ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 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.

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

ABSTRACT: Key association has remained a troublesome issue in Wireless Sensor Network (WSNs) as a deferred result of the essentials of contraption focus point assets. Unmistakable key association plots that exchange off security and operational necessities are proposed as of late. Wireless Sensor Network (WSNs) joins minor sensor focus focuses with strained centrality, memory and estimation limits. They're generally passed on inside the unattended and repulsive environment. So gadget focus focuses region unit frail against ambushes, for case, focus catch and interest assault by unfavorable climb. This paper proposes a key disseminating subject, in context of Exclusion-based structures (EBSs) and t-degree whole. Its assistant degree hugeness gainful part key association plot that performs obliged rekeying to reduce overhead. In this paper, we have a tendency to propose a certificate less-effective key management (CL-EKM) custom for secure correspondence in part WSNs delineated by focus point flexibility. The CL-EKM fortifies practical key overhauls once an inside point leaves or joins a gathering and guarantees forward and in inverse key riddle. The convention besides underpins sensible key disavowal for traded off focuses and minimizes the effect of a middle arrangement on the certification of option correspondence joins. A security examination of our subject demonstrates that our convention is successful in arranged for moved strikes. We tend to execute CL-EKM in Conic OS and recreate it abuse Coola machine to survey now is the perfect time, centrality, correspondence, and memory execution.

KEYWORDS: Wireless sensor networks, key management, clustering, certificate less public key cryptography, security and confidentiality.

I. INTRODUCTION

To viably give every middle point acknowledgment and set up a couple smart key between focus focuses, we accumulate CL-EKM by using an organizing free affirmation less cross breed signcryption subject (CL-HSC) planned by America in A prior work [13], [14]. as a deferred result of the properties of CL-HSC, the pair shrewd key of CL-EKM will be with ability shared between two focus focuses while not requiring troublesome blending operations and the trading of backings. To strengthen focus point quality, our CL-EKM also underpins light-weight shapes for pack key redesigns dead once an inside point moves, and key renouncement is executed once a middle point is seen as harmful or leaves the social occasion for good. CL-EKM is adaptable just if there should be an occasion of included substances of new focus focuses once sorts out masterminding. CL-EKM (testament less-powerful key administration) is secure against focus point bargain, normal examination and duplicate, and guarantees forward and in speak question. The security examination of our subject demonstrates its sufficiency. Underneath we tend to plot the obligations of this paper: • we tend to show the prosperity insufficiencies of existing ECC based by and large key association suspects segment WSNs. We have a tendency to propose the fundamental confirmation less skilled key association subject (CL-EKM) for part WSNs. CL-EKM strengthens four sorts of keys, everything about is utilized for an exceptional reason, and besides secure pair-wise focus point correspondence and get-together focused key correspondence among bunches. Sensible key association approach zone unit depicted out as supporting focus enhancements crosswise over completely specific groups and key denial framework for managed focus focuses. CL-EKM is kept up abuse Contiki OS and utilize

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

a TI exp5438 gorilla to experience the calculation and correspondence overhead of CL EKM. Additionally we tend to add to a machine to experience the centrality utilization of CL-EKM. By then, we tend to facilitate the expansion of focus point headway by tolerating the stochastic framework quality Model and the Manhattan quality Model among the structure. The trial results demonstrate that our CL-EKM subject is lightweight and consequently reasonable for segment WSNs. In Section a few, we tend to in a glimmer examine related work and show the security inadequacies of the present courses of action. As WSNs are conveyed, the extra WSNs are made, the more it persuades the chance to be progressed and part. So there's a need to utilize dynamic key association subject which will update the true blue keys by aggregate and on side interest ceaseless supply of focus point get. This topic improves the structure survivability. The essential anxiety of segment keying might be an organizing the rekeying fragment. EBS [6] is one amongst the master's blueprints. In any case, there's a power that a little blend of focuses could organize and uncover the whole system keys. to reinforce the vital Ebbs' answer, SHELL utilizes the post-sending range data. In any case, it is wasteful; as a deferred result of SHELL depend on the unified key server. Beginning late another expanded Ebbs plan LOCK [8] was proposed. It utilizes 2 layers of Ebbs body keys and t-degree aggregate polynomials. This paper furthermore proposes new key association subject considering Ebbs and t-degree aggregate polynomials. By utilizing conundrum keys between the baccalaureates and assembling heads, this subject could bring extra centrality fit results than LOCK. The straggling leftovers of this paper are sorted out as takes after. Part a few charts the central WSN model and examination estimations. Zone three clears up the foundation structures in a manner of speaking.

II. RELATED WORK

As showed by the sheltered correspondence demand in WSN, 2varieties of key association are required. One is pair shrewd key association; the reverse is pack key establishment. A couple arranges has been expected that joins 3 organizes commonly [10]:(1) key setup before sending, (2) shared-key disclosure once game plan, and (3) way key establishment if 2 sensor centers don't offer an on the spot key. The most in style pair canny key pre-movement answer is Random Pair astute Key subject [11] which addresses unessential limit impediment and gives some key quality. It's maintained Erodes and Reni's [12] work. Every identifying segment center point stores an unpredictable game plan of Nape pair-wise keys to fulfill chance p that 2 centers are related. Neighboring center points will reprimand on the chance that they share an ordinary pair-wise key once they send and get "Key Discovering" Message inside radio degree. Its blemish is that it atonements key property to decrease the limit use. Closest (region based) pair-wise keys pre-movement subject [13] is another to Random pair keen key arrangement. It misuses the condition data to enhance the key accessibility. Later on, Random key-chain based by and large key pre-appointment answer is another discretionary key pre-dissemination game plan that began from the answer of major probabilistic key redistribution arrangement [14]. It depends on upon probabilistic key sharing among the centers of an unpredictable chart. There are various key bolster suggestions to brace security of the developed association keys, and upgrade adaptability. Target is to unequivocally make a novel association or path key by using set up keys, so the puzzle's not com-secure once one or an impressive measure of distinguishing part center point is gotten. One procedure is to grow measure of key spread required in shared key divulgence stage. Q-composite unpredictable key pre transport subject [11] needs letter ordinary keys to develop an association key. Similar framework is foreseen by Pair-wise key association tradition [15] that utilizations edge puzzle sharing for key stronghold. The key fortress courses of action all things considered development system and correspondence quality; however give splendid quality as in dealt key-chain doesn't direct influence security of any associations within the WSN. Regardless, it should be achievable for Associate in Nursing confine to re-cowl early on association keys. Accomplice in Nursing limit will then recover strengthened association keys from the recorded multi-way fortress messages once the association keys are haggled. Symmetric key arrangements don't give off an impression of being possible for adaptable identifier center points in this manner past approachs have concentrated on only on static WSNs. a few approachs are organized maintained PKC to reinforce dynamic WSNs. Hence, in the midst of this section, we review past PKC-based key organization anticipates dynamicWSNs and separate their security inadequacies or shortcomings. Chuang et al. [7] and Agawam et al. [8] masterminded a two-layered key organization theme and a dynamic key upgrade tradition in component WSNs supported the Daffier-Hellman (DH), severally. Regardless, both arrangements don't give off an impression of being fitted to sensors with constrained resources and zone unit not ready to perform critical figurings with colossal key sizes (e.g. no less than 1024 piece). Since PC code is computationally additiona l effective and highlights a short key length

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

(e.g. 160 piece), various techniques with presentation are organized maintained PC code. In any case, resulting to every center point should exchange the assertion to find the pair sharp key and affirm each other's underwriting before use, the correspondence and estimation overhead augmentation radically. In like manner, the BS encounters the overhead of validation organization. Furthermore, existing arrangements don't have all the earmarks of being secure. Alagheband et al. [5] masterminded a key organization theme by misuse ECC-based signcryption, yet this subject is fragile against message impersonation strikes [16].Huang et al. [15] orchestrated an ECC-based key establishment arrangement for self-sorting out WSNs. Regardless, we have a tendency to set up the security inadequacies of their subject. In step two or three their subject, an identifier center point U sends z = qU • H (Mackey) + dU (mown) to the backwards center point V for affirmation, wherever qU may be a static individual key of U. In any case, once V gets the z, it can reveal qU, as an eventual outcome of V starting now got Mackey and dU in step one. Along these lines, V will basically get qU by figuring qU = (z − dU) • H(Mackey) −1. In this way, the pointer center's private secret is introduced to the reverse center point all through the key establishment between 2 center points. Zhang et al. [10] organized a scattered settled key organization theme supported ECC for component WSNs. It uses the isosceles key system for sharing the pair shrewd key for existing center points and uses a disproportionate key approach to manage offer the pair wise keys for another center while get ready. In any case, taking after the hidden key KI is used to figure the individual keys moreover the pair adroit keys in the wake of planning for all center points, if a soul procures KI, the enemy has the flexibility to figure all individual keys and the pair wise keys for all center points. Along these lines, such subject encounters weak adaptability to center point deals. In like manner, since such point uses an unmistakable ECC-based DH key comprehension by abuse every center point's semipermant open key and individual key, the common pair keen puzzle is static and thusly, is not secure against known-key strikes and can't give re-key operation use an ECDSA subject to check the identity of a gathering head and a static EC-DiffieHellman key assention theme to share the pair insightful key between the pack heads. Along these lines, the subject by Duet al. isn't secure against known-key ambushes, as a delayed consequence of the pair sharp key between the group heads is static. On the converse hand, Du et al. use a standard math based isosceles key approach to manage offer the pair savvy key between a locator center and a gathering head. In this way, an identifier center point can't clearly develop a couple savvy key with different locator center points and, rather, it needs the support of the pack head. In their subject, to find a couple adroit key between two centers within the same gathering, the cluster head self-decisively delivers a couple clever key and scrambles it abuse the basic keys with these two centers. By then the gathering head transmits the encoded pairwise key to every center. Subsequently, if the cluster head is exchanged off, the pair astute keys between non-bartered identifier center points in the same gathering will be exchanged 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

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

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

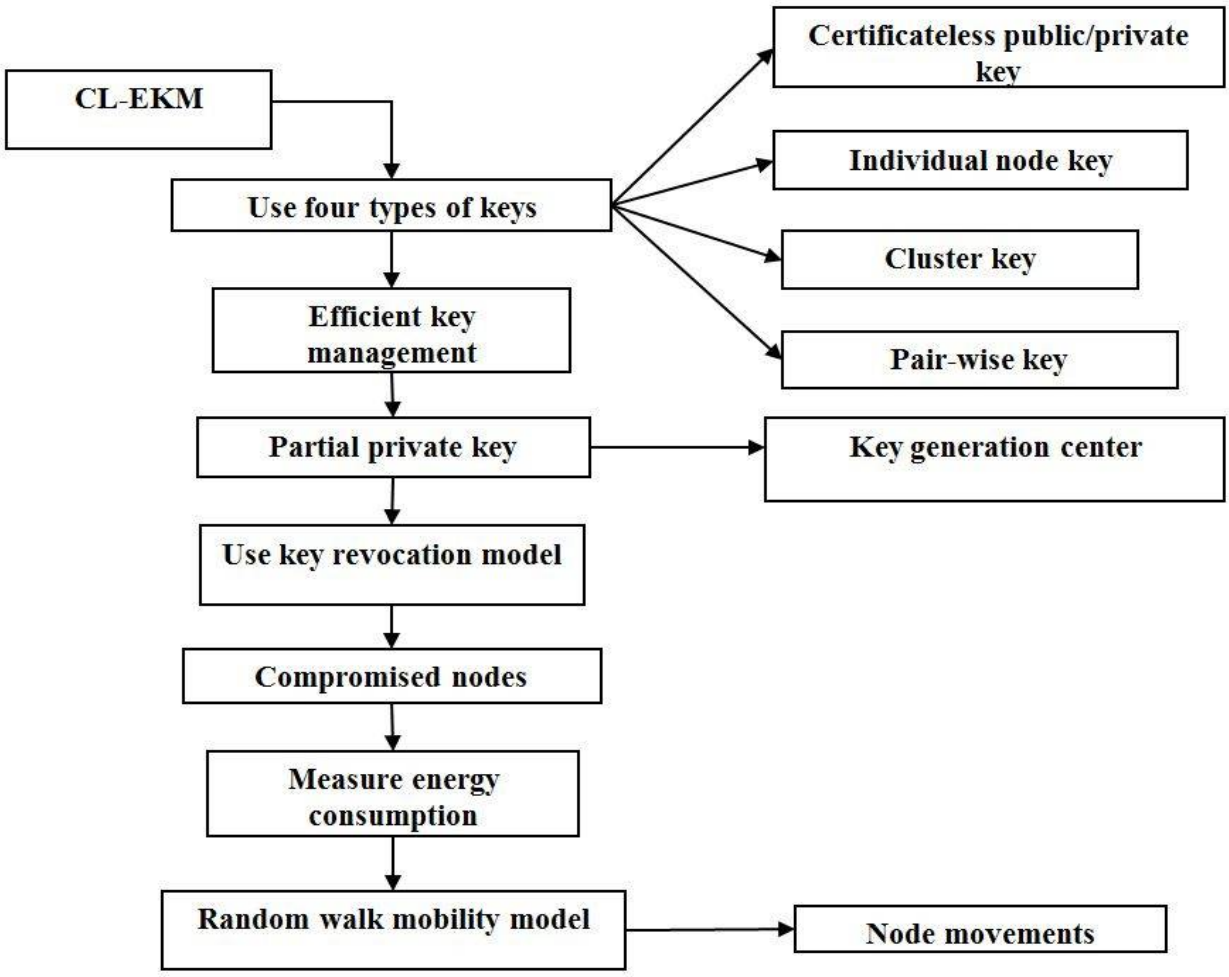


FIG NO 1. CERTIFICATELESS EFFECTIVE KEY MANAGEMENTAND SECURITY MODEL SCHEME

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

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

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

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 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.

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

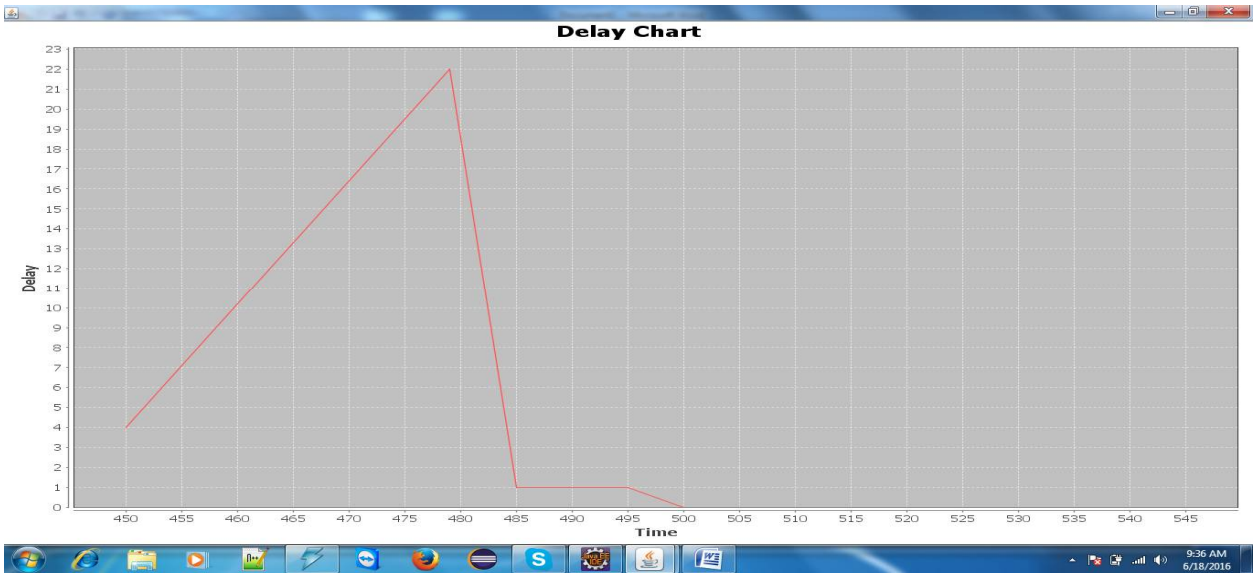
Vol. 5, Issue 6, June 2016

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.

1. DELAY CHART



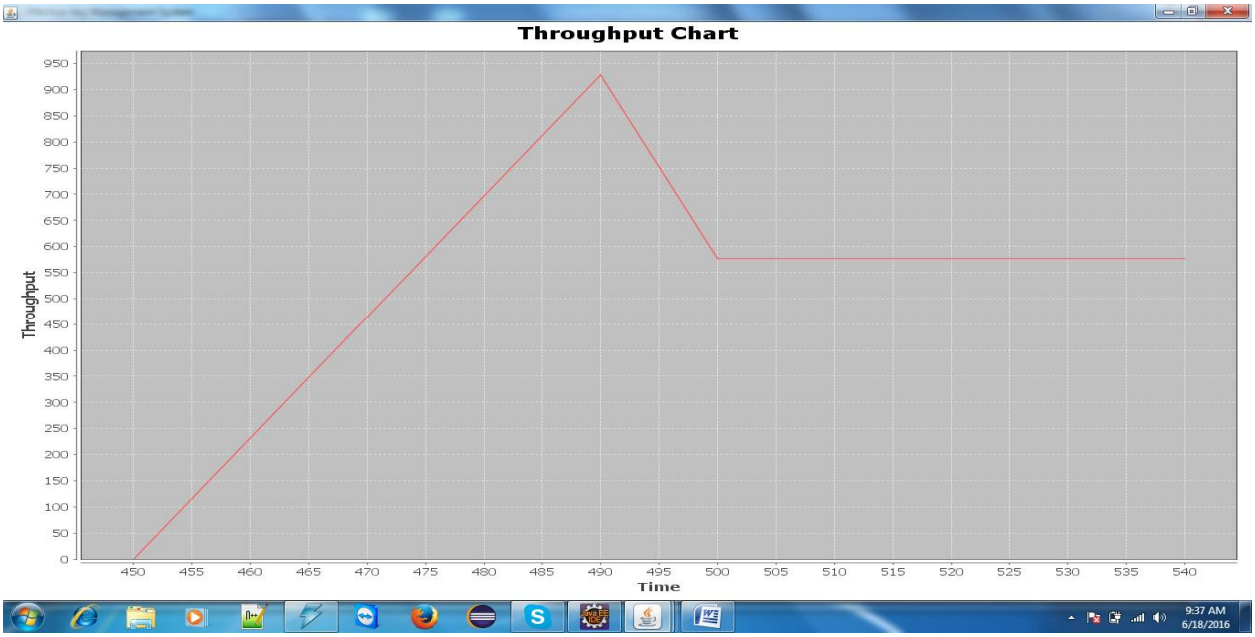
ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

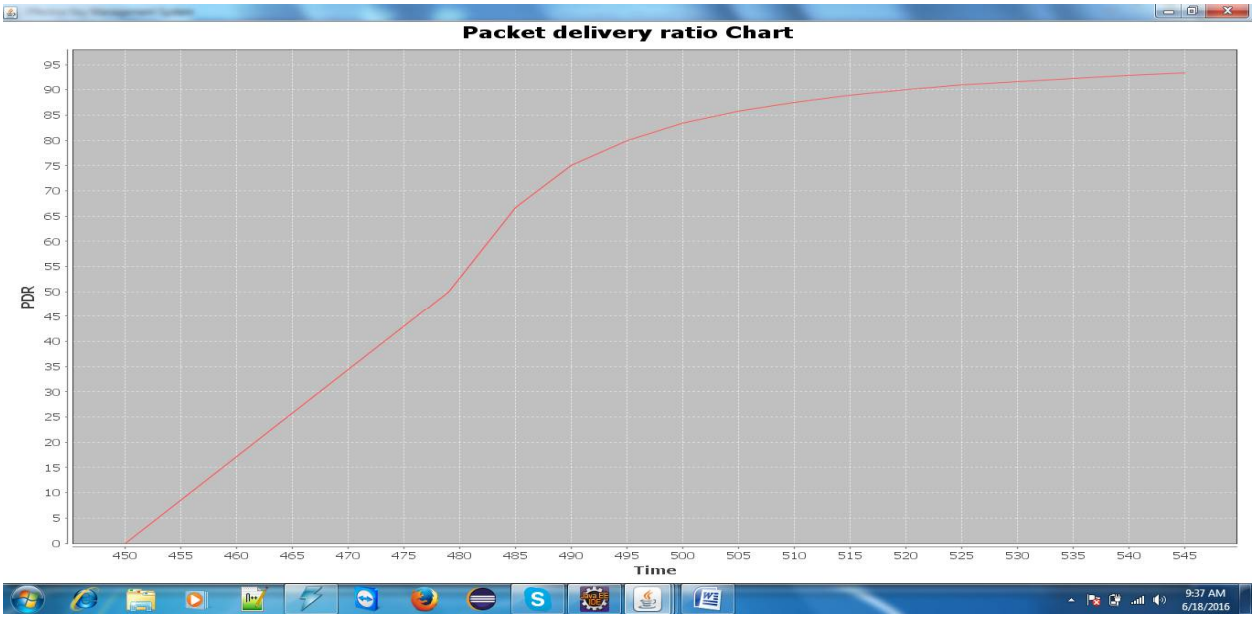
(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

2. THROUGHTPUT CHART



3. PACKAET DELIVERY RATIO CHART



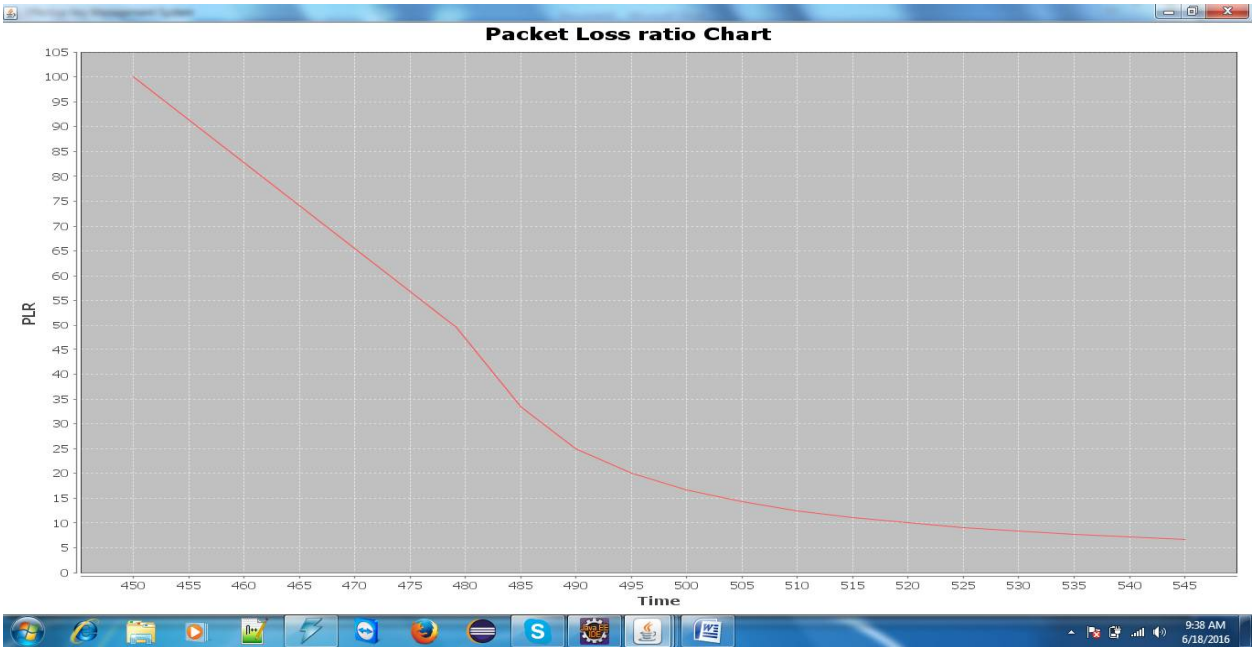
ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

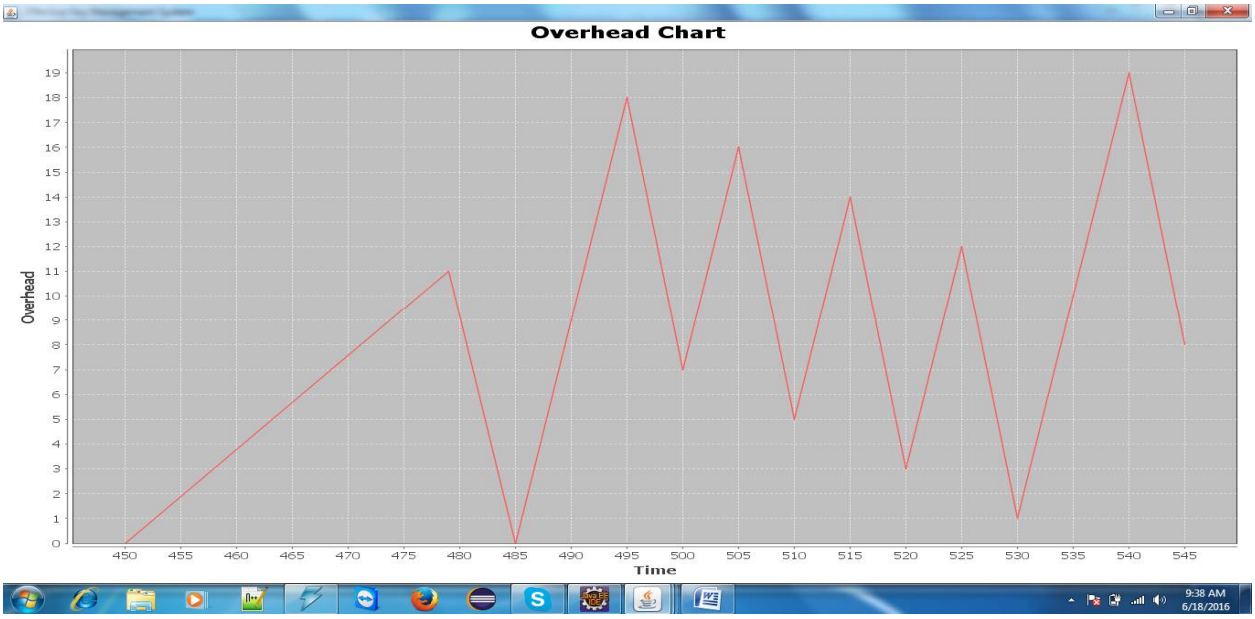
(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

4. PACKAET LOSS RATIO CHART



5. OVERHEAD CHART



VIII. CONCLUSION AND FUTURE WORK

This Project proposed to the pivotal affirmation less persuading key association convention (CL-EKM) for secure correspondence in part WSNs. CL-EKM bolster sparing correspondence for key redesigns and association once an inside point leaves or joins a group and instantly guarantees forward and in inverse key conundrum. Our subject is

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

adaptable against focus trade off, cloning and mimics ambushes and secures the information assurance and uprightness. This try tend to display a substitution subject which will be utilized for advancement differed keys (pair astute keys, way keys and bunch keys) for remote gadget systems. It can do exuberant validity while not drive checks and correspondences. The examination result demonstrates the execution of TKLU is new. Assistant in nursing centrality skilled part key association point mishandle the EBSs, polynomials and question symmetry keys. EEDKM gives limited rekeying which is sensibly performed not puncturing the opposite sections of WSN. Since EEDKM utilizes independently symmetric key between the four year certification and sensor focus point, it will promise the inside point and performs rekeying more centrality quickly than LOCK inside the higher layer. EEDKM is extra adaptable than general key association course of action upheld the EBSs and polynomial keys. In this way rekeying is performed less of times. These numerical models are used to gage the right worth for the Told and Takeoff for parameters kept up the pace other than the required trade between the essentialness use in addition 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.