iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** X **Month of publication:** October 2017

DOI: http://doi.org/10.22214/ijraset.2017.10230

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue X, October 2017- Available at www.ijraset.com

EKM-Cl: Novel Framework for Key Management in Dynamic Wireless Sensor Networks

Raksha R S[1], Shiva Murthy G[2], Ramakrishna Prasad A L[3]
[1, 2, 3] *Department of Computer Science and Engineering, Visvesvaraya Technological University, Center for Postgraduate Studies, Muddenahalli, Chikkaballapur - 562101, India*

Abstract: ***Key management has remained a difficult issue in wireless device networks (WSNs) as a result of the constraints of device node resources. Various key management schemes that trade off security and operational necessities are proposed in recent years .Wireless device Networks (WSNs) comprises tiny sensor nodes with strained energy, memory and computation capabilities. They are typically deployed within the unattended and hostile environment. So device nodes area unit susceptible to attacks such as node capture and collusion attack by adversaries. In this paper, we tend to propose a certificate less-effective key management (CLEKM) protocol for secure communication in dynamic WSNs characterized by node mobility. The sending node first calculates the best shortest path to the base station and sends the key updates. A security analysis of our theme shows that our protocol is effective in defensive against varied attacks. We tend to implement CL-EKM in Conic OS and simulate it exploitation Cola machine to assess its time, energy, communication, and memory performance.***
Keywords: Key Management; Wireless Sensor; Cola machine; node mobility;

I. INTRODUCTION

Dynamic wireless sensor networks (WSNs) which empower portability of sensor hubs, encourage more extensive system scope and more precise administration than static WSNs. There-fore, dynamic WSNs are by and large quickly embraced in checking applications, for example, target following in battlefield reconnaissance, social insurance frameworks, traffic flow and vehicle status observing, dairy cows wellbeing observing [9]. In any case, sensor gadgets are powerless against pernicious assaults, for example, pantomime, block attempt, catch or physical decimation, due to their unattended agent conditions and slips by of availability in remote correspondence [20]. Accordingly, security is one of the most imperative issues in numerous basic dynamic WSN applications. Dynamic WSNs in this manner need to address key security prerequisites, for example, hub validation, information confidentiality furthermore, honesty, at whatever point and wherever the hubs move To address security, encryption key administration conventions for dynamic WSNs have been proposed in the past in view of symmetric key encryption [1]– [3]. Such sort of encryption is appropriate for sensor hubs due to their constrained vitality and preparing capacity. Notwithstanding, it experiences high correspondence overhead and requires expansive memory space to store shared pair wise keys. It is likewise not adaptable and not flexible against bargains, and unfit to help hub portability. Thus symmetric key encryption is not appropriate for dynamic WSNs. All the more as of late, awry key based approaches have been proposed for dynamic WSNs [4-7], [10], [15]. These methodologies exploit of public key cryptography (PKC, for example, elliptic bend cryptography (ECC) or Identity based public key cryptography (ID-PKC) so as to streamline key foundation and information validation between hubs. PKC is generally more costly than symmetric key encryption as for computational expenses. Be that as it may, late changes in the execution of ECC [11] have exhibited the plausibility of applying PKC to WSNs. We tend to show the safety weaknesses of existing ECC based mostly key management schemes for dynamic WSNs. CL-EKM supports four sorts ofkeys, every of that is used for a special purpose, as well as secure pair-wise node communication and group-oriented key communication among clusters. Economical key management procedures area unit outlined as supporting node movements across completely different clusters and key revocation method for compromised nodes.

II. RELATED WORK

According to the secure communication demand in WSN, 2varietiesofkeyinstitution are needed. One is pair wise key institution; the opposite is cluster key institution. A few schemes has beenprojectedthatincorporates3phasesnormally [10]:(1) key setup before deployment, (2)shared-key discovery once preparation, and (3) path-key institution if 2sensor no desdon't share an on the spot key. The most in style pair wise key pre-distribution answer is Random Pair wise Key theme [11] which addresses unessential storage

©IJRASET (UGC Approved Journal): All Rights are Reserved

drawbackand providessome key resilience.It's supportedErodesandReni's[12]work.Every sensing element node stores a random set of Nape pair-wise keys to achieve chance p that2nodes areconnected. Neighboring nodes will tellif they share a common pair-wise key once theysend andreceive "Key Discovering"Message inside radio range. Its defect is that it sacrifices key property to decrease the storageusage. Closest (location-based) pair-wise keys pre-distribution theme [13] is another to Randompair wisekey scheme. It takes advantage of thesituation data toenhancethekey connectivity.Later on, Random key-chain based mostly key pre-distributionanswer is another random keypre-distributionsolution that originatedfrom theanswer of basic probabilistickeyredistributionscheme [14]. It depends on probabilistic keysharing among the nodes of a random graph.

There are many key reinforcement proposals to strengthen security of the established link keys, andimprove resilience. Objective is to firmly generatea novel link or path key by using established keys,so the secret's not com- secure once one or a lot ofsensing element node is captured. One approach isto extend quantity of key overlap needed in sharedkey discovery phase. Q-composite random key predistribution theme [11] needs letter common keysto establish a link key. Similar mechanism isprojected by Pair-wise key institution protocol [15]that uses threshold secret sharing for keyreinforcement. The key reinforcement solutions in general increase process and communicationquality; however give smart resilience in the sense that compromised key-chain doesn't directly havean effect on security of any links within the WSN.But, it should be doable for Associate in Nursingoppose to re-cowl initial link keys. Associate inNursing oppose will then recover strengthened linkkeys from therecorded multi-path reinforcementmessages once the link keys are compromised. Symmetric key schemes don't seem to be viable for mobile detectornodes and so past approaches havetargetedsolely on static WSNs. a coupleof approaches are planned supported PKCtosupport dynamic WSNs. Thus, duringthissection, we review previous PKC-based keymanagementschemes fordynamicWSNs andanalyze theirsecurity weaknesses or disadvantages. Chuang et al. [7] and Agawam et al. [8] planned a two-layered key management theme and a dynamickey update protocol in dynamicWSNssupportedtheDaffier-Hellman (DH), severally. However,bothschemes don't seem to be fitted to sensors with restricted resources and areaunitunabletoperform valuable computationswith massive keysizes (e.g. a minimum of 1024 bit). Since computer code is computationally additionaleconomical and features a short key length (e.g. 160 bit), many approacheswithcertificate areplanned supported computer code. However,sinceevery node should exchange the certificate to ascertain thepair wisekey and verify every other's certificate before use, the communication and computation overheadincrease dramatically. Also, the BS suffers from the overhead ofcertificate management. Moreover, existingschemes don't seem tobesecure.

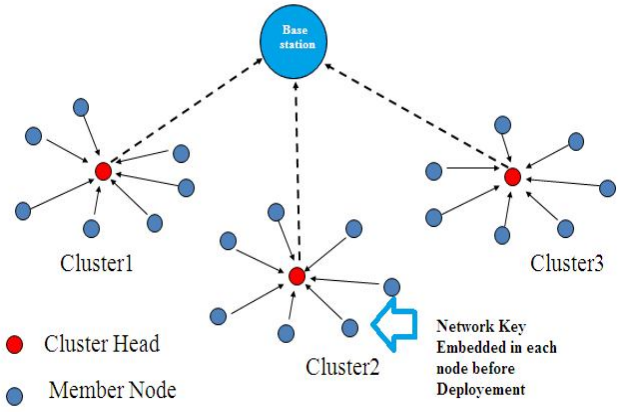


Fig 1: Wireless Sensor Networks Architecture

III. SYSTEM MODEL& ANALYSIS METRICS

A. System Model

The basic system model of this paper is pictured inFigure.1.It consists of 1 BS and lotsof uniform sensing element nodeswith distinctive ID. It uses cluster and two-layer design forscalability.Everyclusterhas some key generation nodes (KGNs) that distribute point keys among that cluster. TheseKGNs is also the final sensing elementnodes elect by clusterheads (CHs).We assume that the fundamental system model is deployed forthepurpose of watching thehostile atmosphere. End-to-endnode communication is unusual as a result of sensing element nodes in eachclustermonitor the finite space. For theinfo aggregation,there squaremeasureseveral communicationsbetween the nodes among the same cluster.Thus, the most task of thismodel couldbe a information transferfrom sensing element nodes to BS and aninformation aggregation in every cluster.

©IJRASET (UGC Approved Journal): All Rights are Reserved

IV. PROPOSED SCHEME

This paper introduces an Energy-Efficient Dynamic KeyManagement (EEDKM)proposalthat uses two-layer architecture. In the lower layer, similar to LOCK, rekeying isperformedconfinedusing the EBS and the t-degreevicariatepolynomial. 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 performedusing the secretkey between BS and sensor node. The secretkey isloadedbeforein each sensor node with unique ID and authenticates the node to the BS. The BS generates one t-degree vicariatepolynomial key and distributes it by meansof sessionkey shared by all CHs. This makes the communication betweenCHs efficient. The rest of this section describes the bootstrapping, initialkey distribution mechanism and some general operations in our key management scheme. This may help you to understand our scheme.

V. OVERVIEW OF THE CERTIFICATE LESS EFFECTIVE KEY MANAGEMENT AND SECURITY MODEL SCHEME

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 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. 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.

The CL-EKM is comprised of 7 phases: system setup,pair wisekey generation, cluster formation, key update, node movement, key revocation, and addition of a new nodeSecure key managementthemefor WSNs supporting mobilenodes, thefollowing security properties are critical:mobilenodes, thefollowing security properties are critical.

A. 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.

B. Resistance Against biological research and Impersonation:

The scheme should support no deauthenticationto safe guard against node replication and impersonation attacks.

Forward and Backward Secrecy: The theme should assure forward secrecy to forestall a node from exploitation Associate in nursingpreviouskeyto 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 antecedentlyexchangedmessages encryptedwith previous keys. Forward and backward secrecyare accustomed defend againstnodecapture attacks.

C. System Setup

Before the network deployment, the BS generates system parameters and registers the node by including it in a member list M.

1) Generation of System Parameters: The KGC at the BS runs the following steps by taking a security parameter
k ∈ Z+ as the input, and returns a list of system parameter= {Fq, E/Fq, Gq, P, Ppub= x P, h0, h1, h2, h3} and x.
Choose a k-bit prime q
Determine the tuple {Fq, E/Fq, Gq, P}.
Choose the master private key x ∈R Z∗q and compute the system public key Ppub= x P.
Choose cryptographic hash functions {h0, h1,h2, h3} so that h0 : {0, 1}∗ × G2 q → {0, 1}∗, h1 :G3 q × {0, 1}∗ × Gq→ {0, 1}n, h2 : Gq× {0, 1}∗ × Gq× {0, 1}∗ × Gq× {0, 1}∗ × Gq→ Z∗q, andh3 : Gq×{0, 1}∗×Gq×{0, 1}∗×Gq×{0, 1}∗×Gq→ Z∗q. Here, n is the length of a symmetric key. The BS publishesand keeps x secret.

2) Node Registration: The BS assigns a unique identifier, denoted by Li , to each L-sensor nLiand a unique identifier,denoted by H j, to each H -sensor n H j , where $1 \leq i \leq N1$, $1 \leq j \leq N2$, $N = N1 + N2$. Here we describe the certificateless public/private key and individual node key operations for Li , the same mechanisms apply for H -sensors. During initialization, each node nLichooses a secret value xLi∈R Z∗q and computes PLi= xLi P. Then, the BS requests the KGC for partial private/public keys of nLiwith the

©IJRASET (UGC Approved Journal): All Rights are Reserved

input parameters Li and PLi. The K GC chooses rLi∈R Z∗q and then computes a pair of partial public/private key (RLi ,dLi) as below:

RLi= rLi P dLi= rLi+ x · h0(Li, RLi, PLi) mod q The Li can validate its private key by checking whether the condition dLi P = RLi+ h0(Li, RLi , PLi)Ppubholds

D. Cluster Formation

Node Discovery and Authentication
$n_{H_j} \rightarrow *$: $\langle H_j, pk_{H_j} \rangle$
(for $i = 1, ..., n$)
$n_{L_i} \leftrightarrow n_{H_j}$: Perform *Pairwise Key Generation* phase

Cluster Key Generation
(for $i = 1, ..., n$)
n_{H_j} : Generate GK_j, Compute $C_2 = E_{k_{L_i H_j}}(GK_j, H_j, L_i)$
$n_{H_j} \rightarrow n_{L_i}$: $\langle H_j, C_2 \rangle$
n_{L_i} : Decrypt C_2 to get GK_j and
Compute $C_3 = E_{k_{L_i H_j}}(L_i, HMAC(k_{L_i H_j}, GK_j))$
$n_{L_i} \rightarrow n_{H_j}$: $\langle L_i, C_3 \rangle$
n_{H_j} : Decrypt C_3 and Check the validity

Membership Validation
n_{H_j} : Compute $C_4 = E_{K^0_{H_j}}(H_j, \mathfrak{M}_j)$, $C_5 = E_{GK_j}(H_j, \mathfrak{M}_j)$
$n_{H_j} \rightarrow$ BS : $\langle H_j, C_4 \rangle$
BS : Check $\mathfrak{M}_j$
BS $\rightarrow n_{H_j}$: $\langle Acknowledgement \rangle$
$n_{H_j} \rightarrow *$: $\langle C_5 \rangle$

VI. 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.

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

VII. CONCLUSION AND FUTURE WORK

This paper proposed to the primary certificate less effective key management protocol (CL-EKM) for secure communication in dynamic WSNs. CL-EKM support economical communication for key updates and management once a node leaves or joins a cluster and thence ensures forward and backward key secrecy. Our theme is resilient against node compromise, cloning and impersonation attacks and protects the info confidentiality and integrity. This paper have a tendency to introduce a replacement theme which will be used for establish varied keys (pair wise keys, path keys and cluster keys) for wireless device networks. It is able to do quick credibility while not further computations and communications. The experiment result shows the performance of TKLU is fresh. Associate in nursing energy-efficient dynamic key management theme victimization the EBSs, polynomials and secret symmetry keys. EEDKM provides localized rekeying which is effectively performed not poignant the opposite elements of

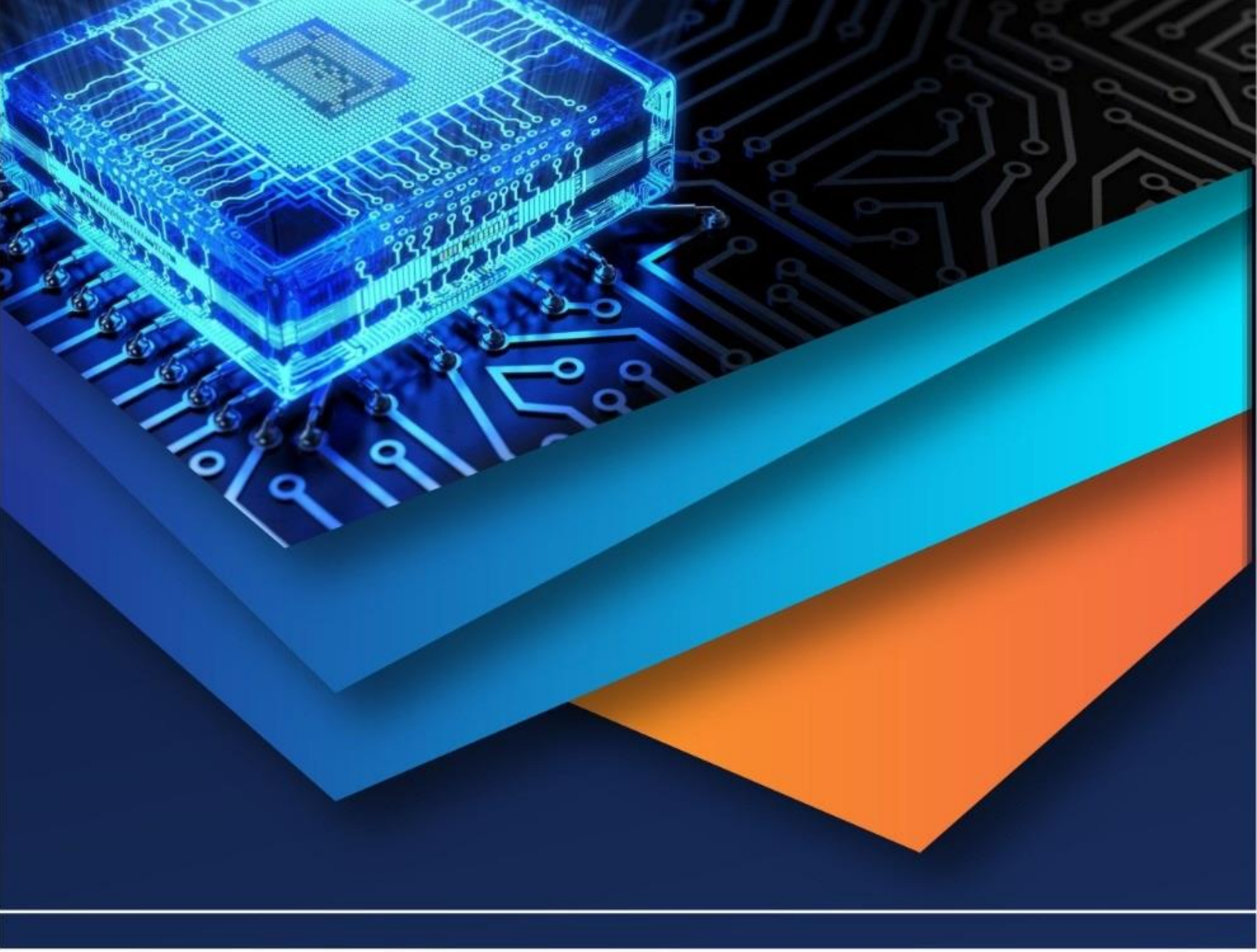
©IJRASET (UGC Approved Journal): All Rights are Reserved

WSN. The BS suffer from mere problem of poor encryption. Since it has four pairs of keys it is not a serious issue. Still the user or the beneficiary authority has to go for more securely encrypted key methods. This problem can be revised and solved and hence to improve this idea of secure data handling. Encryption improvement is the only method to get the most secured way of communication.

REFERENCES

[1] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," in Proc. IEEE Symp. SP,
[2] W. Du, J. Deng, Y. S. Han, and P. K. Varshney, "A key predistributionscheme for sensor networks using deployment knowledge," IEEE Trans.Dependable Secure Comput., vol. 3, no. 1, pp. 62–77, Jan./Mar. 2006.
[3] W. Du, J. Deng, Y. S. Han, P. Varshney, J. Katz, and A. Khalili,"A pairwise key predistribution scheme for wireless sensor networks,"ACM Trans. Inf. Syst. Secur., vol. 8, no. 2, pp. 228–258, 2005.
[4] Distrib.Comput., vol. 70, no. 8, pp. 858–870, 2010
[5] 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
[6] D. S. Sanchez and H. Baldus, "A deterministic pairwise key pre-distribution scheme for mobile sensor networks," in Proc. 1st Int. Conf.SecureComm, Sep. 2005, pp. 277–288.
[7] I.-H. Chuang, W.-T. Su, C.-Y. Wu, J.-P. Hsu, and Y.-H. Kuo, "Two-layered dynamic key management in mobile and long-lived cluster-based wireless sensor networks," in Proc. IEEE WCNC, Mar. 2007,pp. 4145–4150
[8] S. Agrawal, R. Roman, M. L. Das, A. Mathuria, and J. Lopez, "A novelkey update protocol in mobile sensor networks," in Proc. 8th Int. Conf.ICISS, vol. 7671. 2012, pp. 194–207.
[9] S. U. Khan, C. Pastrone, L. Lavagno, and M. A. Spirito, "An energy andmemory-efficient key management scheme for mobile heterogeneous sensor networks," in Proc. 6th Int. Conf. CRiSIS, Sep. 2011, pp. 1–8.
[10] X. Zhang, J. He, and Q. Wei, "EDDK: Energy-efficient distributed deterministic key management for wireless sensor networks," EURASIPJ. Wireless Commun. Netw., vol. 2011, pp. 1–11, Jan. 2011.
[11] N. Gura, A. Patel, A. Wander, H. Eberle, and S. C. Shantz, "Comparingelliptic curve cryptography and RSA on 8-bit CPUs," in Proc. 6th Int.Workshop Cryptograph. Hardw. Embedded Syst., 2004, pp. 119–132.
[12] S. S. Al-Riyami and K. G. Paterson, "Certificateless public keycryptography," in Proc. 9th Int. Conf. ASIACRYPT, vol. 2894. 2013,pp. 452–473.
[13] S. Seo and E. Bertino, "Elliptic curve cryptography based certificateless hybrid signcryption scheme without pairing," CERIAS, West Lafayette,IN, USA, Tech. Rep. CERIAS TR 2013-10, 2013. [Online]. Available:https://www.cerias.purdue.edu/apps/reports_and_papers/.Seung-Hyun
[14] S. H. Seo, J. Won, and E. Bertino, "POSTER: A pairing-free certificate-less hybrid sign-cryption scheme for advanced metering infrastructures,"in Proc. 4th ACM CODASPY, 2014, pp. 143–146.
[15] Q. Huang, J. Cukier, H. Kobayashi, B. Liu, and J. Zhang, "Fastauthenticated key establishment protocols for self-organizing sensor networks," in Proc. 2nd ACM Int. Conf. WSNA, 2003, pp. 141–150.
[16] X.-J. Lin and L. Sun, "Cryptanalysis and improvement of a dynamicand secure key management model for hierarchical heterogeneous sensor networks," in Proc. IACR Cryptol. ePrint Archive, 2013, pp. 698–698.
[17] P. Szczechowiak, L. B. Oliveira, M. Scott, M. Collier, and R. Dahab,"NanoECC: Testing the limits of elliptic curve cryptography in sensornetworks," in Proc. 5th Eur. Conf. WSN, vol. 4913. 2008, pp. 305–320.
[18] K. Chatterjee, A. De, and D. Gupta, "An improved ID-based keymanagement scheme in wireless sensor network," in Proc. 3rd Int. Conf.ICSI, vol. 7332. 2012, pp. 351–359.

©IJRASET (UGC Approved Journal): All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)