Survey on Homomorphic Cryptography Schemes in Wireless Sensor Network

Hrishikesh Kad[1], Dr.S.T.Singh[2]
[1, 2] P.K.Technical Campus, ChakanPune, Maharashtra, India

Abstract-*This paper represents a review of homomorphic cryptography techniques used in wireless sensor net-work. By performing operations on encrypted data, we can preserve privacy in wireless sensor network. In this paper we represent a research on Homomorphic cryptographic techniques used in various areas. This research will help in further research on privacy of wireless sensor network.*

Keywords-Encryption, Homomorphic cryptography, security, privacy

I. INTRODUCTION

1.1 Introduction to Wireless Senor Network and its use in various application:

Fig.1. shows architectural view of wireless sensor network. A wireless sensor network [1] is a collection of sensor nodes which communicate with one another to form a network.
The equation of WSN is:
Sensing power+processor+radio=possible applications.

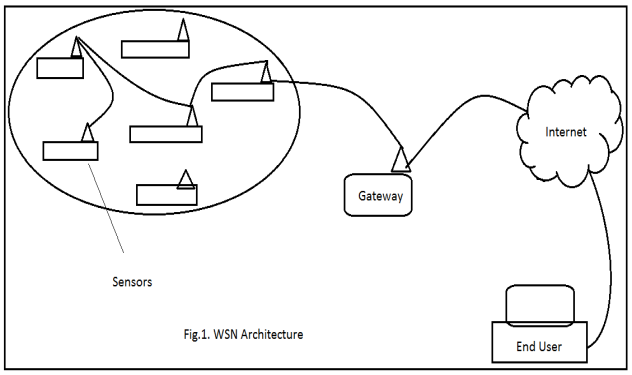

Fig.1. WSN Architecture

Wireless sensor network can be used in many areas [2]. Wireless sensor network can be Underwater, Underground, Terrestrial, Multi-media Wireless sensor network, Mobile Wireless sensor network. These sensor networks are used in many applications like security, monitoring, biomedical research, tracking etc.

These applications are divided into many classes like used in hospitality ,animation, police work, aerial data gathering, automotive applications, environmental, Environmental Military applications, data collection, Security monitoring, Wildfire detection, sensor node tracking, health application, home application, and hybrid networks. Some years ago wireless sensor network was used in only security things like only in military to detect nuclear and chemical attacks , to monitor friendly forces and equipment's but after wide research in WSN , now wireless sensor network can be used in outdoor as well as indoor applications. Role of wireless sensor network in agriculture is very important and useful. Now various machinery in the agriculture in automated which increase productivity and reduces manual work. In hospital, wireless sensor network can be used in the monitoring of glucose level, in the treatment of heart patient etc.

Wireless sensor network is also used in environmental data collection operation used to collect various sensor data in a particular period of time. In disaster relief operation also wireless sensor network is used in wildlife detection by dropping sensor nodes from aircraft over wildlife. Wireless sensor network is also used in vehicle telemetries by providing better traffic control by obtaining finer-grained information about traffic conditions. WSN is also used in home applications like TV, air conditioner.

Wireless can be used in various application [3] but to implement it and to manage it will addressed many challenges. Challenges are : To provide quality of service(QOS),Maintainability,Automotive,privacy,Security,Integrity,Energy-efficient operation, locality, programmability, wide range of density.

a. Integrity: Wireless sensor network does not mean simply transferring data from one place to other, data should be meaningful. E.g. Data should be transfer within a specific time of interval or in the specific region only.
b. Quality of Service: QOS play major role in transferring video, audio and images.
c. Lifetime: Lifetime of sensing node.
d. Fault tolerance: Sensor nodes can be fail because of unintended environment. Protocols and algorithms should be ready to handle these kind of situations.
e. WSN should work and support a large number of sensors.
f. Maintainability: Maintenance of WSN nodes and other devices over changing requirements.

g. Security: An effective and efficient compromise should be achieved, between security demands for secure communication and low bandwidth required for communication in sensor network.

1.2 Role of encryption in security:

Security is an essential requirement in wireless sensor network because of increasing usage of internet for saving of data.

Security is required for preserving privacy of data, integrity, confidentiality and availability of resources data.

To send a data from one source to other there are many security level issues occurs like

Sybill Attacks: In this attack, a malicious node can get different identities and take advantage of legimate nodes.

Denial of Service Attacks: Denials as malfunctioning sensors by malicious action.

Data Corruption attacks: The attacker modify, repeat or delay the content of data transferred.

Physical Attacks: If WSN are deployed in an area where there is not protection, then chances of this attack.

To preserve from these attacks, sending encrypted data from one source to other is essential.

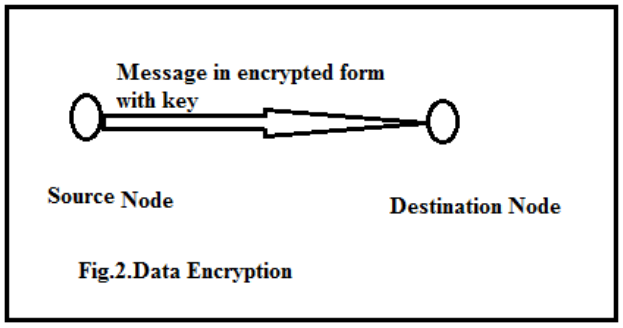

Fig.2.Data Encryption

1.3 Need of Homomorphic Cryptography in WSN

To outsource a large amount of data storage and management activities to third party cloud services raises many privacy issues for individuals and business companies. The privacy concern of this stored data can be addressed if we store data in the encrypted form and users can perform operations on encrypted data. Homomorphic cryptography allows to perform operations on encrypted data. Because of this business can reduce their task of maintaining data at data centers.

Data can be stored in encrypted form at database level. To perform any computation or mathematical operation on encrypted data needs to decrypt the data in normal plain text form but the decrypted data are not secure any more.

To work on encrypted data without converting it to plain text, we use Homomorphic cryptography.

1.4 Definition of Homomorphic Cryptography:

Homomorphic Cryptography allows to perform simple mathematical operations on encrypted data which is stored at database or at node level.

Homomorphic encryption is an encryption scheme where plaintext Pl and cipher text Cr is bind together such that for any key Ky

Cr1 = eKy(m1), Cr2 = eKy(m2), the following condition holds: dKy(cr1 · cr2) = m1 · m2 where · represents the respective group operations in C and M.

Homomorphic Cryptography (HC) Operations[4]:

Homomorphic cryptography includes following four operations:

a. Key establishment and key generation:
   Generate public key(P) and private key(S).
b. Data encryption:
   Encrypt data D using private key which forms E(D). E(D) along with public key , this cipher text data is sent to another node by source node.
c. Data storage: Encrypted data can be stored at DB.
d. Mathematical computation: Thirty party services access the data from DB and perform mathematical operations on it without decrypting data.

II. REVIEW OF HOMOMORPHIC TECHNIQUES

Privacy Homomorphism:

Rivest, Adleman, and Dertouzous [5] proposed first time idea to perform simple computation on encrypted messages, which is known as privacy homomorphisms. The aim for privacy homomorphisms was to allow for an encrypted database to be stored by an untrusted third party, while allowing to owner to perform simple queries without knowing database contents to the third party.

Definition:
φ = decryption key, while the algebraic system U is kept private, and the algebraic system C is made public.

Example:
Assume a user wants to calculate g1(k1,k2) from a set of database values stored by a third party at DB level, without knowing g1.
The user submits a request for g0 1(φ−1(k1),φ−1(k2)), and, upon receiving the response,
Calculates
φ(g01(φ−1(k1),φ−1(k2)))=g1(φ(φ−1(k1)),φ(φ−1(k2)))
……. (By Property 1) = g1(k1,k2).

RSA Cryptography:

RSA cryptosystem [6] by Rivest, Shamir, and Adleman, is a public-key crypto systems.
Definition: Let b and c be two primes, and define a = bc. Also, let P = L = Za, and define

$M = \{(a,b,c,d,e)|de \equiv 1 \bmod \varphi(a)\}$
where φ is the Euler totient function.
For K = (a,b,c,d,e),
define
$e_k(x) = x^e \bmod a$ and
$d_k(y) = y^d \bmod a$ for $x \in P$ and $y \in L$.

The tuple (e,a) is made public, and the tuple (b,c,d) is kept private.
The RSA cryptosystem works because the values e and d are inverses modulo φ(a).

$$d_k(e_k(x)) = (x^e)^d \bmod a$$
$$= x^{ed} \bmod a$$
$$= x^{edmod\varphi(a)} \bmod a$$
$$= x^1$$
$$= x$$

In the above RSA cryptosystem, there is difficulty of calculating e'th roots modulo a, where a = bc for distinct odd primes b and c, when the factorization of c is unknown. Limitation of this is we are able to successfully factoring a, that is sufficient to break RSA.

Brown [7] demonstrated a result in the opposite direction; namely, it was shown that there is no e□cient algorithm that takes a small public RSA exponent and outputs a straight line program that solves the RSA Problem, unless factoring is easy.
Definition:

The RSA cryptosystem provides the basic homomorphic operation of multiplication modulo a.
Given two cipher texts $c_1 = m_1^e \bmod a$
$c_2 = m_2^e \bmod a$, then
$c_1c_2 \bmod a = m_1^e m_2^e \bmod a = (m_1m_2)^e \bmod a$ is an encryption of m_1m_2.

2.3 The Goldwasser-Micali Cryptosystem

The Goldwasser-Micali (GM) cryptosystem [8] isthe first probabilistic cryptosystem proposed.

Definition:
GM cryptosystem is a probabilistic cryptosystems as well as provides the homomorphic operation of XOR, or addition modulo 2.
Consider two cipher texts encrypted under the simplified GM cryptosystem,
$c_1 = -1^{x1}r_1^2$ and $c2 = -1^{x2}r_2^2$.
Then $c_1c_2 = (-1^{x1}r_1^2)(-1^{x2}r_2^2)$
$= -1(x_1+x_2)(r_1r_2)^2$
$= -1(x_1+x_2 \bmod 2)(r_1r_2)^2$
is an encryption of $x_1 + x_2 \bmod 2$.
The GM cryptosystem also allows for a cipher text to be re-randomized without knowledge of the plaintext. Given $c = -1xr_1^2$, choose a random integer $r_2 \in Z* n$ uniformly. Then the integer $r_3 = r_1r_2 \bmod n$ is a uniform random integer in $Z* n$ and $cr_2^2 = -1xr_1^2r_2^2$
$= -1xr_3^2$ is a random encryption of x.

2.4 The ElGamal Cryptosystem

The ElGamal cryptosystem [9] is a public-key cryptosystem based on the problem of solving discrete logarithms.

Definition: The ElGamal cryptosystem provides the homomorphic operation of multiplication of two encrypted messages, as well as multiplication by a known constant and exponentiation by a known constant.

Given ciphertexts (c_1,c_2) and (d_1,d_2) that are encryptions of m1 and m2, using random values y1 and y2, respectively, then
$(c_1d_1,c_2d_2)=(gy_1gy_2,(m_1 \cdot hy_1)(m_2 \cdot hy_2))$
$= (g^{y1+y2},m_1m_2 \cdot h^{y1+y2})$
is a valid encryption of m_1m_2.
Furthermore, given a constant k, then (c1,kc2) = $(g^{y1},km1 \cdot hy1)$ is a valid encryption of km_1.

2.5 The Benaloh Cryptosystem

The security of the Benalohcryptosystem[10] is based on the difficulty of deciding r'th residues, much like the GM cryptosystem is based on the di□culty of deciding quadratic residues.

The Benaloh cryptosystem supports the homomorphic addition and subtraction of ciphertexts.
Given two ciphertexts $c_1 = y^{m1}u_1{}^r$ and $c2 = y^{m2}u_2r$,
$c_1c_2 \bmod n = (y^{m1}u_1{}^r)(y^{m2}u_2r) \bmod n$
$= y^{m1+m2}(u_1u_2)r \bmod n$ is a valid decryption of $m_1 + m_2$,
And
$c_1c_2{}^{-1}\text{mod}n=(y^{m1}u_1{}^r)(y^{m2}u_2r)^{-1}\text{mod}n$
$=(y^{m1}u_1{}^r)(y^{-m2}(u_2{}^{-1})^r)\text{mod } n$
$= y^{m1-m2}(u_1u_2{}^{-1})^r \bmod n$ is a valid encryption of $m_1 - m_2$.

2.6 The Naccache-Stern Cryptosystem:

The Naccache-Stern cryptosystem[11] allows for the homomorphic addition and subtraction of cipher texts, as well as multiplication of a cipher text by a constant.
Examples for the probabilistic variant are provided, but work equivalently for the basic cryptosystem.
Given two cipher texts $c_1 = g^{m1}x_1{}^\sigma \bmod n$ and $c2 = g^{m2}x_2{}^\sigma \bmod n$ as valid encryptions of m_1 and m_2 respectively, then $c_1c_2 \bmod n = g^{m1}x_1{}^\sigma\, g^{m2}x_2{}^\sigma \bmod n = g^{m1+m2}(x_1x_2)^\sigma \bmod n$ is a valid encryption of $m_1 + m_2$.

2.7 The Sander-Young-Yung Cryptosystem

In Sander-Young-Yung cryptosystem [13], cipher text can be efficiently re-randomized by taking the component-wise product with an encryption of 0 under the SYY cryptosystem.

Given two cipher texts x and y as encryptions of m1 and m2 respectively, an encryption of m1 ·m2 can be calculated by first choosing two random non-singular matrices $A,B \in (Z_2)^{l\times l}$, and then calculating c = Ax + By

$$c_i = \left(\prod_{\substack{j \\ a_{i,j}=1}} x_j\right)\left(\prod_{\substack{j \\ b_{i,j}=1}} b_{i,j}\right)$$

2.8 The Okamoto-Uchiyama cryptosystem [12]:

It is a public-key cryptosystem based on the di□culty of the factoring problem.

This cryptosystem supports the homomorphic addition and subtraction of two cipher texts, addition and multiplication by a known constant, and efficient re-randomization of cipher texts. Given $c_0 = g^{m0}h^{r0}$ and $c_1 = g^{m1}h^{r1}$ as valid encryptions of m_0 and m_1 respectively,
$c_0c_1 = g^{m0+m1}h^{r0+r1} \bmod n$ is a valid encryption of $m_0 + m_1$ with randomness $r_1 + r_2$

2.9 The Paillier Cryptosystem:

The Paillier cryptosystem [14] supports homomorphic addition and subtraction of encrypted messages, as well as addition and subtraction of constants, and multiplication by a constant. Let $c_1 = g^{m1}y_1{}^n \bmod n^2$ and $c_2 = g^{m2}y_2{}^n \bmod n^2$. Then $c_1c_2 \bmod n^2 = g^{m1}y_1{}^n\, g^{m2}y_2{}^n$
$= g^{m1+m2}y_1y_2{}^n \bmod n^2$ is a valid encryption of $m_1 + m_2$,
$c_1g^k \bmod n^2 = g^{m1}y_1{}^ng^k = g^{m1+k}y_1{}^n \bmod n^2$ is a valid encryption of $m_1 + k$

III. DISCUSSION AND REMARKS

Many people work on preserving privacy of data. Many people has proposed various homomorphic algorithm in many areas. But as per the survey only few people proposed use of homomorphic encryption techniques in wireless sensor network.

IV. CONCLUSION

This paper represents existing homomorphic encryption techniques in various areas. This research mainly concentrates on use of homomorphic encryption algorithm to protect data privacy. Each technique has its own pros and cons, this will help us in designing new encryption algorithm in wireless sensor network.

REFERENCES

[1] W. Dargie and C. Poellabauer, "Fundamentals of Wireless Sensor Net- works: Theory and Practice, Wiley, 2010.
[2] Kiran Maraiya, Kamal Kant, Nitin Gupta," Applica-tion based Study on Wireless Sensor Network", in In-ternational Journal of Computer Applications (0975 – 8887)Volume 21– No.8, May 2011
[3] Prakhar Gupta, MeenuChawla ,"Privacy preserva-tion for WSN: A Survey", in International Journal of Computer Applications (0975 – 888) Volume 48– No.3, June 2012
[4] PayalV.Parmar,"Survey of Various Homomorphic Encryption algorithms and Schemes", in International Journal of Computer Applications (0975–887)Volume 9 1 –No.8, April 2014

[5] Richard. A. Demillo, David P. Dobkin, Anita K. Jones, and Richard J. Lipton, editors, “Foundations of Secure Computations”, pages 169–177. Academic Press, New York, 1978. 1, 10

[6] Ronald L. Rivest, Adi Shamir, and Leonard M. Adleman. “A method for obtaining digital signatures and public-key cryptosystems” in. Commun. ACM, 21(2):120–126, 1978.

[7] Dan Brown. “Breaking RSA may be as di□cult as factoring” in Technical Report CACR 2005-37, Center for Applied Cryptographic Research (CACR): Universi-ty of Waterloo, 2005. 33

[8] ShafiGoldwasser and Silvio Micali. “Probabilistic encryption’ in J. Comput. Syst. Sci., 28(2):270–299, 1984. 6, 33

[9] Taher El Gamal. “A public key cryptosystem and a signature scheme based on discrete logarithms”. In G. R. Blakley and David Chaum, editors, CRYPTO 1984, volume 196 of Lecture Notes in Computer Science, pages 10–18. Springer, 1984. 35

[10] Josh Benaloh. Dense “probabilistic encryption”. In Selected Areas of Cryptography (SAC 1994), pages 120–128, 1994. 38, 39

[11] David Naccache and Jacques Stern. “A new public key cryptosystem based on higher residues”. In ACM Conference on Computer and Communications Securi-ty, pages 59–66, 1998. 40, 43

[12] Tatsuaki Okamoto and Shigenori Uchiyama. “A new public-key cryptosystem as secure as factoring”. In Nyberg [75], pages 308–318. 46, 47, 48, 49

[13] Tomas Sander, Adam Young, and Moti Yung. “Non-interactive cryptocomputing for NC1”. In FOCS 1999, pages 554–567. IEEE, 1999. 44, 102, 110

[14] Pascal Paillier. “Public-key cryptosystems based on composite degree residuosity classes”. In Stern [97], pages 223–238. 27, 29, 51, 53, 55