IOSR Journal of Electronics and Communication Engineering (IOSRJECE)
ISSN : 2278-2834 Volume 2, Issue 4 (Sep.-Oct. 2012), PP 05-09
www.iosrjournals.org

A Security Framework for Wireless Sensor Networks: IBE-Trust

[1]Malathi V, [2]Dr. B Sivakumar
[1] PG Student, Bangalore
[2]Professor & H.O.D, Dept. Of Tce, Dr A.I.T, [2]bangalore

Abstract: *The importance of key management protocol in ensuring secure communications in WSN is undeniable. This paper presents an IBE-Trust security framework utilizing the well-known identity based encryption scheme not to only establish secure communications but to ensure the trustworthiness of the communication between sensor nodes and base station. The framework incorporates ideas from Trusted Computing Group (TCG) and the Identity based cryptosystem developed by Boneh Franklin in ensuring trusted and secure communications between sender and receiver. The framework and proposed implementation procedures are briefly discussed. The proposed framework which was developed on TinyOS platform was simulated using TOSSIM on Micaz nodes and a study was carried out to compare memory utilizations of the proposed security framework with those obtained in a recent similar work.*

I. Introduction

Wireless Sensor Networks (WSN) is proven to be a useful technology especially in the area of data gathering and monitoring. As consequences, the technology has been applied in many areas ranging from basic temperature measurement to complex applications such as in health and medical and military. Security issues related to Wireless Sensor Networks (WSN) is therefore a must in ensuring the credibility of WSN applications and its services. Until recently, majority of works on securing WSNs relied on symmetric cryptography. Although its overall efficiency is better than asymmetric cryptography or public key cryptography (PKC), the symmetric key distribution scheme is unable to provide the level of security offered by public key based systems. As such there is a growing interest within the research community to look for possibilities of reducing energy consumption of public key cryptography, to make it feasible for energy constrained environments such as WSNs.

The Elliptic Curve Cryptography (ECC) which is based on random elliptic curve has been found feasible for WSNs [1- 3]. It has been proven to provide the same level of security offered by an RSA-based system with a large modulus with a much smaller key size thus reducing storage and transmission requirements.

II. Key Distribution Scheme

1.1 ID-Based KeyAgreement Scheme

ID based key agreement scheme is based on an Elliptic Curve Cryptography (ECC) type algorithm.IBE has simplified the certificate based public key encryption scheme, in certificate based public key scheme, a user has to verify another user's certificate before his/her public key can be used. This of course induce large memory and high computing time to store and to verify others certificate.

In IBE, an arbitrary string is used as a public key. Public key can be calculated from any string such as email, project name or any other string. No CA is needed to extract the certificate. One main characteristic that differentiates IBE from other server-based cryptographic is the communication-less with the server during encryption operation where the sender only needs to know the recipient's ID for it to encrypt the message.

IBE scheme consists of four algorithms which is explained below:

a) Setup – This process should be done by Trusted Agent (TA). In WSN, TA can be the Base Station (BS). Input a security parameter *k,* BS will generate global parameters and master key.
b) Extract- Is executed at BS or Sensor node. Input string ID (public key ID) and used master key to generate private key. The public key can be a combination of date or department or group name and unique string.
c) Encrypt – encrypt message using receiver ID and public parameters and finally
d) Decrypt – decrypt message using recipient's private key.

III. Fundamentals of IBE Algorithm

This section describes some basic mathematical properties which are useful to understand and our work will only involve the key management technique without modifying any mathematical equations. Using Bilinear pairing, $\hat{e} : G_1 * G_1 \rightarrow G_2$ in which G1 is a group on elliptic curve $y^2 = x^3 + 1$ over Fp with order q and G2

is a group on finite field with the same order. Elliptic curve point P is a random number generator of G1. The public system parameters are (q, G1, G2, e, n, P, Ppub, H1, H2) and are generated after the setup process.

During the extract process, H_1 which is a cryptographic hash function will hash the input identity to a point on elliptic curve: $\boldsymbol{QIDx = H_1(IDx)}$ and calculate the private key: $\boldsymbol{dID = sQID}$ where $\boldsymbol{s}$ is a master-key and is based on random number integer.

In the encryption process, the message $\boldsymbol{M}$ is encrypted with the encryption function:

$\boldsymbol{E(Ppub, A, M) = (rP, M \oplus H2(gA^r))}$ to produce cipher a ciphertext $\boldsymbol{c = (u, v)}$. **(A**= receipient ID and $\boldsymbol{u}$ and $\boldsymbol{v}$ are the ciphertext key and ciphertext message respectively**)**. Decryption process will decrypt the cipher text with the function: $D(u, v, sQ(H_1(A)) = v \oplus H_2(e(d_A, u))$

IV. Conclusion

Performance enhancement in security implementation is achievable in many ways. Determining the level of security needed for the intended applications should be the very first step. By looking into this issue carefully, the user can determine the type of cryptography needed (symmetric or public key), the minimum number of bits required to secure the applications, one time pad and other security features. As security level increases linearly with memory and power consumption, the level of security should be agreeable to that which is required in the intended applications. This work proposed a high-level security framework for applications which deals with information such as crucial financial information, noncritical military communications, medical data, and critical corporate information. This paper focuses on trusted key management scheme. New IBE scheme has been proposed to minimize workload on the sensor node platform thus increasing its lifespan. Security features have been enhanced by introducing trusted authentication mechanism in the IBE framework. This mechanism ensures the integrity of the data received in the data centric environment. Future work will be focused on implementation of IBE-trust framework and validating the framework using formal methods.

V. Results

Fig 1: Initial Topology

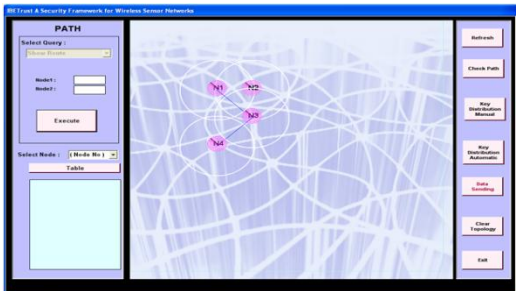


Fig 2: Creating Node and Checking Path

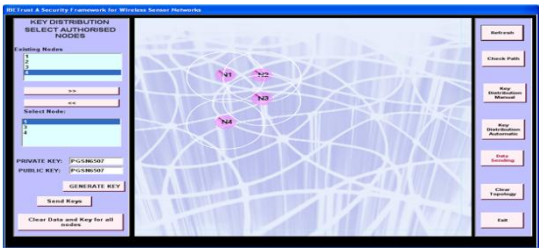


Fig 3: Key Distribution

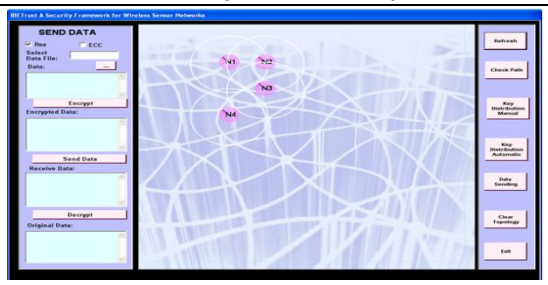


Fig 4: Browsing For Input Data

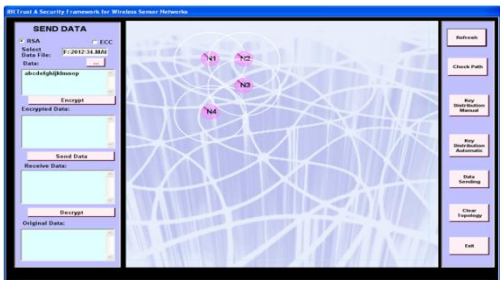


Fig 5: Providing Data to Encrypt

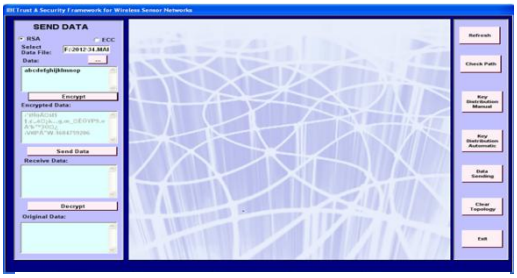


Fig 6: Encrypted Data

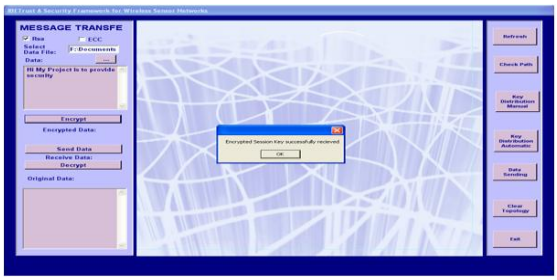


Fig 7: Encryption Session Successful

Fig 8: Authentication Step

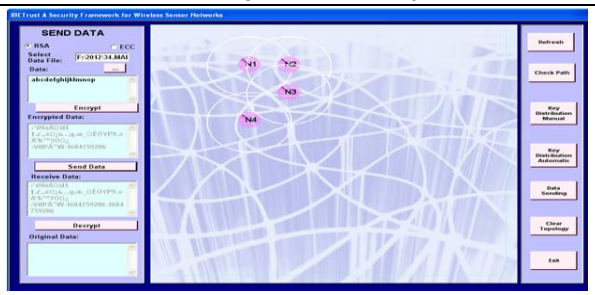


Fig 9: Sending Data to Decrypt

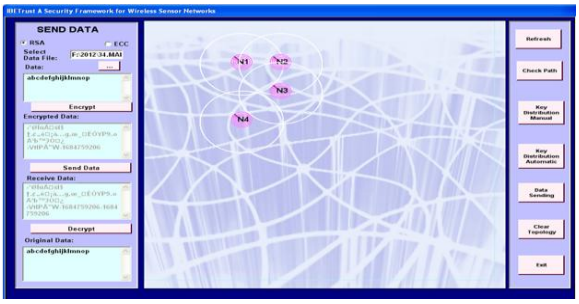
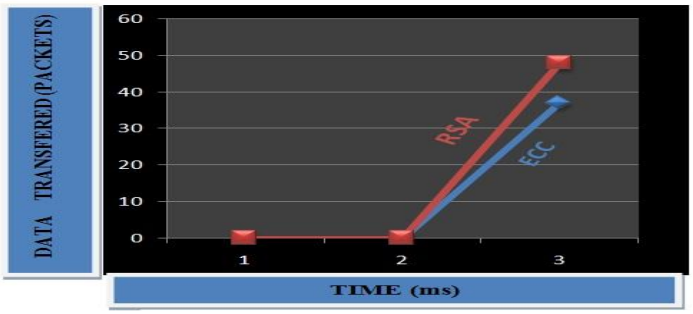


Fig 10: Decrypted Data



ECC: ELLIPTIC CURVE CRPTOGRAPHY
RSA: RIVEST SHAMIR ADLEMAN

Fig 11: Transmission Time

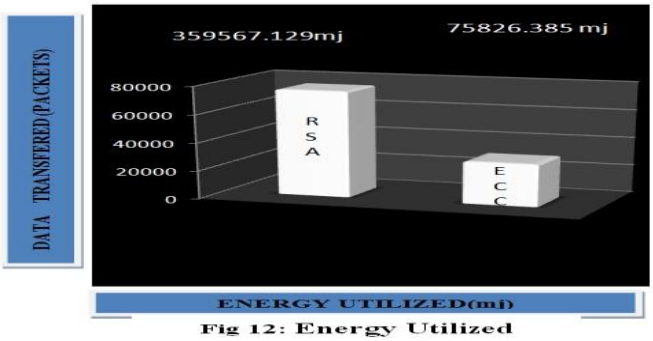


Fig 12: Energy Utilized

Comparison of RSA and ECC Algorithm

SL. NO	Algorithm	Energy Utilized (mj)	Transmission Time(ms)
1.	RSA	359567.1291	32.9013
2.	ECC	75826.3851	37.0043

References

[1] N. Gura, A. Patel, A. Wander *et al.*, *Comparing Elliptic Curve Cryptography and RSA on 8-Bit CPU*: Spingler Berlin, 2004.

[2] D. J. Malan, M. Welsh, and M. D. Smith, "A Public key Infrastructure for key Distribution in Tiny-OS based on Elliptic Curve Cryptography," in First IEEE Conference on Sensor and Ad Hoc Communications and Neworks, California, pp. 71-80,2004

[3] A. S. K. Pathan, and H. Choong Seon, "Feasibility of PKC in resource-constrained wireless sensor networks," in Computer and Information Technology, 2008. ICCIT 2008. 11th International Conference on, pp. 13- 20,2008.

[4] A. Shamir, "Identity-based cryptosystems and signature schemes," *Advances in Cryptology- Crypto84*, vol. 196, pp. 47, 1984.

[5] D. Boneh, and M. Franklin, "Idenetity-based encryption from weil pairing," *Advance in cryptology-crypto*, vol. 2139, pp. 29, 2001.

[6] J. Zhang, and V. Varadharajan, "Wireless sensor network key management survey and taxonomy," *Journal of Network and Computer Applications*, vol. In Press, Corrected Proof, 2009.

[7] R. Watro, D. Kong, S.-F. Cuti *et al.*, "TinyPK: Securing Sensor Networks with Public Key Technology," in 2nd Workshop on Security of Ad Hoc and Sensor Networks SASN'04, Washinton DC, USA, pp. 59-64,2004.

[8] L. Martin, G. Appenzeller, and M. Schertler, "RFC5408 - Identity-Based Encryption Architecture and Supporting," Network working Group, 2009.

[9] G. Yang, C.-m. Rong, C. Veigner *et al.*, "Identity-based key agreement and encryption for wireless sensor networks," *The Journal of China Universities of Posts and Telecommunications*, vol. 13, no. 4, pp. 54-60, 2006.

[10] G. Zhi, S. Huiping, C. Zhong *et al.*, "Efficient Identity-Based Key Issue with TPM," in Young Computer Scientists, 2008. ICYCS 2008. The 9th International Conference for, pp. 2354- 2359,2008.

[11] ym_yussoff, and H. Hashim, "Trusted Wireless Sensor Node Platform," in International Conference on Wireless Network, London, United Kingdom, 2010.

[12] P. Chandra, A. Bensky, J. S. Wilson *et al.*, *Wireless security : Know it all*: Elsevier, 2010.

[13] D. Grawrock, *Dynamics of a Trusted Platform*: Intel Press, 2009.

[14] T. G. Roosta, "Attacks and defenses of ubiquitous sensor networks ", Electrical Engineering, University of California, Berkeley, 2008.

[15] L. B. Oliveira, D. F. Aranha, E. Morais *et al.*, "TinyTate: Computing the Tate Pairing in Resource-Constrained Sensor Nodes," in Network Computing and Applications, 2007. NCA 2007. Sixth IEEE International Symposium on, 2007, pp. 318-323.[16] P. Szczechowiak, A. Kargl, M. Scott *et al.*, "On the application of pairing based cryptography to wireless sensor networks," in Proceedings of the second ACM conference on Wireless network security, Zurich, Switzerland, 2009.

[17] X. Xiaokang, D. S. Wong, and D. Xiaotie, "TinyPairing: Computing Tate Pairing on Sensor Nodes with Higher Speed and Less Memory," in Network Computing and Applications,2009.Eighth IEEE International Symposium on, 2009, pp. 187-194,2009.

[18] X. Xiaokang, D. S. Wong, and D. Xiaotie, "TinyPairing: A Fast and Lightweight Pairingbased Cryptgraphic Library for Wireless Sensor Network," in IEEE Wireless Communication and Networking Conference, Sydney, Australia, 2010.