International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-8 Issue-10, August 2019

Modified Master Key Based Multipath Reinforcement Pre-Distribution Scheme for Wireless Sensor Networks

B.Paulchamy, J.Jaya, K.Kalpana

Abstract: ***Wireless Sensor Network (WSN) is one of the budding fields of technology. It is mainly used for Environmental monitoring and Data accumulation. Due to the limited energy in WSNs, it faces many practical difficulties. The main challenge is the security issues. Objective of this project is to provide security against clone attack in a WSN that are arranged in cluster topology. In this paper, a method to implement three important security measures namely i) Master – Key Pre-distribution solutions, ii) Super imposed disjunct matrix code and iii) Multipath key reinforcement scheme is discussed. One method complements the advantage of other method and thus provides high security. The final analysis shows that the computational overhead is minimum.***

Key words: WSN, Data accumulation, super imposed disjunct matrix code, Multipath key.

I. INTRODUCTION

Wireless Sensor Network consists of many small sensor nodes arranged in indefinite topology. The location of each sensor node with respect to its neighbour is calculated only after its deployment with the help of HELLO messages. The sensor nodes are helpful in collecting information from areas in which human access is not possible. They also have their use in defence. When used in such applications importance must be given for security [2]. The data collected by a sensor network must not be accessible to intruders or enemies. For this purpose many encryption and authentication schemes are used. Before choosing a security scheme for WSN, its topology, condition under which it is deployed and energy / lifetime of the network has to be taken into consideration. The sensor node has limited battery backup, so any security measures that are chosen must not deplete the energy of the sensors. The next important parameter to be considered is the memory. They have very low memory capacity which is often susceptible to override. Mostly pre-distribution schemes are preferred for WSNs since they reduce half of the computations. The aim of pre-distribution schemes is to establish secure network communication [1]. The main evaluation metrics are resilience against node capture, resistance against node replication and computational overhead.

Manuscript published on 30 August 2019.
*****Correspondence Author(s)
Dr.B.Paulchamy, Professor and Head, Department of ECE, Hindusthan Institute of Technology, Coimbatore-32
Dr.J.Jaya, Principal, Akshaya College of Engineering & Technology, Coimbatore-109
K.Kalpana, Associate Professor, Department of ECE. Hindusthan institute of technology, Coimbatore-32

In the first section the paper discusses about the various methods that are already available to provide security for WSNs. The second section gives the details that are shared in each sensor node before deployment. The third section gives information about topology in which the method is implemented and analysed. The consecutive sections describe how the above mentioned three schemes are one by one executed in the given topology.

II. RELATED WORK

Many works has evolved around pair-wise key pre-distribution scheme. Yen – Hua Liao et.al explained about the use of tame pool based pair-wise key pre-distribution for large scale sensor networks. In this scheme a mathematical function called Tame automorphism is implemented for WSN. Bulent Yener and Seyit A.Camptepe described about various key distribution schemes available for Wireless sensor Networks[1,6]. That paper included details for both the distributed and hierarchical wireless sensor networks. From these papers the various key distribution schemes available for WSNs are evident. Though the main concentrations were on pair-wise keys the master keys have the advantage of memory. A single key is enough. Even though the key is not kept as a secret, they provide high security.

III. TOPOLOGY

The topology considered for analysis is the cluster topology. Initially after deployment of the sensor nodes each sensor transmits a Hello message. If there is any sensor node nearby that hears this hello message, then it replies to the sender by transmitting its details as a response. Then the first sensor node which started the Hello message updates the information about the replied node in its Routing table. If it doesn't receive any reply after waiting for a particular period it again transmits another hello message. This process is continued till the whole topological information is gathered by a node (either directly or through the neighbours). Each sensor node is given an ID. Normally clustering of Sensor nodes is done to save energy. In a cluster topology, all the information is conveyed to the base station only through the Cluster Head. The network is divided into many small groups. Each group elects a leader called Cluster Head (CH). The main function of CH is fusion and aggregation. CHs are frequently re-elected in order to prevent the depletion of energy in Single Node [11].

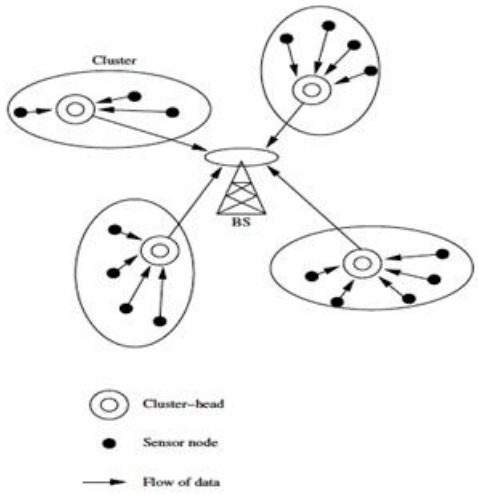

Fig.1.Clustered Architecture.

IV. PRE-DEPLOYMENT DETAILS

Prior to deployment the following details must be stored in each and every sensor nodes

- Authentication key a_i
- Key generation key b_i and
- Super imposed j disjunct matrix.

where i is the ID of the sensor node. There is a single master key which is given to all the sensor nodes. Since all these details are given prior to deployment half of the computation is reduced and the details stored are highly confidential [5].

V. AUTHENTICATION PHASE

The first phase after deployment and selection of CH is the authentication phase[3]. In this phase the base station first authenticates all the cluster heads. Base station uses the master key and the authentication key to authenticate the Cluster Head. For instance consider the following scenario:

Master key = X

Base station = B it has the nonce RB

Cluster Head = CH1 it has the nonce RCH1

They share the nonce value with each other. Then each individually calculate the authentication key as follows,

$$k_{(B,CH1)} = PRF(X/RB/RCH1) \quad (1)$$

If the key generated in both the base station and the CH is same then the first step of authentication is done. If not then the CH is considered as an intruder, because only the genuine nodes knows about the master key.

The same step is repeated in every cluster. Here each cluster head authenticates its group members. They share their nonce and calculate the authentication key. After this first step of verification we go for generation of session between the nodes with the help of super imposed disjunct matrix and multipath key reinforcement scheme.

VI. SESSION KEY GENERATION

The session key is generated with the help of superimposed matrix. As it is said earlier, each sensor node is provided with a super imposed matrix. Here we are using superimposed j disjunct matrix. j is nothing but the maximum number of possible paths that can be available between two sensor nodes that needs to have the session. Let the super imposed matrix be denoted by λ[12].

$$\lambda_i = \begin{bmatrix} Si(1,1) & Si(1,2) & Si(1,3)\cdots & Si(1,j) \\ \vdots & & \ddots & \vdots \\ Si(j,1) & Si(j,2) & Si(j,3)\cdots & Si(j,j) \end{bmatrix}$$

where i is the ID of the sensor node.The matrix λ_i is a m*n binary matrix. Each value in the row and column can be defined as

$$\sum_{i=1}^{j} S(i,j) = a \quad (2)$$

Consider that two nodes U and V have to establish a session key between them. Let there be j number of paths between U and V. The number of links in each oath may vary. If there is more than j number of links in a single path then the path insecurity increases. The following equations explain the calculation in single path.

Path 1=(U,N_1), (N_1,N_2), (N_2,N_3)….. (N_{j-1},N_j),(N_j,V) (3)

Then each link shares the values in the first row. Similarly all the rows are shared between the j paths. If there are more than j numbers of links in a single path then the row is again repeated from the first. When all the values are shared between both the nodes the key is generated as

In path 1,

$K_1= A_1(S_{i(1,1)}$ XOR $S_{i(1,2)}$ XOR $S_{i(1,3)}$ XOR …$S_{i(1,j)})$ (4)

In path 2,

$K_2= A_1(S_{i(2,1)}$ XOR $S_{i(2,2)}$ XOR $S_{i(2,3)}$ XOR … $S_{i(2,j)})$ (5)

and so on up to path j that is K_j.

The session key between the node U and V is given by,

$K= K_1$ XOR K_2 XOR K_3 XOR …… K_j (6)

The secrecy of the session key is protected by all the K_i values. It is practically impossible to track all the paths and calculate the path key and use the path key to generate the session key.

Retrieval Number: H6549068819/19©BEIESP
DOI: 10.35940/ijitee.H6549.0881019
Journal Website: www.ijitee.org

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

If the probability of compromising one link in any path is *q*, then the probability of breaking a path is given by

$$q' = q(jq-q^j)^j \quad (7)$$

Where j is the number of links in a path. Thus the probability of breaking a session key between U and V is, *jq'* if there were j paths.

VII. RESULTS AND DISCUSSION

The paper mainly concentrates on the security of WSNs. Thus the probability of being captured or breaking a link is calculated using the above given formula. The energy consumed for all these computations and efficiency of the system is also calculated. The efficiency of the system increases when multipath method is used. The number of path in the topology doesn't affect the efficiency. They are simulated using NS2 software. The scenario is tested for a network considering 100 nodes.

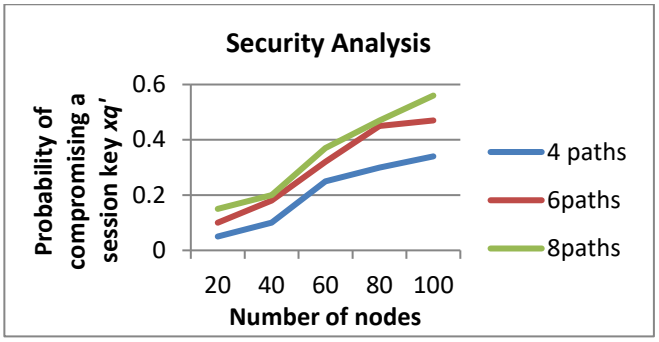

Fig.2.Probability of compromising a session key for different number of paths between two nodes

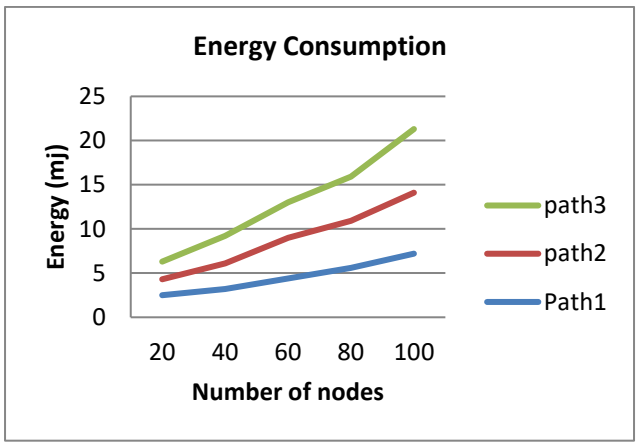

Fig.3. Energy consumed for computations in three paths with 8 links

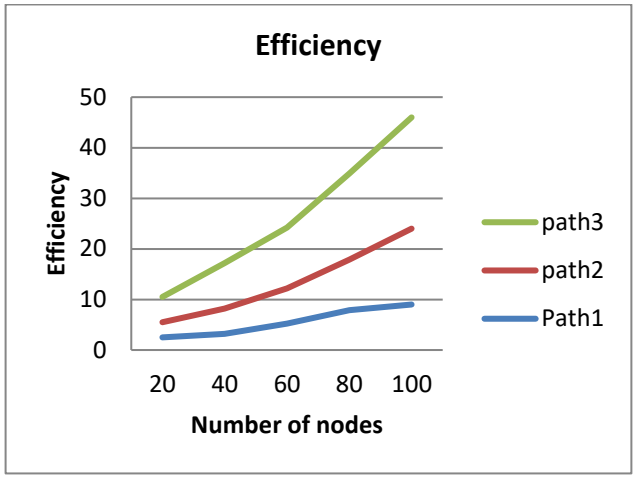

Fig.4. Efficiency of the system for paths with 8 links

VIII. CONCLUSION AND FUTURE WORK

The results show that the proposed method has improved the security considerably. It is impossible to break the hybrid super imposed j disjunct matrix code and multipath key reinforcement method. The energy consumption of the method is also low since the computations used are only simple additions and multiplications. There are around almost j(j+1)additions required in every path. These operations are very simple and do not take much energy from the sensor nodes and at the same time they provide a very high security. The project can be modified in such a way to reduce the number of communications between the nodes. This will further reduce the energy consumption.

REFERENCES:

1. Ross Anderson and Adrian Perrig. Key infection: Smart trust for smart dust. Unpublished Manuscript,November 2001.
2. Dirk Balfanz, Drew Dean, Matt Franklin, Sara Miner, and Jessica Staddon. Self-healing key distribution with revocation. In *Proceedings of the IEEE Symposium on Research in Security and Privacy*, pages 241–257, May 2002.
3. M. Beller and Y. Yacobi. Fully-fledged two-way public key authentication and key agreement for low-cost terminals. *Electronics Letters*, 29(11):999–1001, May 1993
4. Peter Bergstrom, Kevin Driscoll, and John Kimball. Making home automation communications secure. *IEEE Computer*, 34(10):50–56, Oct 2001.
5. C. Bekara, M. Laurent-Maknavicius. "A new protocol for securing wireless sensor networks against Maknavicius. "A new protocol for securing wireless sensor networks againstnodes replication attacks", In Proceedings of the 3rd IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), 2007. nodes replication attacks", In Proceedings of the 3rd IEEE International Con Mobile Computing, Networking and Communications (WiMob), 2007.
6. B. Parno, A. Perrig, and V.D. Gligor, "Distributed Detection of Node Replication Attacks in Sensor Proc. IEEE Symposium. Security and Privacy, pp. 49-63, May 2005. Networks," Proc. IEEE Symposium. Security and Privacy, pp. 49.
7. Detection of Clone Attacksin Wireless Sensor Networks", IEEE Transactions on Dependable and Secure Computing., vol. 8, no. Management Scheme for Distributed Sensor Networks," Proc.

8. R. Brooks, P. Govindaraju, M. Pirretti, N. Vijaykrishnan, and M.T. Kandemir, “On the Detection of Clones in Sensor Networks Using Random Key Predistribution,” IEEE Trans. Systems, Man and Maknavicius. “A new protocol for securing wireless sensor networks againstference on Wireless.
9. Kai Xing Fang, Liu Xiuzhen, Cheng David, H. C. Du, Real-Time Detection of Clone Attacks in Wireless Sensor Networks Proceedings of the 28th International Conference on Distributed Computing Systems, 2008, Pages 3-10.
10. Joseph Binder, Hans Peter Bischof, Zero Knowledge Proofs of Identityfor Ad Hoc Wireless Networks An In-Depth Study, Technical Report, 2003. http://www.cs.rit.edu/ jsb7384/zkpsurvey.pdf.
11. Klempous R.; Nikodem J.; Radosz, L.; Raus, N. ByzantineAlgorithms in Wireless Sensors Network, Wroclaw Univ. ofTechnol.,Wroclaw; Information and Automation, 2006. ICIA2006.International Conference on, 15-17 Dec. 2006, pages :319-324
12. A. J. Macula. A simple construction of d-disjunct matrices withcertain constant weights Discrete Math., 162(13):311-312, 1996 .
13. K. Xing, X. Cheng, L. Ma, and Q. Liang.,Superimposed Code Based Channel Assignment in Multi-radio Multichannel Wireless Mesh Networks. In MobiCom’07, pages 15-26, 2007.

AUTHORS PROFILE

Dr.B.Paulchamy received his Ph.D. in Digital Signal Processing, Approach for De-Noising from EEG signal from Anna University Chennai, M.E degree in Applied Electronics from PSG College of Technology, Coimbatore, affiliated to Anna University Chennai, TamilNadu and B.E degree in Electronics and communication Engineering from National Engineering College, Kovilpatty, affiliated to Anna University Chennai, Tamilnadu.He has more than a decade of teaching experience in various Engineering colleges in Tamil Nadu. Currently he is working as Professor & Head in the department of ECE at Hindusthan Institute of Technology, Coimbatore. His research interests include Signal processing, Image processing and soft computing. He published around 15 papers in refereed conferences and journals. He is the Life Member in the Indian Society for Technical Education &IEANG..

Dr. J Jaya received her Ph.D in Information and Communication Engineering from Anna University, Chennai. She completed her M.Tech in Advanced Communication Systems from SASTRA University, thanjavur, Tamilnadu and B.E in Electronics Communication Engineering from Sri Ramakrishna Engineering College, Coimbatore, Tamilnadu. She has 18 years of Teaching and Research experience in various institutions. She presently holds the post of Principal in Akshaya College of Engineering and Technology, Coimbatore. She is a pioneer in the fields such as Image Processing, Signals and Systems, Digital Signal Processing, Medical Image Processing and Optimization Technology. She has published two books, and has published 28 research papers in International journals and 34 research papers in National level. She has reviewed many National and International level books and journals.

Mrs.K.Kalpana: She received her M.E degree in VLSI Design from Karpagam University,Coimbatore,TamilNadu and B.E degree in Electronics and communication Engineering from Periyar Maniayammai College of Engineering and Technology for Women, Affiliated to Bharathidhasan University, Thanjavur,Tamilnadu.She has more than a decade of teaching experience in various Engineering colleges in Tamil Nadu. Currently she is working as an Assistant Professor in the department of ECE at Hindusthan Institute of Technology, Coimbatore. Her area of interests is image processing, Signal Processing and VLSI Design. She published around 5 papers in refereed conferences and journals.