Journal of Advanced Research in Technology and Management Sciences
Volume: 01 Issue: 03 ISSN: 2582-3078 November 2019
Available online at: http://www.jartms.org

ANALYSIS OF KEY MANAGEMENT AND CRYPTOGRAPHY IN WIRELESS SENSOR NETWORKS

A Basi Reddy [1], , B Ramakantha Reddy [2] , P Krishna Kishore [3] , K Prathima[4]

[1](Assistant Professor, Dept. of IT, S V College of Engineering, Tirupati, India)
Email-Id: basireddy.a@gmail.com
[2](Assistant Professor, Dept. of CSE, S V College of Engineering, Tirupati, India)
Email Id: ramakantharedy@gmail.com
[3](Assistant Professor, Dept. of CSE, Chadalawada Ramanamma Engineering College, Tirupati, India)
Email Id: krishna.boinapalli@gmail.com
[3](Assistant Professor, Dept. of CSE, Chadalawada Ramanamma Engineering College, Tirupati, India)
Email Id: prathimareddy61@gmail.com

Abstract: The deployment of Wireless Sensor Networks (WSN) in the field of military, battlefield, healthcare applications etc has seen a plethora of growth towards variety of sensory devices. Irrespective of different locations, the sensor nodes has to do its task. Hence, the dynamic wireless sensor networks should ensure better quality of sensor nodes that covers wider network area and additional services in relative to static WSNs systems. By doing so, it requires secure data communication among the sensor nodes in wireless environment. Key Management is the recent security concept enabled to provide secure communication between sender and receiver nodes. In this paper, we have proposed efficient key updates systems between the nodes. In any scenario, the nodes may join or leaves the network environment which facilitates to initiate a secret key between intended sender and intended receiver. A certificate less key secrecy system is designed for secure communication in wireless links. By designing so, we have addressed the issues like node authentication, data confidentiality, and data integrity. Experimental analyses have shown the effectiveness of proposed system.

Keywords: Wireless Sensor Networks, Dynamic networks, Sensor nodes, Sensory devices, Key management, Key updates and Node authentication.

I. INTRODUCTION

Nowadays, the exploration on wireless technologies has attracted several network users. Wireless networks is the recent technology where tremendous volume of data can be accessed from anywhere at any time. The prominent features like fault resistance, self-adaptability, scalability, traceability etc have developed greater impact among the wireless users [1]. Wireless networks consist of two types, namely, static wireless sensor networks and dynamic wireless sensor networks. In relative to the static WSNs, the dynamic WSNs ensure the accurate node detection, relevant network coverage and facilitating best QoS. Henceforth, Dynamic Wireless Sensor Networks play a vital role in many parts of the real-time systems. Most of the dynamic wireless sensor networks are applied to detect the criminal offences, healthcare systems, traffic flow and vehicle detection. Thus, security is one of the most important concepts in dynamic WSN applications [2].

Key management system is one of the solutions for effective security systems. In the view of security, authentication and privacy make use of the key systems. Generally, key is the secret thing which is used for authenticating the users [3]. Similarly, key function is also used for encrypting and decrypting the information. Key is the fixed length streams of random bits which are only known for specific parties. It also makes use of mathematical functions to retrieve the original information using their keys. In order to effectively generate and manage the keys, the mathematical functions should be generated properly. Since, different features of WSN have impressed the users for different applications [4].

Key establishment is any method in the cryptography by which cryptographic keys are exchanged between two parties, allowing the use of a cryptographic algorithm. If the sender and the receiver wish to exchange encrypted messages, each should be equipped to encrypt messages that are to be sent and decrypt messages received. The nature of the equipping requirement depends on the encryption technique that is used. If they use a code, both shall require a copy of the same codebook [5]. If they use a cipher, they will need appropriate keys. If the cipher is of

asymmetric key cipher, both shall need a copy of the same key. If an asymmetric key cipher with the public/private key property, both shall need the other's public key.

The rest of the paper is organized as follows: Section II describes the related work, Section III presents the proposed work; Section IV presents the experimental analysis and results and concludes in Section V.

II. RELATED WORK

This section presents the fundamentals of security and prior works carried out by other researchers.

2.1 Security prerequisites for key administering schemes:

An effective key system is defined from generation and establishment of sensor networks. The following are the important points [6]:

- Nodes should be in admissible range for communication.
- Deployed nodes must ensure secure node-to –node communication.
- Additional nodes can also deploy which should ensure better communication systems.
- Any nodes can join or leave the networks.
- If the nodes are misbehaved, any alternate nodes should take care of further responsibilities.

Similarly, the key management should satisfy the basic security requirements like confidentiality, authentication, integrity and non-repudiation [7]. Relied upon the application environment, the keys should be established properly. The evaluation metrics to be considered are security, efficiency and flexibility. In addition to, the metrics like node revocation, secrecy and collusion resistance [8].

a) Node revocation: If any nodes are compromised, then alternate nodes should be revoked or provoked.
b) Secrecy: Before outsourcing the data, it should be properly encrypted and then forward to the intended users.
c) Attacks resistance: In any scenario, the adversary may threaten the networks. A better key management system induces better resistance towards attacks.
d) Resilience: It depends on the execution of nodes from the memory of the sensor nodes [9].

2.2 Prior works:

This part portrays prior works processed by other researchers. The author in [10] discussed about key administration process using clustering based WSNs. Their model was compared with the two layered key management systems which proved that clustering based model has generated efficient keys in reduced time. They depicted a better performance over clustering model. The author in [11] presented pairing based key agreement protocols using elliptic curves. This protocol acted as intermediate between users who hold similar same keys. It reluctantly reduced key space and resolved the attacks like message theft and reply attacks.

The author in [12] presented key administration process over heterogeneous sensor networks. They have utilized on static sensor nodes which shown reduced communication overhead. The author in [13] presented key generation process for mutual authentication process in mobile sensor nodes. They supplied two keys, namely, pairwise and cluster keys. This key was supplied to elliptic curve digital signature algorithms. Relied upon the mobility of nodes, the pairwise and cluster keys are established. The author in [14] discussed about signcryption based heterogeneous systems. They introduced Elliptic Curve Cryptography (ECC) algorithm for lessened communication overhead and storage keys.

The author in [15] surveyed about efficiency metrics of dynamic key management systems that resource constrained properties of sensor nodes that exhibited dynamic key established process. As indicated by the safe correspondence request in WSN, 2varieties of key organization are required. One is pair astute key organization; the inverse is bunch key foundation. A couple plans has been anticipated that joins 3 stages typically [10]:(1) key setup before sending, (2) shared-key revelation once arrangement, and (3) way key foundation if 2 sensor hubs don't offer

an on the spot key. The most in style pair insightful key pre-conveyance answer is Random Pair savvy Key topic [16] which addresses unessential capacity disadvantage and gives some key strength. Its upheld Erodes and Reni's [17] work. Each detecting component hub stores an irregular arrangement of Nape pair-wise keys to accomplish chance p that 2 hubs are associated. Neighboring hubs will tell on the off chance that they share a typical pair-wise key once they send and get "Key Discovering" Message inside radio extent. Its imperfection is that it penances key property to diminish the capacity utilization.

Nearest (area based) pair-wise keys pre-conveyance subject [18] is another to Random pair savvy key plan. It exploits the circumstance information to improve the key availability. Later on, Random key-chain based generally key pre-appropriation answer is another arbitrary key pre-circulation arrangement that started from the answer of fundamental probabilistic key redistribution plan [14]. It relies on upon probabilistic key sharing among the hubs of an irregular diagram. There are numerous key support recommendations to fortify security of the built up connection keys, and enhance flexibility [19]. Target is to solidly create a novel connection or way key by utilizing set up keys, so the mystery's not com-secure once one or a considerable measure of detecting component hub is caught [20].

III. PROPOSED WORK

3.1 Motivation:

The advancements made in the wireless technologies have attracted several wireless users with its unique features. We have analyzed different mechanisms which drives the event of key management systems. Most of the key management system's performance restricted by its node constraint and mobility constraints. Environment variables are responsible for achieving better key establishment systems. In order to gather the information about its nearest nodes, the secret key should be efficiently and effectively generated with uncompromised mathematical operators. Inspired by this fact, we have designed non-certificate key establishment process in Dynamic Wireless Sensor Networks (DWSNs). Though, different sorts of key governance process have been researching, the issues like restricted energy and processing capability are not yet resolved.

3.2 Proposed Non-Credentials Key Governance Process(NC-KGP):

a) Prerequisites keys for NC-KGP:

- Non-credentials public and private key: The basestation creates a pair of public and private keys from Key Generation Center (KGC). This process is done before the deployments of nodes.
- Independent keys: This key is created for every node.
- Creation of pairwise keys: It is created between the nodes for mutual authentication process.
- Cluster keys: This key is distributed to its node in groups. Cluster head will be chosen by its nodes in networks.

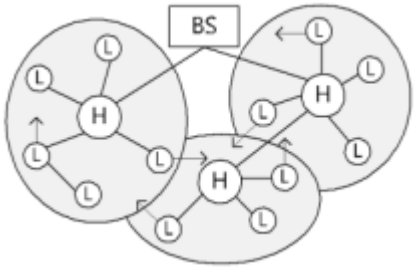

Fig.1. System Architecture

b) Steps in NC-KGP:

System Set-up: This process initiates the number of sensor nodes with the help of Base Station (BS). Each node registers itself with its parameters before the deployment process.

Establishment of pair wise key: Initially, a node sends "Hello message and public key" to its neighboring nodes and collect its details like energy rate, transmission rate, packet length etc. a pair of Master keys and encryption keys are

generated. Pair of master keys is established for secure message transmission. Pair of encryption keys is generated for successful validation of HMAC systems.

Establishment of clusters: After the deployment of nodes by H sensor, the L sensor is generated for content transformation and security validation process. This process creates cluster keys for every node in its groups.

Key tidings: Key tiding is the process of validating the keys for every stipulated time to eliminate the activities processed by adversaries.

Motility of nodes: This step gets succeed only when cluster key is efficiently administered by H sensors. Every change in the node is monitored progressively that updates the cluster keys.

Revocation of keys: Intrusion Detection Systems (IDS) is introduced by the Base station (BS) to study and monitors the malicious events. With the advent of node's status, the information gets updated and processed to the Base Station.

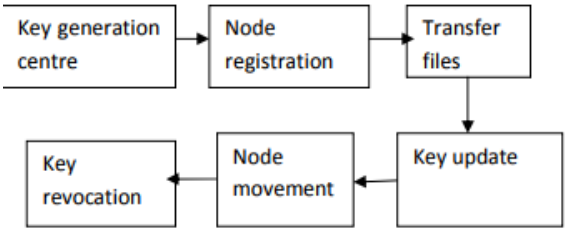

Fig.2. Proposed workflow

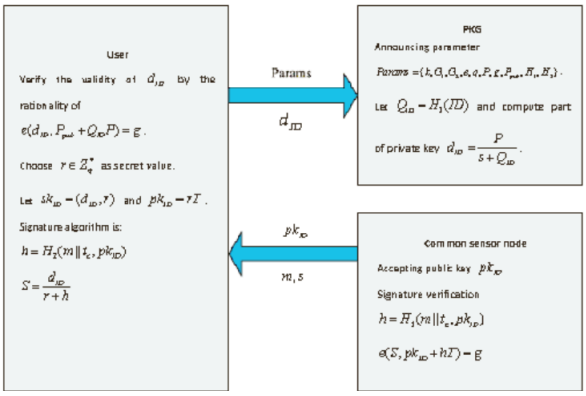

Fig.3. Execution process of NC-KGP scheme

IV. EXPERIMENTAL ANALYSIS

This section presents the experimental analysis of our proposed NC-KGP scheme with static no. of nodes under restricted assets. The objective of the study is to effectively utilize the energy of the nodes with reduced data loss and without compromising the accuracy of authentication. The following are the evaluation metrics analyzed:

a) Efficiency of keys:

While doing the protocol analysis, the processing cost taken by hash operation are eliminated. Since the validation algorithm involves scalar multiplication and bilinear pairing process, the proposed NG-KGP scheme effectively analyzes the message function with certain limitations. The length of public key and pairwise keys generation are

done by point compression of group G1 which shows that the proposed scheme incurs less bits for key generation than the existing schemes.

b) Processing cost:

Generally, the processing cost is studied by the interchanging parameters of the sensor nodes. Since bilinear pairing is used for generating master keys and pairwise keys. Below the fig.4 represents the processing cost taken by analyzing the neighboring nodes. It is inferred that our proposed scheme includes lesser processing cost as the no. of neighboring nodes.

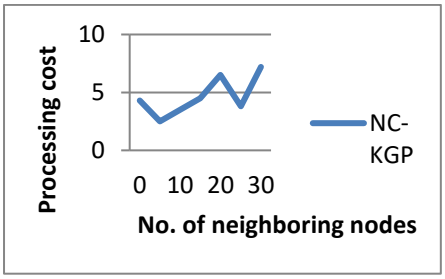

Fig.4. Processing cost analysis of NC-KGP scheme

c) Energy Consumption analysis:

Since the nodes are dynamic in nature, the secure communication depends on the energy consumed by the nodes using the updated neighboring nodes from the Base Station. Based on the storage of public keys, the energy analysis is done. From the fig.5, it is inferred that the bandwidth and energy of our proposed scheme is relatively small and suitable for WSN.

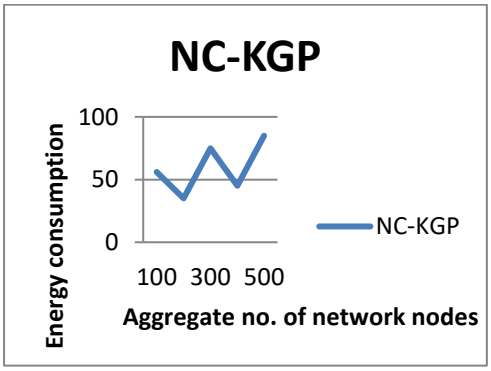

Fig.5. Energy consumption analysis

V. CONCLUSION

Developments made in Dynamic Wireless Sensor Networks have made us to delve into the study of security schemes and its adoption in real-time practices. This paper is the study of enhancing the security mechanism without compromising the energy consumption and data loss. To resolve this issue, we have proposed Non-Credentials based Key Governance Process (NC-KGP) scheme which mutually authenticates the wireless users without revealing their original identities. Most of the key management system's performance restricted by its node constraint and mobility constraints. Environment variables are responsible for achieving better key establishment systems. In order to gather the information about its nearest nodes, the secret key should be efficiently and effectively generated with uncompromised mathematical operators. Simulation analysis has been carried out in terms of keys efficiency, processing cost and energy consumption analysis. The results have shown that our proposed scheme works better than the other baseline algorithms.

REFERENCES

[1] Seung-Hyun Seo et al, "Effective Key Management in Dynamic Wireless Sensor Networks", IEEE transactions on information forensics and security, 10 (2), 2015.

[2] Andrea Tassi, Francesco Chiti, Romano Fantacci, and Fabio Schoen " An Energy-Efficient Resource Allocation Scheme for RLNC-Based Heterogeneous Multicast Communications" IEEE Communications Letters, Vol. 18, No. 8, August 2014.

[3] Andrea Tassi, Francesco Chiti, Romano Fantacci, And Fabio Schoen "An Energy-Efficient Resource Allocation Scheme For RLNC-Based Heterogeneous Multicast Communications". IEEE Communications Letters, Vol. 18, No. 8, August 2014.

[4] Bo Zhu, Member, IEEE, Sanjeev Setia, Sushil Jajodia, Senior Member, IEEE, Sankardas Roy, Member, IEEE, and Lingyu Wang, Member, IEEE. "Localized Multicast: Efficient and Distributed Replica Detection in Large-Scale Sensor Networks" IEEE Transactions On Mobile Computing, Vol. 9, No. 7, July 2010.

[5] Taekyoung Kwon, Member, IEEE, JongHyup Lee, Student Member, IEEE, and JooSeok Song, Member, IEEE . "Location-Based Pairwise Key Predistribution for ireless Sensor Networks" IEEE Transactions On Wireless Communications, Vol. 8, No. 11, November 2009.

[6] Wei-Shou Li, Student Member, IEEE, Tung-Shih Su, Student Member, IEEE, and Wen-Shyong Hsieh. "Multi-Neighbor Random Key Pre-Distribution: A Probabilistic Analysis". IEEE Communications Letters, Vol. 13, No. 5, May 2009

[7] Azzam I. Moustapha, Member, IEEE, and Rastko R. Selmic, Member, IEEE. "Wireless Sensor Network Modeling Using Modified Recurrent Neural Networks : Application to Fault Detection". IEEE Transactions On Instrumentation And Measurement, Vol. 57, No. 5, May 2008.

[8] Wenliang Du, Member, IEEE, Jing Deng, Member, IEEE, Yunghsiang S. Han, Member, IEEE, and Pramod K. Varshney, Fellow, IEEE."A Key Predistribution Scheme for Sensor Networks Using Deployment Knowledge". IEEE Transactions On Dependable And Secure Computing, Vol. 3, No. 1, January-March 2006

[9] X.-J. Lin and L. Sun, "Cryptanalysis and improvement of a dynamic and secure key management model for hierarchical heterogeneous sensor networks," in Proc. IACR Cryptol. ePrint Archive, 2013, pp. 698–698.

[10] D. Du, H. Xiong, and H. Wang, "An efficient key management scheme for wireless sensor networks," Int. J. Distrib. Sensor Netw., vol. 2012, Sep. 2012, Art. ID 406254.

[11] X. He, M. Niedermeier, and H. de Meer, "Dynamic key management in wireless sensor networks: A survey," J. Netw. Comput. Appl., vol. 36, no. 2, pp. 611–622, 2013.

[12] M. Rahman and K. El-Khatib, "Private key agreement and secure communication for heterogeneous sensor networks," J. Parallel Distrib. Comput., vol. 70, no. 8, pp. 858–870, 2010.

[13] M. R. Alagheband and M. R. Aref, "Dynamic and secure key manage-ment model for hierarchical heterogeneous sensor networks," IET Inf. Secur., vol. 6, no. 4, pp. 271–280, Dec. 2012

[14] M. Eltoweissy, M. Moharrum and R. Mukkamala, "Dynamic Key Management in Sensor Networks," Communications Magazine, IEEE, vol 44, pp 122- 130, April 2006.

[15] Arvinderpal S. Wander, Nils Gura, Hans Eberle,Vipul Gupta, and Sheueling Chang Shantz.(2005) EnergyAnalysis of Public Key Cryptography for Wireless Sensor Networks. In Proceedings of the Third IEEE International Conference on Pervasive Computing and Communications, pages 324– 328.

[16] He Daojing, Chen Chun, Chan Sammy, Security Analysis and Improvement of a Secure and Distributed Reprogramming Protocol for Wireless Sensor Networks, IEEE Transactions on Industrial Electronics 60, 5348-5354 (2013).

[17] Li Chun-Ta, Weng Chi-Yao, Lee Cheng-Chi, An Advanced Temporal Credential-Based Security Scheme with Mutual Authentication and Key Agreement for Wireless Sensor Networks, Sensors 13, 9589-9603 (2013).

[18] Yu Yong, Ni Jianbing, Sun Ying, Security Analysis of a Distributed Reprogramming Protocol for Wireless Sensor Networks, IEICE Transactions o Information And Systems E96D, 1875-1877 (2013).

[19] Sun Da-Zhi, Li Jian-Xin, Feng Zhi-Yong, The security and improvement of a two-factor user authentication scheme in wireless sensor networks, Personal and Ubiquitous Computing 17, 895-905 (2013).

[20] Kifayat Kashif, Merabti Madjid, Shi Qi, Component-based security system (COMSEC) with QoS for wireless sensor networks, Security and Communication Networks 6, 461-472 (2013).