Use of Key Distribution Techniques with Homomorphic Cryptography in Wireless Sensor Network

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

Abstract-*In this paper we have used two key distribution techniques named as pairwise and triple key distribution scheme and encryption technique homomorphic cryptography. In wireless sensor network data is very crucial as we need to transfer data and information among different sensor nodes. Therefore to have data secure, maintaining privacy of data is very important. To achieve this, we have used various cryptography based schemes. As a part of data operation, we came to know that in WSN we performed mathematical operations on the data which we transferred between different nodes. As per the research done till now we have observed that regular cryptography schemes are not useful to pre-serve privacy of data. Homomorphic scheme can be used to perform mathematical operations on encrypted data which transferred between different nodes. Aim of this paper is to use key distribution techniques to established connection between different nodes and then to perform operation's on encrypted data which we are sending between different nodes. To achieve this, use homomorphic cryptography.*

Keywords-homomoprhic cryptography, Key Distribution, pairwise key distribution, triple key distribution.

I. INTRODUCTION

A wireless sensor network is a collection of sensor nodes which has resource limitations such as battery power, storage and communication capability. This collection of sensor nodes use radio interface to communicate with one another to form a network. This network plays an important role in many applications like Environmental Military applications, data collection, security monitoring, wildfire detection, sensor node tracking, health application, home application etc.

Various key distribution schemes are used in wireless sensor network like random pairwise key distribution scheme, grid-based key distribution scheme, group based key distribution scheme, key distribution using combinatorial design. In our paper, we use simultaneous pairwise and triple key distribution using combinatorial design. Combinatorial design structure has its own advantages like unique key generation, fast calculation, no repetition of key. In pairwise key distribution only one key is used to secure unicast communication between a pair of sensor nodes over single or multi-hop wireless link and in triple key distribution also one key is used to secure unicast communication between three sensor nodes over single or multi-hop wireless link. We are simultaneously using pairwise and triple key distribution, when there are two nodes in which communication is performed then pairwise key distribution is used and when there is a condition in which three nodes communication is required (e.g. parent node wants to take data from two child nodes) then triple key distribution is used to generate only one key for three nodes.

When key distribution is done to maintain privacy of data and other information which is transferred between the nodes we are use homomorphic cryptography. Homomorphic cryptography provides a third party with the ability to perform simple computations on encrypted data without revealing any information about the data itself. Typically, a third party can calculate one of the encrypted sums or the encrypted product of two encrypted messages. This is possible due to the fact that the encryption function is a group homomorphism, and thus preserves group operations. This makes homomorphic cryptosystems useful in a wide variety of privacy preserving protocols. A homomorphic cryptosystem is a cryptosystem where the set of possible plaintexts P and the set of possible ciphertexts C are both groups such that for any $K \in K$ and any two ciphertexts $c1 = eK(m1)$, $c2 = eK(m2)$, the following condition holds: $dK(c1 \cdot c2) = m1 \cdot m2$ where represents the respective group operations in C and M.

Mitchel and Piper [19] were the first to use combinatorial designs in key distribution and Camtepe and Yener [20], [21] applied combinatorial designs for key predistribution in WSN. A set system can be used to a key predistribution scheme in the following way. Let (X,A) be the set system with elements from set X, where A is a set of subsets with elements from X. The subsets belonging to A are also called blocks (or key chains) of the design. The pool of key identifiers is the set X. A special type of design is Balanced Incomplete Block Design, BIBD [22], with the parameters v, b, r, k and λ, where $v = |X|$, b is the number of subsets of A or blocks, r is the number of blocks in which a

particular element occurs, k is the size of each subset, λ is the number of blocks in which a given pair of elements occur. Following this design, each sensor is loaded with k keys along with their identifiers. The keys are chosen from a pool of v keys. Any pair of keys can occur in precisely two nodes. If K1 and K2 are two keys shared by nodes A and B then the common unique pairwise key is hash(K1||K2||idA||idB).Also for three nodes D,E and F, unique triple key is calculated by hash(K1||K2||K3||idA||idB||idC).

A. Own Contributions

When we distribute keys using pairwise and triple key distribution, to maintain privacy of data which is being transferred between different nodes in network and perform mathematical computation on the encrypted data transferred, we are using homomorphic cryptography.

Homomorphic encryption techniques allows mathematical computations on data which is in encrypted form for a long time. A homomorphic cryptosystem is a cryptosystem where the set of possible plaintexts PL and the set of possible ciphertexts CL are both groups such that for any K ∈ K and any two ciphertexts cl1 = $e_1K(m1)$, cl2 = $e_1K(m2)$, the following condition holds: dK(cl1 · cl2) = m1 · m2 where · represents the respective group operations in C and M.

II. SURVEY DETAILS

In this section we discuss existing pairwise key management and key distribution techniques and various existing privacy preserving techniques in wireless sensor network.

A. key distribution in wireless sensor network-

In[4] *L. Eschenauer et.al. proposed a random pairwise scheme*. In this approach, a key ring for a node containing some fixed number of keys is chosen randomly. Node is assigned a key ring. The key identifiers of a key ring and corresponding sensor identifiers are stored in a trusted controller node. If there exists a path of nodes sharing keys pairwise between those two nodes, they may communicate via that path. This scheme is flexible, scalable and easy to use but not used in regions which are prone to massive node capture attack. In [5]H. Chan et.alproposed a random pairwise key distribution using q-composite scheme. According to their q-composite scheme two nodes must share at-least q number of keys to have a secure path between them. The path key will be formed by the hash of all the common keys. This scheme improved resiliency but not scalable.

In[2] S. Ruj,et.al.represented various key predistribution techniques for single-hop networks and discussed their merits and demerits in terms of resiliency. In[1] R.Blom,et.al. proposed a key predistribution scheme that allows any two nodes of a group to find a pairwise key. The security parameter of the scheme is c.In[3] *C. Blundo also proposed a* key predistribution scheme that allows any two nodes of a group to find a pairwise key using symmetric bivariate polynomial.

In[6] Donggang Liu and Peng Ning et.al. proposed a pairwise key distribution using polynomial pool-based key predistribution. Two sensor nodes share some secret key if the keys are generated from the same polynomial. This scheme is good key resilence and scalable but Node has preloaded pairwise keys for C sensor nodes. In[3] Zhu, Shouhuai Xu et.al. proposed a scheme to establish pairwise keys using probabilistic key sharing and threshold secret sharing. This scheme enables any two nodes to establish a pairwise key on the fly, without the use of an online key pre-distribution center. Nodes find their pairwise keys only by knowing the key ids, and no key identifier list is to be broadcasted. Hence the communication overhead is minimized.

B. Privacy preserving techniques in wireless sensor network-

Various privacy preserving techniques are present in wireless sensor network. There are many attacks against the privacy. These privacy attacks are classified into two main categories and this shows why privacy preservation is needed in WSN. Categories are 1.Data oriented privacy and 2. Context oriented privacy

In[10] Jianbo Yao et.al. presents scheme for source location privacy in WSN. Author proposed a DROW (directed random walk) scheme for privacy of monitoring object when wireless sensor network is used to monitor the sensitive objects. In[11] George, C.M. et.al. proposed a recurrent cluster mechanism for location privacy. Author also described data-oriented and context-oriented privacy preserving techniques. Author used cluster mechanism for preserving privacy of information on location of events or on location of base stations. In[12]Sivashankari, S. et.al. have proposed techniques for source location privacy and sink location privacy. Periodic collection and source simulation are the techniques used to provide location privacy to monitored object and sink simulation and backbone flooding are techniques used to provide location privacy to data sinks. In[13]Spachos, P., Liang Song et. al. have presented opportunistic routing schemes for source location privacy in wireless sensor network. In this scheme each node sends a

packet to the destination using dynamic path therefore for an adversary to backtrack hop-by-hop to the origin of the sensor data. In[14]YaHui Li, Ding Yong et. al. have proposed secure message distribution scheme with configurable privacy for a heterogeneous wireless sensor network (HWSN).The characteristic of this scheme is user can only see a message that is intended for him and the sensor node can only generate one signature for all the messages for all the users, which can save the communication and computation costs of the sensor node. In[15]Shaikh, R.A.,Jameel, H. Et. al. have presented novel scheme for full network level privacy. For this author used Identity, Route and Location (IRL) privacy algorithm and data privacy mechanism. In[16] Yun Li,JianRen et.al. have presented novel scheme for source location privacy. Author represents routing to randomly select intermediate node/nodes before the message is transmitted to the sink node for maintaining privacy. In[17]WenboHe, Xue Liu et.al. represents two schemes - Cluster-based private data aggregation (CPDA) and Slice-Mix-AggRegaTe (SMART)for data aggregation privacy preservation. CDPA includes clustering protocol and algebraic properties of polynomials and SMART includes slicing techniques and associative property of addition.

In [8] JianboYao,Guangjun Wen et.al. have presented DADPP (Data Aggregation Different Privacy-Levels Protection)for data aggregation privacy for wireless sensor networks. Jianbo proposed DADPP used for different levels of data aggregation privacy. At different levels, nodes within the same cluster are divided into many groups and privacy levels are described for each group that is node belonging to same group having same privacy level. In[9]Jianbo Yao et.al. represents location privacy of mobile sink node in WSN. Author used this based on local flooding of source and greedy random-walk of sink which means that source does not have any information about sink and sink uses greedy random walk to collect data from other nodes which prevents predicting their locations and movements from attackers.

In[18] Yun Li,Jian RenSensor et.al. have proposed novel schemes for content confidentiality and source-location privacy through routing to a randomly selected intermediate node (RRIN) and a network mixing ring (NMR).RRIN provides local source- location privacy and NMR gives network-level (global) source- location privacy.In[19] Bista, R., Hye-Kyeom Yoo et.al. represents one mechanism for privacy preserving data aggregation. A sink node must be aware of the Ids of those all sensor nodes which contribute in aggregated value of sensors data in order to derive exact result. To solve this problem, a set of real numbers are assigned as the IDs of sensor nodes so that a single bit is sufficient to hold ID of a sensor node during transmission of aggregated data to the sink node In[20] Gurjar, A et.al. proposed a cluster based anonymization scheme for source location privacy. This scheme says hide the real node identities during communication, by replacing them with random identities generated by the cluster heads. In[21] Jian Ren et.al. have proposed a scheme to provide both content confidentiality and source-location privacy through routing to a randomly selected intermediate node. In[22] Oualha N.,Olivereau A et.al. have analyzed the existing approaches for privacy protection in WSNs and investigate the approaches that aim at supporting the integration of privacy-preserving WSNs into large scale industrial environments.

C. To perform mathematical computation on data we are using homomorphic cryptography-

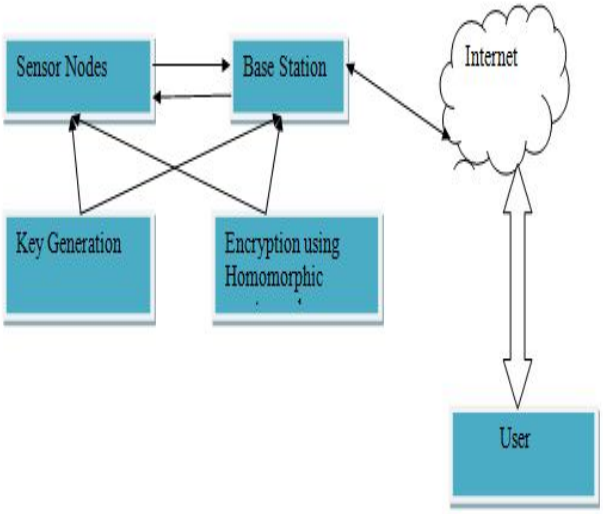
In[23]Kristin Lauter et.al. represented information about homomorphic.

A cryptosystem provides a method for transforming one message, called a plaintext, into another message, called a cipher text, using some secret key. If the cryptosystem is secure, then the cipher text can safely be made public, and no party without knowledge of the secret key can recover the plaintext. There are various types of cryptography techniques which have some drawbacks for example in the RSA cryptography, if two messages m1 = m2 are encrypted, then the resulting ciphertexts c1 and c2 are identical; i.e., encryption is a deterministic process. If the adversary observes an encrypted message c, it can easily be checked if c is an encryption of m by checking if eK(m) = c. An adversary could construct a database containing encryptions of all English words and common phrases, potentially allowing for many observed messages to be revealed. To protect against this sort of attack, it is often required that ciphertexts produced by a cryptosystem be indistinguishable. By this, it is meant that an adversary, given a single encryption of a known message chosen from the set {m0, m1}, should not be able to determine which message the cipher text represents with probability significantly greater than 1/ 2.

III. PROPOSED SYSTEM

A. Architecture

Fig. shows an architectural view of proposed system. Application data generation means data is transmitted between sensor nodes. Simulation data generation means preloaded data like key pool. First initial key distribution is done using pairwise and triple key distribution to preserve privacy and mathematical properties of data homomorphic cryptography is used.



B. Algorithm and Mathematical Model

Problem Definition: Use of key distribution techniques with homomorphic cryptography to preserve privacy in wireless sensor network.

1. Mathematical Model:

Let s = kl where k and l are large prime numbers
Thus,
$\varphi(s)=(k-1)(l-1) = |Z^*_j|$ ..... (1)
$\lambda(s)=lcm(k-1,l-1)$ .....(2)
$|Z^{*}_{s^2}| = \varphi(s^2) = j\varphi(s)$
$\forall x \in Z^{*}_{s^2}$
$\Longrightarrow$ $x^{\lambda(s)} \equiv 1 \bmod s$
$x^{s\lambda(s)} \equiv 1 \bmod s^2$
Let $g \in Z^{*}_{s^2}$
Eg : $Z_s \times Z_s^* \rightarrow Z_{s^2}^*$

Let N be the total number of sensor nodes. Let N_i be the sensor node where i = (1, 2, 3,....., N).

Let {Ni, t, (s_1,s_2,s_3,.....,sp)}be the tuple sent by node N_i to sink node S at time t and (s_1,s_2,s_3,.....,sp) are data values which are sent.
We formulate our problem as given N number of nodes who send tuples { N_i, t , (s_1,s_2,s_3,.....,sp)} to sink S preserve the privacy of stored data and yet allow to have mathematical operations or queries on it by user U.

2. Algorithm:

2.1 Key establishment Algorithm:

Suppose node *A* which has the identifier (*i, j, u*) wants to establish a pairwise key with *B* whose identifier is (*i_, j_, u_*). The following algorithm runs in node *A*.
Algorithm 1 Pair-wise key establishment algorithm
Input: Identifier (*i_, j_, u_*) of *B*

Output: Pairwise key between *A* and *B* if one exists, and NULL if none exists

Step 1. **if** $u = u\_$ **then**
Step 2. Print "No common key"
Step 3. Return NULL
Step 4. **else**
Step 5. $y = ((i - i\_)2 + 4(j - j\_)) \bmod q$
Step 6. **if** $\sqrt{y}$ exists, **then**
Step 7. $x1 = (i-i\_)+\sqrt{y} \pmod q$
Step 8. $x2 = (i-i\_)-\sqrt{y} \pmod q$
Step 9. **if** $x1 < k$ and $x2 < k$ **then**
Step 10. $XAB = K(x1,x1i+j)||K(x2,x2i+j)$
Step 11. $KAB = hash(XAB||idA||idB)$
Step 12. Return *KAB*
Step 13. **else**
Step 14. Print "No common key"
Step 15. Return NULL
Step 16. **end if**
Step 17. **else**
Step 18. Print "No common key"
Step 19. Return NULL
Step 20. **end if**
Step 21. **end if**

2.2 Use of Homomorphic cryptography to preserve privacy:

Step1. Node N_i creates data value tuple {Ni, t, (j_1,j_2,j_3,.....,jp)} after sensing data.

Step 2. Node N_i uses key generation for generating keys by selecting l as security parameter and then it selects two randomly m bit prime numbers k,l and sets j=kl. It then selects random base g∈B

Step 3.Node N_i then encrypts data values (j_1,j_2,j_3,.....,jp) by using following formula
Cipher text $C= g^m m^d \bmod j^2$
Where m is random value $m \in Z^*_j$

Step 4.Node N_i then forms tuple {Ni, t, (c_1,c_2,c_3,.....,cp)}

Where (c_1,c_2,c_3,.....,cp) is the set of encrypted data values.

Step 5.User U sends queries to sink and sink can perform queries and mathematical operations on values without revealing plaintext.

IV. ANALYTICAL RESULT

This section describes analytical result of proposed scheme.

Below parameters have been considered for the same:

A. Resilience of our scheme

B. Time taken for encryption

Amount of time taken to encrypt the data.

C. Connectivity of the network

D. Time complexity

V. CONCLUSION AND FUTURE WORK

We use cryptography in wireless sensor network to protect data but there are many issues in key distribution of wireless sensor network. This paper represents a scheme where we implements two key distribution techniques for initial key distribution. To maintain privacy of data and mathematical properties we develop privacy preserving scheme using homomorphic cryptography. As homomorphic scheme is very slow, future work will be resource improvement.

ACKNOWLEDGEMENTS

I would like to thank my guide for her help and support during my studies. I would also like to thank all teachers and principal, for their helpful suggestions.

REFERENCES

[1] R. Blom, “An optimal class of symmetric key genera-tion systems,” in Proceeding of EUROCRYPT, pp. 335–338, 1984.

[2] S. Ruj, A. Nayak, and I. Stojmenovic, Key predistri-bution in wireless sensor networks when sensors are within communication range, Chapter 24, Theoretical Aspects of Distributed Computing in Sensor Networks, (Sotiris Nikoletseas, Jose Rolim, eds.), Monographs in Theoretical Computer Science. An EATCS Series, Part 7, Springer, 787-832, 2011

[3] Sencun Zhu, Shouhuai Xu, Sanjeev Setia, and Sushil Jajodia. @Establishing pairwise keys for secure com-munication in ad hoc networks: A probabilistic ap-proach@. In ICNP, pages 326–335, 2003.

[4] Jianbo Yao,Guangjun Wen,” Protecting Classifica-tion Privacy Data Aggregation in Wireless Sensor Net-works”,in WenWireless Communications, Networking and Mobile Computing, 2008. WiCOM '08. 4th Interna-tional Conference on2008.

[5] H. Chan, A. Perrig, and D. X. Song. Random key predistribution schemes for sensor networks. In: IEEE Symposium on Security and Privacy, IEEE Computer Society, pages 197–213, 2003.

[6] Donggang Liu and Peng Ning. Establishing pairwise keys in distributed sensor networks. In ACM Confer-ence on Computer and Communications Security,pages 52–61, 2003.

[7] C. Blundo, A. D. Santis, A. Herzberg, S. Kutten, U. Vaccaro, and M. Yung, “Perfectly-secure key distribu-tion for dynamic confer- ences,” In Advances in Cryp-tology: Proceedings of CRYPTO’92, Santa Barbara, CA, LNCS, vol. 740, pp. 471–486, 1993

[8] L. Eschenauer and V. D. Gligor, “A key-management scheme for distributed sensor networks,” in ACM Conference on Computer and Communications Security, pp. 41–47, 2002

[9] Jianbo Yao,” Preserving Mobile-Sink-Location Pri-vacy in Wireless Sensor Networks”,in Database Tech-nology and Applications (DBTA), 2010 2nd Interna-tional Workshop on2010.

[10] Jianbo Yao, Guangjun Wen,” Preserving Source-Location Privacy in Energy-Constrained Wireless Sen-sor Networks”,in Distributed Computing Systems Workshops, 2008. ICDCS '08. 28th International Con-ference on2008.

[11] George C.M,Kumar M.,” Cluster based Location privacy in Wireless Sensor Networks against a univer-sal adversary”,Information Communication and Em-bedded Systems (ICICES), 2013 International Confer-ence on2013.

[12] Sivashankari S., Raseen M.Mohamed,” A frame-work of trust management on location privacy and min-imising the error rate in wireless sensor networks”,in Optical Imaging Sensor and Security (ICOSS), 2013 International Conference on2013.

[13] Spachos, P., Liang Song, Hatzinakos D.,” Oppor-tunistic routing for enhanced source-location privacy in wireless sensor networks”,in Communications (QBSC), 2010 25th Biennial Symposium on2010.

[14] YaHui Li,Ding Yong,Jian feng Ma,” Secure Mes-sage Distribution Scheme with Configurable Privacy for Heterogeneous Wireless Sensor Networks”,in Embed-ded and Ubiquitous Computing, 2008. EUC '08. IEEE/IFIP International Conference on22008.

[15] Shaikh R.A., Jameel H., d'Auriol B.J., Sungyoung Lee, zoung-Jae Song, Heejo Lee ,” Network Level Pri-vacy for Wireless Sensor Networks”,in Information Assurance and Security, 2008. ISIAS '08. Fourth Inter-national Conference on2008.

[16] Yun Li, Jian Ren," Source-Location Privacy through Dynamic Routing in Wireless Sensor Net-works",in INFOCOM, 2010 Proceedings IEEE 2010.6th Annual IEEE Communications Society Conference on2009.

[17] J. Lee and D. R. Stinson, "A combinatorial ap-proach to key pre- distribution for distributed sensor networks," in IEEE WCNC, New Orleans, LA, USA, pp. 1200–1205, 2005.

[18] W. Dargie and C. Poellabauer, Fundamentals of Wireless Sensor Net- works: Theory and Practice, Wiley, 2010.

[19] Bista, R., Hye-Kyeom Yoo, Jae-Woo Chang," Achieving Scalable Privacy Preserving Data Aggrega-tion for Wireless Sensor Networks ", in Computer and Information Technology (CIT), 2010 IEEE 10th Interna-tional Conference on2010.

[20] Gurjar A., Patil A.R. B.," Cluster Based Anony-mization for Source Location Privacy in Wireless Sen-sor Network", in Communication Systems and Network Technologies (CSNT), 2013 International Conference on2013.

[21] Jian Ren, Yun Li, Tongtong Li," Routing-Based Source-Location Privacy in Wireless Sensor Net-works",in Communications, 2009. ICC '09. IEEE Inter-national Conference on2009.

[22] Oualha N., Olivereau A.," Sensor and Data Privacy in Industrial Wireless Sensor Networks", in Network and Information Systems Security (SAR-SSI), 2011 Conference on2011

[23] Kristin Lauter,Michael Naehrig ,Vinod Vaikuntan-athan, "Can Homomorphic Encryption be Practical?".

[24] Seyit Ahmet C¸amtepe and Bu¨lent Yener. 'Com-binatorial design of key distri-bution mechanisms for wireless sensor networks ', In ESORICS, pages 293–308,2004.

[25] "Pairwise and Triple Key Distribution in Wireless Sensor Networks with Applications" by Sushmita Ruj, Member, IEEE, Amiya Nayak, Senior Member, IEEE and Ivan Stojmenovic, Fellow, IEEE SEECS, University of Ottawa, Canada in IEEE TRANSACTIONS ON COM-PUTERS 2012

[26] C. J. Mitchell and F. Piper, "Key storage in secure networks," Discrete Applied Mathematics, vol. 21, pp. 215–228, 1988.

[27] Wenbo He, Xue Liu, Hoang Nguyen, Nahrstedt K., Abdelzaher T.," PDA: Privacy-Preserving Data Aggre-gation in Wireless Sensor Networks",in INFOCOM 2007. 26th IEEE International Conference on Computer Communications. IEEE2007.

[28] Yun Li, Jian RenSensor," Preserving Source-Location Privacy in Wireless Sensor Networks",in Mesh and Ad Hoc Communications and Networks, 2009. SECON '09.