ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

Vol. 4, Issue 3, March 2016

# Effective Key Management Technique in Dynamic Wireless Sensor Network

Akshay Shrikhande[1,] Dr. R. S Kawitkar[2]

PG Student, Department of ETC, Sinhagad College of Engineering, Vadgaon (BK), Pune, Savitribai Phule Pune University, Pune India.

Professor, Department of ETC, Sinhagad College of Engineering, Vadgaon (BK), Pune, Savitribai Phule Pune University, Pune India.

**ABSTRACT:** Key organization has remained a troublesome issue in remote device frameworks (WSNs) as a delayed consequence of the prerequisites of contraption center point resources. Distinctive key organization plots that trade off security and operational necessities are proposed recently. Remote device Networks (WSNs) incorporates minor sensor center points with strained essentialness, memory and estimation limits. They're usually passed on within the unattended and disagreeable environment. So device center points locale unit powerless against ambushes, for instance, center catch and intrigue attack by unfavorable ascent. This paper proposes a key scattering subject, in perspective of Exclusion-based structures (EBSs) and t-degree sum. Its accomplice degree imperativeness profitable component key organization plot that performs constrained rekeying to diminish overhead. In this paper, we tend to propose a verification less-convincing key organization (CL-EKM) tradition for secure correspondence in component WSNs depicted by center point adaptability. The CL-EKM reinforces commonsense key updates once a center point leaves or joins a group and ensures forward and in opposite key puzzle. The tradition moreover supports reasonable key revocation for exchanged off centers and minimizes the impact of a center deal on the affirmation of alternative correspondence joins. A security examination of our theme shows that our tradition is effective in prepared for moved strikes. We have a tendency to execute CL-EKM in Conic OS and reproduce it misuse Coola machine to assess now is the ideal time, essentialness, correspondence, and memory execution.

**KEYWORDS:** Certificate less public key cryptography,clustering, key management, security and confidentiality,wireless sensor networks.

## I. INTRODUCTION

To effectively give each center point acceptance and set up a couple shrewd key between center points, we amass CL-EKM by utilizing a coordinating free confirmation less cross breed signcryption subject (CL-HSC) masterminded by America in An earlier work [13], [14]. as a delayed consequence of the properties of CL-HSC, the pair canny key of CL-EKM will be with capability shared between two center points while not requiring troublesome mixing operations and the exchanging of supports. To reinforce center point quality, our CL-EKM in addition supports light-weight shapes for pack key upgrades dead once a center point moves, and key repudiation is executed once a center point is perceived as noxious or leaves the gathering for good. CL-EKM is flexible only if there ought to be an event of included substances of new center points once organize arranging. CL-EKM is secure against center point deal, natural examination and copy, and ensures forward and in converse riddle. The security examination of our subject shows its ampleness. Underneath we tend to plot the duties of this paper: • we have a tendency to exhibit the wellbeing inadequacies of existing ECC based generally key organization anticipates component WSNs. We tend to propose the vital verification less capable key organization subject (CL-EKM) for component WSNs. CL-EKM reinforces four sorts of keys, everything about is used for an uncommon reason, and furthermore secure pair-wise center point correspondence and social event centered key correspondence among clusters. Reasonable key organization approach zone unit portrayed out as supporting center improvements across over absolutely particular clusters and key renouncement system for dealt center points. CL-EKM is maintained misuse Contiki OS and use a TI exp5438 gorilla to encounter the computation and correspondence overhead of CL EKM. Also we tend to add to a machine to encounter the essentialness use of CL-EKM. By then, we have a tendency to coordinate the proliferation of center point advancement by accepting the stochastic system quality Model and the Manhattan quality Model among the structure.

## II. RELATED WORK

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 [11] which addresses unessential capacity disadvantage and gives some key strength. It's upheld Erodes and Reni's [12] 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 [13] 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. 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. One methodology is to expand amount of key cover required in shared key disclosure stage. Q-composite irregular key pre conveyance subject [11] needs letter normal keys to build up a connection key. Comparative system is anticipated by Pair-wise key organization convention [15] that uses edge mystery sharing for key fortification. The key fortification arrangements all in all expansion procedure and correspondence quality; however give brilliant strength as in bargained key-chain doesn't straightforwardly affect security of any connections inside of the WSN. In any case, it ought to be feasible for Associate in Nursing restrict to re-cowl introductory connection keys. Partner in Nursing restrict will then recuperate fortified connection keys from the recorded multi-way fortification messages once the connection keys are bargained. Symmetric key plans don't appear to be feasible for versatile identifier hubs thus past methodologies have focused on exclusively on static WSNs. two or three methodologies are arranged upheld PKC to bolster dynamic WSNs. Subsequently, amid this segment, we survey past PKC-based key administration plans for dynamicWSNs and break down their security shortcomings or weaknesses. Chuang et al. [7] and Agawam et al. [8] arranged a two-layered key administration topic and a dynamic key redesign convention in element WSNs bolstered the Daffier-Hellman (DH), severally. Notwithstanding, both plans don't appear to be fitted to sensors with limited assets and zone unit not able to perform important calculations with enormous key sizes (e.g. at least 1024 piece). Since PC code is computationally additiona l efficient and highlights a short key length (e.g. 160 piece), numerous methodologies with declaration are arranged upheld PC code. Notwithstanding, subsequent to each hub ought to trade the declaration to discover the pair astute key and confirm each other's endorsement before utilize, the correspondence and calculation overhead increment drastically. Likewise, the BS experiences the overhead of authentication administration. Besides, existing plans don't appear to be secure. Alagheband et al. [5] arranged a key administration topic by exploitation ECC-based signcryption, yet this subject is frail against message imitation assaults [16].Huang et al. [15] arranged an ECC-based key foundation plan for self-sorting out WSNs. In any case, we tend to establish the security shortcomings of their topic. In step a couple of their subject, an identifier hub U sends z = qU • H (Mackey) + dU (mown) to the inverse hub V for confirmation, wherever qU might be a static individual key of U. Be that as it may, once V gets the z, it can uncover qU, as an aftereffect of V as of now got Mackey and dU in step one. In this way, V will essentially get qU by figuring qU = (z − dU) • H(Mackey) −1. In this manner, the indicator hub's private mystery is presented to the inverse hub all through the key foundation between 2 hubs. Zhang et al. [10] arranged a dispersed settled key administration topic bolstered ECC for element WSNs. It utilizes the isosceles key methodology for sharing the pair astute key for existing hubs and utilizations a lopsided key way to deal with offer the pair insightful keys for another hub when preparing. Be that as it may, following the underlying key KI is utilized to figure the individual keys furthermore the pair astute keys in the wake of preparing for all hubs, if a spirit acquires KI, the foe has the adaptability to figure all individual keys and the pair insightful keys for all hubs. Therefore, such subject experiences powerless flexibility to hub bargains. Likewise, since such topic utilizes a clear ECC-based DH key understanding by exploitation each hub's semipermant open key and individual key, the mutual pair savvy mystery is static and therefore, is not secure against known-key assaults and can't give re-key operation utilize an ECDSA subject to check the personality of a group head and a static EC-DiffieHellman key assention topic to share the pair shrewd key between the bunch heads. In this way, the topic by Duet al. isn't secure against known-key assaults, as an aftereffect of the pair savvy key between the bunch heads is static. On the inverse hand, Du et al. utilize a standard math based isosceles key way to deal with offer the pair shrewd key between a locator hub and a group head. In this manner, an identifier hub can't straightforwardly build up a couple insightful key with various locator hubs and, rather, it needs the backing of the bunch head. In their subject, so as to discover a couple insightful key between two hubs inside of the same group, the bunch head self-assertively produces a couple astute key and scrambles it exploitation the common keys with these two hubs. At that point the group head transmits the encoded pairwise key to each hub. Hence, if the bunch head is traded off, the pair shrewd keys between non-bargained identifier hubs in the same group will be traded off.

## III. SYSTEM MODEL& ANALYSIS METRICS

### A. SYSTEM MODEL

The basic system model of this paper is pictured in Figure.1.It consists of 1 BS and lots of uniform sensing element nodes with distinctive ID. It uses cluster and two-layer design for scalability. Every cluster has some key generation nodes (KGNs) that distribute point keys among that cluster. These KGNs is also the final sensingelement nodes elect by cluster heads (CHs).We assume that the fundamental system model is deployed for the purpose of watching the hostile atmosphere. End-to-end node communication is unusual as a result of sensing element nodes in each cluster monitor the finite space. For the info aggregation, there square measure several communications between the nodes among the same cluster. Thus, the most task of this model could be a information transfer from sensing element nodes to BS and an information aggregation in every cluster

### B. ANALYSIS METRICS

WSNs have some criteria that represent fascinating characteristics in key management scheme. To boot, energy consumption is that the most vital criterion thanks to the power constraint of detector nodes. Energy consumption might affect primarily the network lifespan. The key criteria square measure shown below.

• Resilience against node capture • Revocation • Scale • Energy consumption

## IV. PROPOSED SCHEME

This paper introduces an Energy-Efficient Dynamic Key Management (EEDKM) proposal that uses two-layer architecture. In the lower layer, similar to LOCK, rekeying is performed confined using the EBS and the t-degree vicariate polynomial. Each cluster has a clear number of KGNs which makes it hard that an attacker can exposes the network keys by obtaining some KGNs. In upper layer, rekeying is performed using the secret key between BS and sensor node. The secret key is loaded before in each sensor node with unique ID and authenticates the node to the BS. The BS generates one t-degree vicariate polynomial key and distributes it by means of session key shared by all CHs. This makes the communication between CHs efficient. The rest of this section describes the bootstrapping, initial key distribution mechanism and some general operations in our key management scheme. This may help you to understand our scheme.

## V. OVERVIEW OF THE CERTIFICATELESS EFFECTIVE KEY MANAGEMENTAND SECURITY MODEL SCHEME

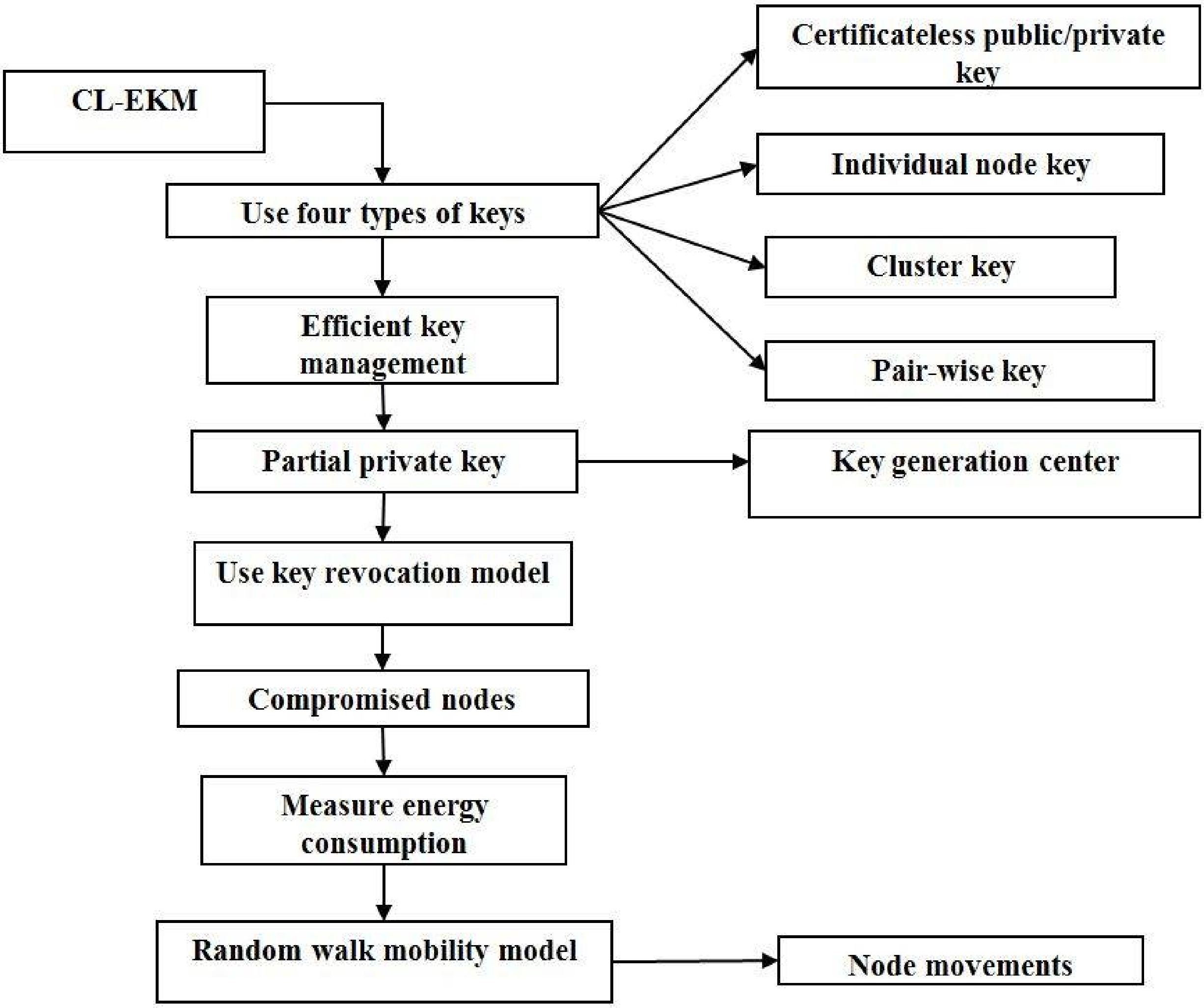


FIG NO 1. CERTIFICATELESS EFFECTIVE KEY MANAGEMENTAND SECURITY MODEL SCHEME

**Explanation-**

Key management before wsn will exchange information firmly, encryption keys should be established among sensing element nodes. Key distribution refers to the distribution of multiple keys among the sensing element nodes, which is typical in an exceedingly non-trivial security theme. Key management could be a broader terms for key distribution, which conjointly includes the processes of key setup, the initial distribution of keys, and key revocation — the removal of a compromised key.

### A. Network Model

We contemplate a heterogeneous dynamic wireless device network (See Fig. 1). The network consists of variety of stationary or mobile device nodes and a bachelor's degree that manages the network and collects knowledge from the sensors. Device nodes will be of 2 types: (i) nodes with high process capabilities, referred to as H-sensors, and (ii) nodes with low process capabilities, said as L-sensors. We have a tendency to assume to own N nodes within the network with variety N1 of H-sensors and variety N2 of L-sensors, wherever N = N1 + N2, and N1 N2. Nodes could be part of and leave the network, and thus the network size could dynamically amendment. The H-sensors act as cluster heads whereas L-sensors act as cluster members. They are connected to the bachelor's degree directly or by a multi-hop path through other H-sensors. H-sensors and L-sensors will be stationary or mobile. Once the network preparation, every H-sensor forms a cluster by discovering the neighboring L-sensors through beacon message exchanges. The L-sensors will be part of a cluster, move to different clusters and conjointly re-join the previous clusters. To maintain the updated list of neighbors and property, the nodes in anexceedingly cluster sporadically exchange very light-weight beacon messages. The H-sensors report any changes in their clusters to the bachelor's degree, as an example, once an L-sensor leaves or joins the cluster. The bachelor's degree creates a listing of legitimate nodes; Associate in Nursing updates the standing of the nodes once an anomaly node or node failure is detected. The bachelor’s degree assigns every node a unique symbol. A L-sensor nil is unambiguously known by node ID Li whereas a H-sensor nHj is assigned a node ID Hj . A Key Generation Center (KGC), hosted at the bachelor's degree, generates public system parameters used for key management by the BS and problems certificate less public/private key pairs for every node within the network. In our key management system, a unique individual key, shared solely between the node and also the bachelor's degree is assigned to every node. The certificate less public/private key of a node is employed to ascertain pair wise keys between any 2 nodes. A cluster secret's shared among the nodes in a very cluster.

### B. Adversary Model and Security Requirements

We assume that someone will mount a physical attack on a device node once the node is deployed and retrieve secret information and knowledge keep within the node.The someone also can populate the network with the clones of the captured node. Even while not capturing a node, Associate in nursing someone will conduct Associate in nursing impersonation attack by injecting Associate in nursing illegitimate node, which attempts to impersonate a legitimate node. Adversaries will conduct passive attacks, such as, eavesdropping, replay attack, etc to compromise knowledge confidentiality and integrity. Specific to our planned key management theme, if someone perform a known-key attack to be told pair wise master keys if it somehow learns the short keys, e.g., pair wise secret writing keys.

## VI. CL-EKM MECHANISM

The CL-EKM is comprised of 7 phases: system setup, pair wise key generation, cluster formation, key update, node movement, key revocation, and addition of a new node Secure key management theme for WSNs supporting mobile nodes, the following security properties are critical:

I. **Compromise-Resilience:** A compromised node should not affect the protection of the keys of different legitimate nodes. In different words, the compromised node should not be in a position to reveal pair wise keys of non-compromised nodes. The compromise-resilience definition doesn't mean that a node is resilient against capture attacks or that a captured node is prevented from causing false knowledge to different nodes, BS, or cluster heads.

II. **Resistance Against biological research and Impersonation:** The scheme should support node authentication to safeguard against node replication and impersonation attacks.

III. **Forward and Backward Secrecy:** The theme should assure forward secrecy to forestall a node from exploitation Associate in nursing previous key to continue decrypting new messages. It should conjointly assure backward secrecy to forestall a node with the new key from going backwards in time to decode

DOI: 10.15680/IJIRCCE.2016. 0403259

antecedently exchanged messages encrypted with previous keys. Forward and backward secrecy are accustomed defend against node capture attacks.

IV. **Resilience against Known-Key Attack:** The theme should be secure against the known-key attack.

### A. Types of Keys

a. **Certificate less Public/Private Key:** Before a node is deployed, the KGC at the BS generates a singular certificate less private/public key **combine** and installs the keys in the node. This key combine is employed to get a reciprocally authenticated pair wise key.

b. **Individual Node Key:** every node shares a singular individual key with BS. As an example, an L-sensor will use the individual key to write Associate in Nursing alert message sent to the BS, or if it fails to speak with the H-sensor. An H-sensor will use its individual key to write the message akin to changes within the cluster. The BS also can use this key to write any sensitive information, such as compromised node info or commands. Before a node is deployed, the BS assigns the node the individual key.

c. **Pair wise Key:** every node shares a unique pair wise key with every of its neighboring nodes for secure communications and of those nodes. As an example, in order to hitch a cluster, a L-sensor ought to share a pair wise key with the H-sensor. Then, the H-sensor will firmly encrypt and distribute its cluster key to the L-sensor by victimization the pair wise key. In Associate in Nursing aggregation supportive WSN, the L-sensor will use its pair wise key to firmly transmit the detected information to the H-sensor. Each node can dynamically establish the pair wise key between itself and another node victimization their various certificate less public/private key pairs.

d. Cluster **Key:** All nodes in an exceedingly cluster share a key, named as cluster key. The cluster key's chiefly used for securing broadcast messages in an exceedingly cluster, e.g., sensitive commands or the amendment of member standing in an exceedingly cluster. Only the cluster head will update the cluster key once a L-sensor leaves or joins the cluster.

## VII. EXPERIMENTAL SET UP

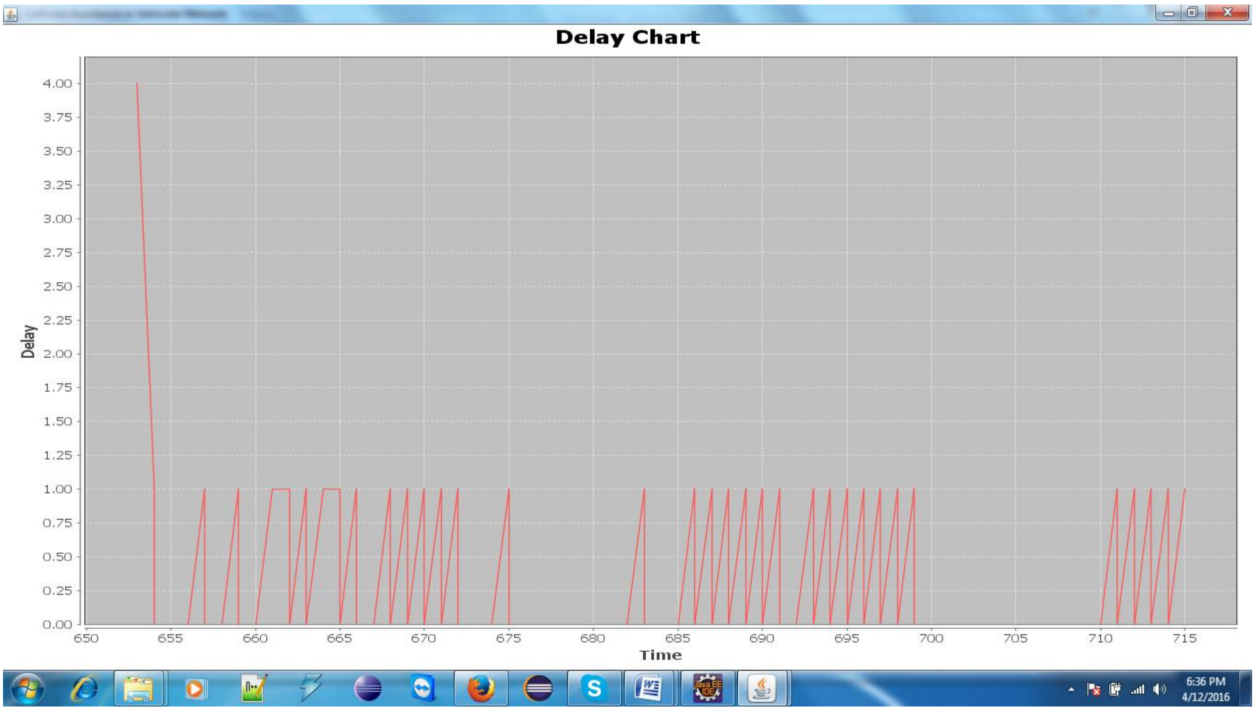
We use Network simulator IN java to show the performance of our proposed scheme. A WSN consists of 10 sensor nodes are randomly deployed over a square region of 1600 ×1600 m2 used in this simulation. The size of the data packet is 512 bytes. Adhoc on Demand Routing (AODV) protocol is used. We have 2 cluster groups. As compared to existing scheme, our proposed scheme has better performance in terms of energy consumption, delay, and throughput. The following section shows the simulation parameters, results and comparison performance of the proposed system. Table 1 shows the simulation parameters for the proposed key management method.

**Simulation Parameters**

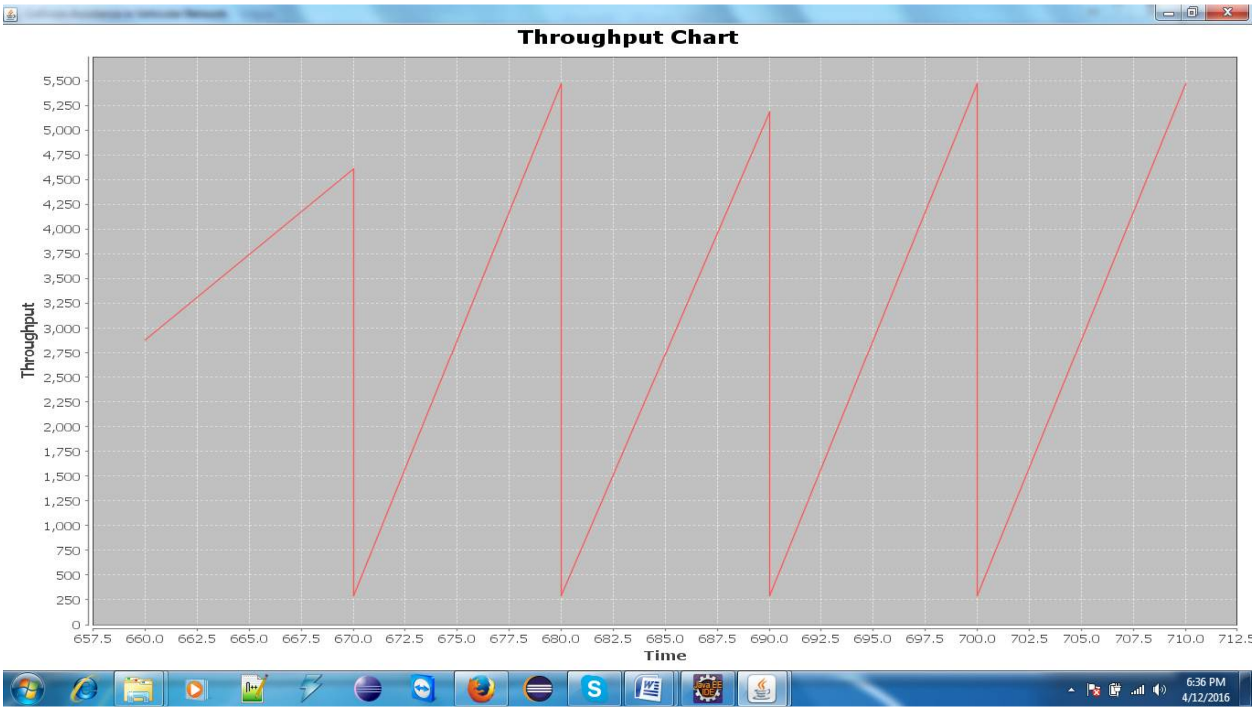
| Parameter | value |
|---|---|
| Field size | 1600×1600 m2 |
| Number of sensor nodes | 10 |
| Propagation type | Two ray ground |
| Routing type | AODV |
| Packet size | 512 bytes |
| Channel | Wireless |
| Simulation time | 3.8 seconds |

Table 1 Simulation Parameters **Performance Results** In this section, the performance of our protocol is compared with the existing method in terms of energy consumption, throughput and delay.

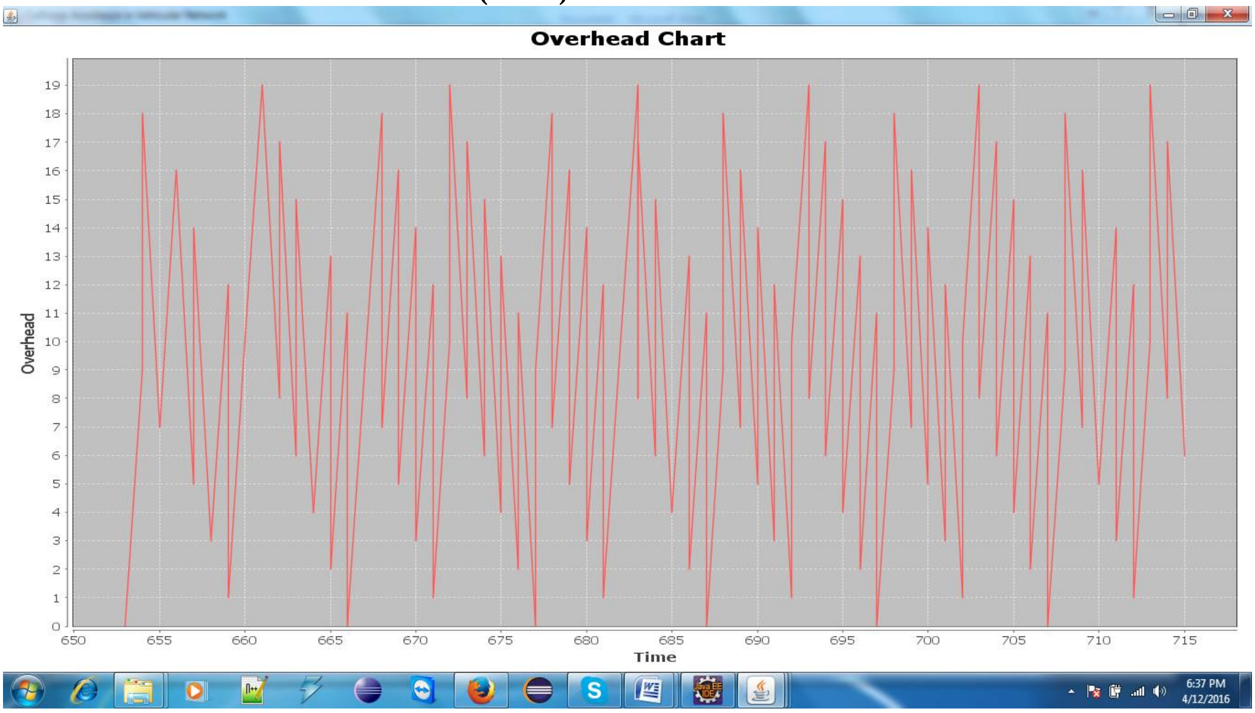
## DELAY GRAPH FOR VEHICULAR NODE



## THROUGHPUT



OVERHEAD COST (TIME) FOR REACHING WARNING SIGNAL.



## VIII. CONCLUSION AND FUTURE WORK

This Project proposed to the crucial confirmation less convincing key organization tradition (CL-EKM) for secure correspondence in component WSNs. CL-EKM support saving correspondence for key updates and organization once a center point leaves or joins a bundle and immediately ensures forward and in opposite key riddle. Our subject is flexible against center exchange off, cloning and impersonates ambushes and secures the data protection and uprightness. This endeavor tend to exhibit a substitution subject which will be used for development varied keys (pair sagacious keys, way keys and cluster keys) for remote device frameworks. It can do lively credibility while not propel counts and correspondences. The examination result shows the execution of TKLU is new. Accomplice in nursing essentialness capable component key organization point abuse the EBSs, polynomials and riddle symmetry keys. EEDKM gives restricted rekeying which is reasonably performed not puncturing the converse segments of WSN. Since EEDKM uses separately symmetric key between the four year affirmation and sensor center point, it will guarantee the center point and performs rekeying more essentialness rapidly than LOCK within the higher layer. EEDKM is additional flexible than general key organization arrangement supported the EBSs and polynomial keys. Thusly rekeying is performed less of times. These numerical models are utilized to gage the right worth for the Told and Takeoff for parameters maintained the pace besides the needed exchange between the imperativeness usage moreover the security level.

## REFERENCES

[1] H. Chan, A. Perrig, and D. Song, “Random key predistribution schemes for sensor networks,” in Proc. IEEE Sump. SP, May 2003, pp. 197–213.

[2] W. Du, J. Deng, Y. S. Han, and P. K. Varshney, “A key redistribution scheme for sensor networks using deployment knowledge,” IEEE Trans. Dependable Secure Compute., vol. 3, no. 1, pp. 62–77, Jan./Mar. 2006.

[3] W. Du, J. Deng, Y. S. Han, P. Varshney, J. Katz, and A. Kaila, “A pair wise key redistribution scheme for wireless sensor networks,” ACM Trans. Inf. Syst. Secur., vol. 8, no. 2, pp. 228–258, 2005.

[4] M. Rah man and K. El-Katie, “Private Key agreement and secure communication for heterogeneous sensor networks,” J. Parallel Diatribe. Compute. vol. 70, no. 8, pp. 858–870, 2010.

[5] M. R. Alagheband and M. R. Aref, “Dynamic and secure key management model for hierarchical heterogeneous sensor networks,” IET Inf. Secure., vol. 6, no. 4, pp. 271–280, Dec. 2012

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

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

[8] Liu, D. and Ning P. 2003. Establishing pairwise keys in distributed sensor networks. In CCS '03: Proceedings of the 10th ACM conference on Computer and communications security. ACM, New York, NY, USA, 52−61.

[9] Liu D., and Ning P., “Efficient distribution of key chain commitments for broadcast authentication in distributed sensor networks”. In Proceedings of the 10th Annual Network and Distributed System Security Symposium, pages 263–276, 2004.

[10] ParadisL.and Han Q., “A survey of fault management in wireless sensor networks,” J. Netw. Syst. Manage., vol. 15, no. 2, pp. 171–190, 2007.

[11] Perrig A., Szewczyk R., Tygar J. D., Wen V., and Culler D. E. “Spins: security protocols for sensor networks”. Wireless Networking, 8(5):521–534, 2002.

[12] Perrig A., Stankovic J., and Wagner D., ―Security in Wireless Sensor Networks,‖Commun. ACM, vol. 47, no. 6, June 2004, pp. 53–57.

[13] Rassam M. A., Maarof M. A., and Zainal A., “A survey of intrusion detection schemes in wireless sensor networks,” Amer. J. Appl. Sci., vol. 9, no. 10, pp. 1636–1652, 2012.

[14] Sattam S. Al-Riyami and Kenneth G. Paterson., Information Security Group,” Certificateless Public Key Cryptography”, Royal Holloway, University of London, Egham, Surrey, TW20 0EX.

[15] Seung-Hyun Seo., IEEE Transactions On Information Forensics And Security, Vol. 10, No. 2, February 2015.

[16] Wen Tao Zhu, Jianying Zhou, Robert H. Deng and FengBao., “A Detecting node replication attacks in mobile sensor networks.” Vol:5, issue:5, pages 496-507, May-2012.

[17] Zhu W. T., Zhou J., Deng R. H., and Bao F., “Detecting node replication attacks in mobile sensor networks: Theory and approaches,” Secur. Commun. Netw., vol. 5, no. 5, pp. 496–507, 2012.