{}( P, Q) \neq 1$.

3) Computability: There is an efficient algorithm to $e\hat{}( P, Q)$ for all $P,Q \in C_1$.

The modified Weil pairing and the Tate pairing are of this type. Refer[6],[8] for details of these pairing.

The security of our scheme depends on the hardness of the following problems.

Given two groups $C_1$ and $C_2$ of the same prime order p, a bilinear map $e^{\wedge} : C_1 \times C_1 \rightarrow C_2$ and a generator P of $C_1$, the q-bilinear Diffie-Hellman inversion problems (q-BDHIP) in $(C_1,C_2,e^{\wedge})$ is to compute $e^{\wedge}(P,P)^{1/\alpha}$ given $(P,\alpha p,\alpha^2P,\ldots,\alpha^qP)$. We call bilinear Diffie-Hellman inversion problem (BDHIP) when q = 1.

*Definition 1*: The (e, t)-BDHIP assumption holds if no t-polynomial time adversary S has advantage .

Given two groups C1 and C2 of the same prime order p, a bilinear map $e\hat{} : C1 \times C1 \rightarrow C2$ and a generator P of G1, the q-strong Diffie-Hellman problem (q-SDHP) in (C1, C2, e^) is to find a pair $(w, (1/\alpha+w)(P) \in Z_p^* \times C1$ given $(P, \alpha P,\alpha^2P,\ldots..,\alpha^qP)$.

*Definition 2*: The (e, t)-q-SDHP assumption holds if no t-polynomial time adversary C has advantage at least e in solving the q-SDHP problem.

## *III. MODEL OF HOOSC*

In this area, we give the definition and security notions oh HOOSC. The paper is based on the concept that sender belongs to the IBC and receivers belong to the PKI.

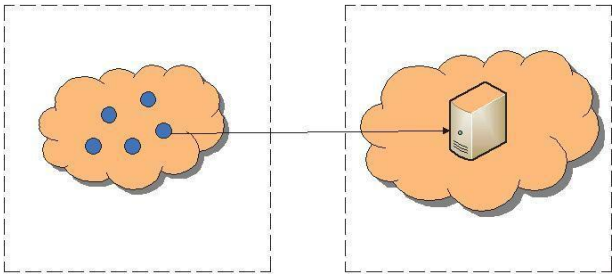


Fig. 1. Communication model for integrating WSNs into the Internet.

### *A. Syntax*

A general HOOSC scheme consists of the following five algorithms.

Setup: This is a probabilistic algorithm that runs by PKG that takes as input a security parameter k, and outputs a master secret key msk and the system parameters params that includes a master public key mpk.

*Ibc-Kg*: This is used as a key generation algorithm for IBC users. The user submits an identity ID to the respective PKG. The PKG computes the corresponding secret key sk and transmits it to the user in a secure way.

*pki-kg*: This is used as a key generation algorithm for PKI users. The user can choose its secret key sk and publishes the corresponding public key pk. This public key needs a digital certificate that is sign by its CA.

*off-signcrypt*: This is a commonly used probabilistic offline signcryption algorithm run by a sender that takes input as the system parameters param, a sender's private key $sk_s$

and a receiver's public key $pk_r$ , and outputs an offline signcryption δ.

*On-Signcrypt*: This is a probabilistic online signcryption algorithm run by the sender that takes as an input the system parameters param, a message m and an offline signcryption δ, and outputs a full signcryption ciphertext σ .

*Unsigncrypt:* This is a deterministic unsigncryption algorithm that is run by a receiver that takes input as a ciphertext σ , a sender's public key $pk_s$ and the receiver's secret key $sk_r$ , and outputs the plaintext m or the symbol ⊥ if σ is an invalid ciphertext between the sender and the receiver.

These algorithms will satisfy standard HOOSC scheme.

For secure communication for integrating WSNs into the Internet, a sensor node is considered as a sender and an Internet host is considered as a receiver. HOOSC provides a secure channel between the sensor node and the Inter-net host that timbers end-to-end confidentiality, integrity, authentication and non-repudiation services.

In Fig.1 there is a connection from nodes to host in internet through IBC and PKI.

### *B. Security Notations*

The standard security notations for signcryption are indistinguishability against adaptive chosen ciphertext attacks (IND-CCA2) and existential unforgeability against adaptive chosen messages attacks (EUF-CMA). We can modify the notations slightly based on [6],[8] to adapt for HOOSC.

*Phase 1*: A performs a polynomially bounded number of unsigncryption queries in an adaptive manner. In an unsign-cryption query, A submits a sender's identity I $D_s$ and a ciphertext σ . C runs Unsigncrypt(σ, I $D_s$ , $sk_r^*$ ) algorithm and sends the result to A.

Phase 2: A can ask a polynomially bounded number of queries adaptively again as in the Phase 1. This time it cannot make an unsigncryption query on $(\sigma^*, ID_s^*)$ to obtain the respective plaintext.

*Definition 3*: A HOOSC scheme is (e, t, $q_u$ )-IND-CCA2 secure if no probabilistic t-polynomial time adversary A has advantage at least e after at most $q_u$ unsigncryption queries in the IND-CCA2 game.

*Definition 4*: A HOOSC scheme is (e, t, $q_k$ , $q_s$ )-EUF-CMA secure if no probabilistic t-polynomial time adversary F has advantage at least e after atmost $q_k$ key generation queries and $q_s$ signcryption queries in the EUF-CMA game.

## IV. A HOOSC SCHEME

In this area, we propose an efficient HOOSC scheme which is based on barreto et al.'s signcryption scheme[9].

*Setup*: Given a security parameter *k*, the PKG chooses groups *C*1 and *C*2 of prime order *p* (with *C*1 additive and *C*2 multiplicative), a generator *P* of *C*1, a bilinear map $\hat{e} : C1 \times C1 \rightarrow C2$, and hash functions $H1 : \{0, 1\}^* \rightarrow Z^*_p$, $H_2 : \{0,1\}^n \times C_1 \times C_2 \rightarrow Z^*_p$, and H3: $G2 \rightarrow \{0,1\}^n$. Here *n* is the number of bits of a message to be signcrypted.

For secure communication integrating WSNs into the Internet, a sensor node is considered as a sender and an Internet host is regarded as a receiver. First, the sensor node is loaded with precomputed results δ = (x , r, β, S, T ) of the offline phase from a more efficient device. When the sensor node wants to send a message m to the Internet host, the sensor node runs σ =On-Signcrypt(m, δ) algorithm and sends the ciphertext σ to the Internet host. In this process, the sensor node only does light computations, such as exclusive OR, hash function, modular multiplication and modular inverse. When receiving the ciphertext σ , the Internet host runs m = Unsigncrypt(σ, I $D_s$ , $sk_r$ ) algorithm to obtain the message m. Our scheme simultaneously achieves confidentiality, integrity, authentication and non-repudiation.

Fig.2 explains the steps for secure communication using heterogeneous online/offline scheme

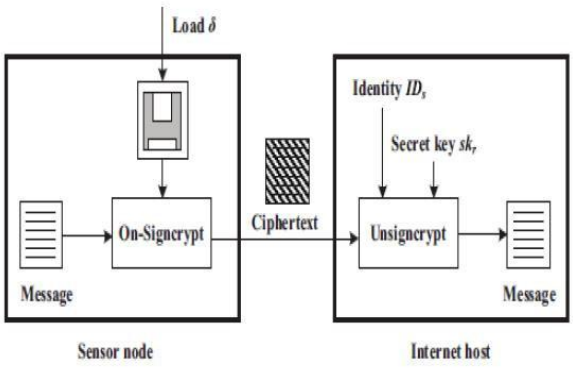


Fig.2. steps for secure communication using the scheme

TABLE I
PERFORMANCE COMPARISON

| Schemes | Computational cost | | Security | | | Key size (bits) | | Ciphertext size (bits) | Offline storage (bits) |
|---|---|---|---|---|---|---|---|---|---|
| | Signcrypt | Unsigncrypt | CCA2 | CMA | IS | IBC users | PKI users | | |
| A [13] | 1F | 1F | Yes | No | No | 320 | 320 | 640 | 0 |
| B[12] | 3M | 2M+2F | Yes | Yes | Yes | 480 | 320 | 960 | 0 |
| C [12] | 2M | 4M | Yes | Yes | Yes | 480 | 320 | 960 | 0 |
| Ours | 2M(offline) | 2M+2F | Yes | Yes | Yes | 320 | 320 | 640 | 1824 |

*C.Performance*

We compare the main computational cost, security, key size, ciphertext size and storage of those existing scheme[10]. We can use a proper signature scheme [11] to attain non repudiation property. We consider that $|G_1|$ = 160 bits, $|G_2|$ = 1024 bits, $|p|$ = 160 bits, $|m|$ = 160 bits and $|ID|$ = 160. In the ―Schemes‖ column, A is the original version in [13]that has not the non-repudiation since a receiver can generate the same ciphertext as a sender does. . However, we are in need of another two pairings computation. B and C are the first scheme and second scheme, as in [12]. We denote by M the point multiplication in $G_1$ and F the pairing computation in the ―Computational cost‖ column. In the ―Security‖ column, CCA2, CMA and IS denotes IND-CCA2, EUF-CMA and insider security, respectively . From Table I, we can see that SL does not satisfy insider security. A, B and our scheme satisfy insider security. For our ease, we consider the pairing and point multiplication operations since the two operations take the most running time of the full algorithm [12].Our scheme splits the signcryption into two phases: offline phase and online phase. Two point multiplication operations have been previously done offline. The online phase is very efficient and does not require any pairing and point multiplication operations. The key size of PKI users in all schemes is 320 bits. For IBC users, A and our scheme are the same and are 320 bits. B and C are 480 bits. For ciphertext length, SL and our scheme are 640 bits. B and C are 960 bits. Of course, our scheme needs an offline storage with 1824 bits. For energy consumption, a point multiplication uses 19.1mJ and a pairing uses 62.73mJ [14], [15]. To Signcrypt a message, SL, A and B roughly uses 62.73mJ, 57.3mJ and 38.2 mJ, respectively That is, our scheme can complete the entire signcryption process when a message is present. The computational energy consumption of our scheme is negligible Therefore, our scheme is completely suitable to provide security solution for sensor nodes. We try to reduce the cost more by using another method.

## VI. RESULT

From TABLE I for different schemes we obtain cost, security, key size, ciphertext size(bits). We try to reduce the cost, size and increase the security by another method.

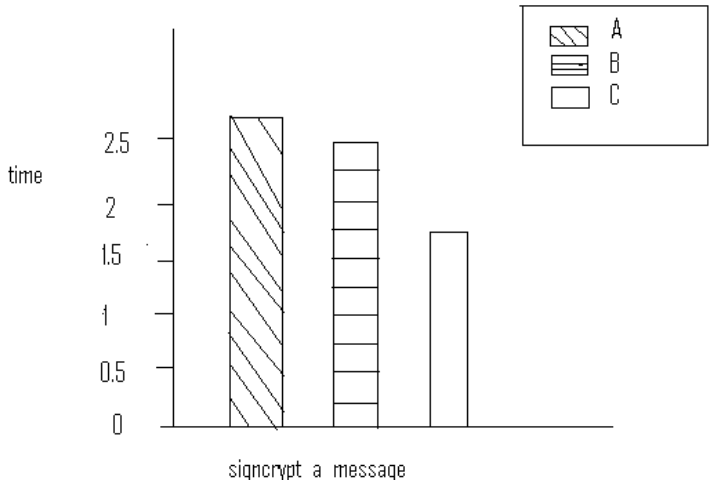


Fig 3. Time for signcrypting a message

## VI. CONCLUSION

In this paper we have used heterogeneous online/offline signcryption scheme. It permits a sensor node in IBC to send a message to an internet host in the PKI. Our scheme has chosen both online/offline technique and IBC technique to reduce computational cost of sensor nodes to a greater extent. Internet hosts allows to support many terms such as end-to-end confidentiality, authentication and non repudiation services. We will use this scheme and work out for an industrial application. This method helps us to give a new security solution for integrating WSN into internet as a part of IoT.

*REFERENCES*

[1] Fagen Li And Pan Xiong, ―practical secure communication for integrating wireless sensor networks into the internet of things‖,2013.

[2] L. Atzori, A. Iera, and G. Morabito, ―The internet of things: A survey,‖ *Comput. Netw.*, vol. 54, no. 15, pp. 2787–2805, Oct. 2010.

[3] R. Roman and J. Lopez, ―Integrating wireless sensor networks and the Internet: A security analysis,‖ *Internet Res.*, vol. 19, no. 2, pp. 246–259, 2009.

[4] D. Boneh and M. Franklin, ―Identity-based encryption from the weil pairing,‖ in *Advances in Cryptology* (Lecture Notes in Computer Science), vol. 2139. New York, NY, USA: Springer-Verlag, 2001, 213–229.

[5] Shi Cui, Pu Duan, Choong Wah Chan, and Xiangguo Cheng,‖An Efficient Identity-based Signature Scheme and Its Applications‖,2007.

[6] B. Libert and J. J. Quisquater, ―A new identity based signcryption schemes from pairings,‖ in *Proc. IEEE Inf. Theory Workshop*, Paris, France, 2003, pp. 155–158.

[7] Y. Sun and H. Li, ―Efficient signcryption between TPKC and IDPKC and its multi-receiver construction,‖ *Sci. China Inf. Sci.*, vol. 53, no. 3, 557–566, Mar. 2010.

[8]P. S. L. M. Barreto, B. Libert, N. McCullagh, and J. J. Quisquater, ―Efficient and provably-secure identity-based signatures and signcryp-tion from bilinear maps,‖ in *Advances in Cryptology* (Lecture Notes in Computer Science), vol. 3788. New York, NY, USA: Springer-Verlag, 2005, pp. 515–532.

[9] Y. Sun and H. Li, ―Efficient signcryption between TPKC and IDPKC and its multi-receiver construction,‖ *Sci. China Inf. Sci.*, vol. 53, no. 3, 557–566, Mar. 2010.

[10] J. C. Cha and J. H. Cheon, ―An identity-based signature from gap Diffie-Hellman groups,‖ in *Public Key Cryptography* (Lecture Notes in Computer Science), vol. 2567. New York, NY, USA: Springer-Verlag, 2003, pp. 18–30.

[11] S. Cui, P. Duan, C.W. Chan, and X. An efficient identity-based signature scheme and its applications,‖ *Int. J. Netw. Security*, vol. 5, no. 1, pp. 89–98, Jul. 2007.

[12] Q. Huang, D. S. Wong, and G. Yang, ―Heterogeneous signcryption with key privacy,‖ *Comput. J.*, vol. 54, no. 4, pp. 525–536, Apr. 2011.

[13] Y. Sun and H. Li, ―Efficient signcryption between TPKC and IDPKC and its multi-receiver construction,‖ *Sci. China Inf. Sci.*, vol. 53, no. 3, 557–566, Mar. 2010.

[14] 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.

[15] 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.