Dynamism and Reminiscence-Capable Key Management Technique for Portable Heterogeneous Sensor Networks

S.Thylashri[1], C.Shanmuganathan[2], Dr.P.Raviraj[3]
[1]P.G.Student, Department of CSE, St.Peter's College of Engineering & Technology, Chennai, 600054, India
[2]Research Scholar, Department of CSE ,Manonmaniam Sundaranar University , Tirunelveli, 627012, Tamilnadu, India
[3]Prof.& Head, Department of CSE, Kalaigner Karunanidhi Inst.of Tech, Coimbatore, 641402,Tamilnadu, India

Abstract *— Wireless Sensor Network (WSN technology is being gradually more adopted during a big variety of applications loco mote from home/building and industrial automation to additional safety critical applications together with e-health or infrastructure monitoring. Considering quality within the on top of application scenarios truly introduces further technological challenges, especially with regard to security. The resource aberrant devices be supposed to be strong to numerous security attacks and communicate firmly whereas they 're residence the thought-about environment to the current aim, correct authentication and key management schemes supporting node quality should be used. This paper presents an efficient mutual authentication and key establishment theory for heterogeneous sensor network consisting of various mobile Sensor nodes and solely some additional powerful fixed sensor nodes. The obtained results show that the proposed resolution assures higher network propert y, consumes less memory, has low communication overhead throughout the authentication and key establishment section and has higher network resilience against mobile nodes attacks compared with existing approaches for authentication and key establishment.*

Keywords — *Wirless Sensor Networks, Key Management, Security; Heterogeneous Networks, Portable Nodes.*

I. INTRODUCTION

Wireless sensor networks (WSNs) comprise of an extensive number of small, scruffy, computational, and vitality obliged sensor nodes. They have increased various applications, for example, scrutiny, target following, and military fields for information assembling and handling. Sensor nodes are haphazardly conveyed in uncommon zones to gather data. Subsequent to the information bundles are transmitted over the air, it is not difficult for the enemies to take data by listening in. To ensure the confidentiality of data transmitted between sensor nodes, the messages ought to be encoded before being transmitted. It is an incredible test to execute encryption algorithms in remote sensor systems as a result of the obliged asset. Besides, malignant nodes might imitate to be authentic nodes and correspond with other substantial nodes. This might subvert the entire networks.

The natural WSN attributes including resources shortage, constrained correspondence transfer speed and ad-hoc networking capability present numerous difficulties additionally as for secure correspondence. To guarantee a specific level of security, particular countermeasures should be chosen so as to shield the nodes from various possible attacks. Be that as it may, the restricted assets obstruct the selection of traditional security approaches. As a result, new security arrangements suitable for WSNs are being characterized. All the more particularly, key management can be considered as the fundamental establishment whereupon other security primitives are manufactured. Specialists have proposed various key management plans in the literature.

Asymmetric cryptography (RSA) and the EllipticCurve Cryptography (ECC) were at first considered not to be suitable for most sensor applications because of their high computational cost, vitality utilization and capacity necessities. By the by, late studies demonstrated that public key cryptography, for example, Elliptic Curve (because of little key size and low computational overhead) and Rabin's plan (because of quick encryption/unscrambling time contrasted with RSA) may be plausible even in sensor systems [4][3].

WSNs can be fundamentally isolated into two primary classes (1) homogeneous sensor networks and (2) heterogeneous sensor networks. Homogeneous sensor systems pulled in the vast majority of the scientist's considerations in adding to the security algorithms. In any case, their key adaptability and performance restrictions, demonstrated by both theoretical and simulation analysis [9], constrained specialists to consider Heterogeneous Sensor Networks (HSNs) joining a blend of nodes with generally differing abilities. Yarvis [5] increments normal conveyance rate and arrange life time without introducing so as to expand the expense vitality and join heterogeneity alongside the best possible organization of HSNs. Duarte-Melo and Liu investigated vitality utilization and life time of HSNs in by giving intermittent information from the sensing field to remote recipient.

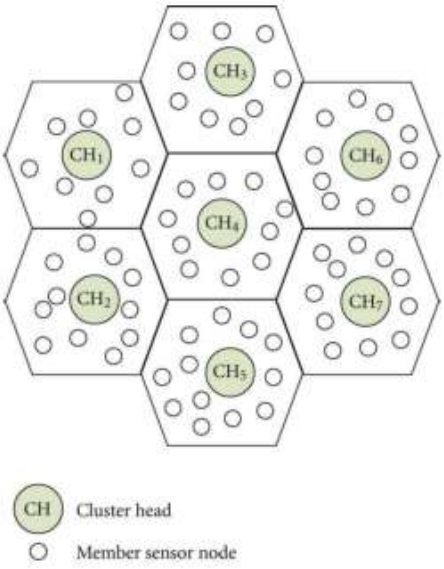

Fig 1. Heterogeneous Wireless Sensor Network

This paper proposes an online key generation and management plan for HSNs, developing the work exhibited in [1]. The primary commitment of this paper is to diminish the correspondence overhead and *energy* utilization by streamlining the *initial node* validation step, which is crucial to keep the *energy* expense of the general approach low. This paper likewise presents a *novel mutual authentication and key establishment* method keeping up better system availability and flexibility against *node capture attacks* contrasted with contending approaches.

II. RELATED WORK

This part gives a overview of key management schemes that have been displayed in literature for both homogeneous and heterogeneous WSNs. Perrig et al. [7] displayed SPINS, an centralized keying technique for sensor systems in which every node contains a secret key whose relating key is put away in the base station and utilizes one-way hash chains for making an age postponed key discharge component for the utilization in validated show. On the other hand, two sensor nodes can't have a typical secret key straightforwardly. In the event that two nodes A and B need to set up a correspondence key with one another, A sends a request to B, which makes and advances a token to the base station. The base station then produces a session key for A and B, encodes it with the mystery keys that it offers with A and B and after that sends scrambled information to A and B separately. Subsequent to the node utilize the base station as a trusted server to set up a secret key, this plan won't work if the base station is not reachable or has a high correspondence overhead, particularly on account of multi- hop correspondence.

Eschenauer and Gligor [8] proposed an random key predistribution plot that does not require the base station for The key establishment between any two nodes. By scheme,a set of arbitrarily chose keys from a substantial pool is doled out to every sensor nodes before the system sending. Two nodes convey straightforwardly to set up a secret key just in the event that they have no less than one key in like manner. Chan further enhanced The security of [8] by presenting the "q keys"concept. To build up a secret key,two nodes must share atleast q keys however this plan requires putting away countless in every sensor nodes. Liu exhibited a key establishment plan utilizing a former learning of hub arrangement combined with Rabin's plan toachieve a high level of availability (while diminishing the memory cost) and organize strength against the node capture attacks. Zhang exhibited the NPKPS pairwise key predistribution plan for WSNs to accomplish better security, availability and proficiency and less memory cost contrasted with [8]. Efficient authentication plans are proposed to enhance over past work as far as security, validation overhead and capacity necessities.

With a specific end goal to introduce a key management conspire that lessens energy cost and bolsters node versatility, Kim proposed a level-based key management plan for multicast correspondence that has sensible directing overhead and low portability management overhead. For portability bolstered cluster based WSNs, a two-layered dynamic key management plan was proposed by Chuang while polynomial-based key pre-distribution plan for mobile sensor systems was proposed by Blundo. Sarmad [1] exhibited a runtime key generation plan for the verification and mystery key foundation to lessen the memory cost and build the system flexibility. Camtepe and Yener proposed a combinatorial outline approach for key pre-distribution. To begin with they proposed a straightforward key pre- distribution plan in light of Finite Projective Plane (FPP) which gives direct key establishment, resistance to node capture and no computational and correspondence overhead, however with restricted system adaptability and strength and without node authentication.. Their hybrid approach enlarges adaptability of the initial plan to the expense of giving up direct network.

Sanchez and Baldus [6] apply a FPP configuration to the predistribution of Blundo polynomial shares. Their methodology Enables direct pairwise key foundation for countless free of the physical availability of the WSN.To diminish the memory overhead and bolster hub versatility among diverse systems, Maerien [2]proposed the MAnagement of Secret keYs convention (MASY) for portable WSNs which allocates to a node one and only symmetric

key, shared just with the back-end server of its system, and which expect a trust relationship between the recently entered system and the node 's old guardian network.

III. PROPOSED SCHEME

In this segment, the proposed key establishment plan for HSNs is introduced. The reference system model characterizes a HSN made out of a Base Station (BS), Fixed Nodes (FNs) and Mobile Nodes (MNs). These nodes are heterogeneous regarding computational force, memory and energy resources. On the other hand, the same correspondence innovation is received. The BS and the FNs are intense gadgets while MNs are described by exceptionally restricted assets and can change their position inside of the given environment taking after a particular portability model. In addition, the MNs are a bigger number of various than the FNs, and just the FNs should be outfitted with alter safe equipment.

In this subsequent situation, the BS just corresponds with the FNs and goes about as a trusted server for them. To address adaptability issues, a group based methodology has been embraced. Indeed, FNs go about as Cluster Heads (CHs) and are responsible for managing authentication and key establishment operations for a gathering of MNs.

A. Key Pre-Allocation

In this area, key pre- distribution among the FNs and the MNs is depicted. A secret key (SK) is alloted to each MN; all the more particularly, such key is produced utilizing a Secret Key Generator (SKG), a prime number that is pre-relegated to every MN of the system (MNPN), and the two arbitrarily created prime numbers utilizing a restricted secret key generation function f( ).

Each FN is furnished with public key of the BS, its own particular the accompanying key material: public/private key pair, a one way authentication key generation function *g(),*a Secret Key Generator (SKG) and a one way Secret key generation function *f( ),* a Compromised Node Detection Key (CNDK) and a system private key (K prt) alongside its own prime. It is significant that FNs should likewise execute a quick key revocation algorithm keeping in mind the end goal to secure the Secret Key Generator (SKG) and the system private key.

Similarly as the MNs are concerned, the accompanying key material is viewed as: a secret key (SK), a network public key K plc, an authentication key K auth. , the Fixed Node Prime Number Sum (FNPNS), its own prime number and an arbitrary number.

B. Cluster Development

Once the system is deployed, FNs begin the cluster formation stage. Amid the cluster formation stage, all the FNs intermittently show a Hello messages to neighboring MNs for a given number of times . Such messages incorporate nodes IDs and an irregular nonce scrambled utilizing the system private key. It is expected that the FNs are conveyed such that most MNs get Hello messages from more than one FN. The choice of FN as a CH relies on upon the Hello message signal quality. Every MN additionally keeps a rundown of neighboring FNs from which it has gotten Hello messages to perhaps recognize reinforcement CHs. On the off chance that, for reasons unknown, the MNs don't get any FN Hello message inside of a given time period, they begin broadcasting Hello message including a nonce scrambled by the system *public* key to find credible neighboring FNs.

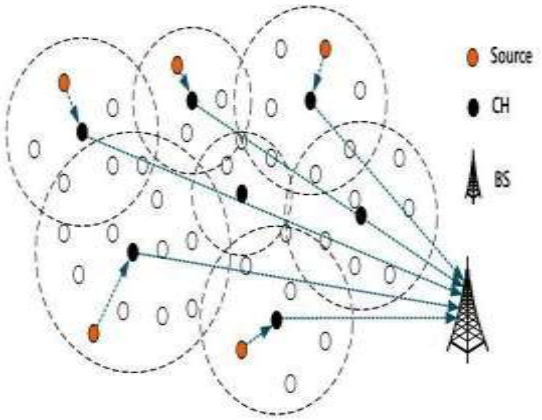

Fig 2. Clustering

C. Portable Nodes Substantiation

To access the system, every MN needs to validate itself with a chose CH. To do as such, the MN sends a “Join request” encoded utilizing the system *public* key. The solicitation incorporates the Fixed Node Prime Number Sum, an arbitrary number identified with its confirmation key and the nonce gave inside of the Hello Message sent by the chose CH alongside its own prime number scrambled by MN's validation key. When gotten such data, the CH can surmise the validation key of the MN by utilizing one way confirmation key generation function *g()* as takes after

Kauth = g(FNPNS, random number, SKG)

Prolific decryption of the encrypted nonce and MN prime number by the CH utilizing the derived Kauth demonstrates the MN genuineness. It is important that the utilization of SKG in
Kauth generation ensures that a proper FN is really producing the Kauth and that MN prime number is not revealed to any rival node. After the authenticity

check, the FN sends the joining affirmation and a Network Authentication Code (NAC) to the MN. This is utilized to decrease the authentication load while the MN travels through various clusters inside of the same system. The Network Authentication Code is likewise intermittently overhauled as a countermeasure to
replay attacks or node replication attacks performed by a rival.

D. Key Establishment and Management

To secure correspondence between the CH and the MN, every MN is doled out a secret key SK while its generation function is doled out to the FNs before the deployment. Amid the authentication stage, each CH gets the MN prime quantities of its part MNs. CHs utilizing these MN prime numbers and the secret key generator SKG create the first prime number utilizing prime number generator (PN1); this prime number is further consolidated with the MN prime numbers and secret key generator SKG to produce the second prime number (PN2). At that point, the CH produces the required secret key utilizing a *one way* secret key *generation function f( )*, accordingly acquiring the same secret key claimed by the particular MN
Secret key = f(PN1, PN2, MNPN, SKG)

For secure correspondence between the MNs, a secret key between them is created by the CH. For example, if a mobile node A needs to set up an immediate correspondence join with portable node B, it sends its IDA alongside the IDB to its CH. At that point the CH produces a secret key for them utilizing their IDs, prime numbers and *one way* secret key *generation function f( )* and sends it to both MNs utilizing the secret key imparted to each of them. CHs additionally occasionally educate the BS about their part MNs to maintain a strategic distance from the node replication attacks in the system.

IV. PERFORMANCE EVALUATIONS

In this section, we evaluate and compare the performance of the ECC Method along with the proposed method. Simulation results show that our proposed scheme satisfies higher network property, consumes less memory, has low communication overhead and withstands all node attacks.
Fig. 3 shows the result after performance evaluation. The x-axis gives the number of nodes and the y-axis indicates the memory consumption. The diagram gives the reasonable shot of the memory consumed by the nodes.

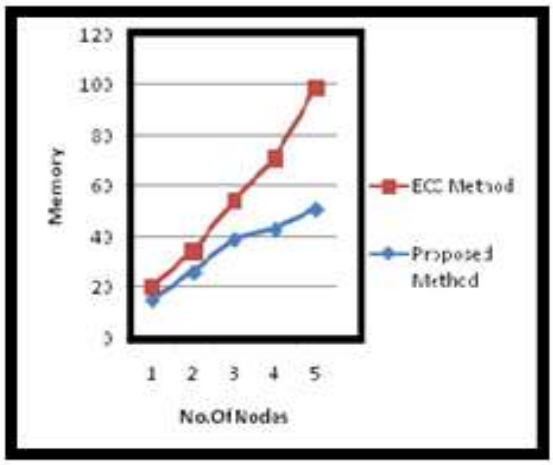

Fig.3. Analysis graph for Memory Consumption in various nodes

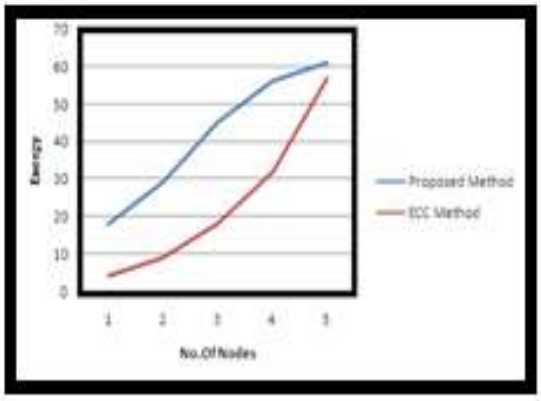

Fig.4.Analysis graph of Energy Consumption for key Generation

The next graph i.e. Fig. 4, the correlation between key Generation got to against the energy or the energy taken for processing these Keys. The graph clearly indicates how the proposed method is ended up being quicker when contrasted with that of the ECC method.

V. CONCLUSION

In this paper, a key management plan is proposed for cluster based heterogeneous sensor systems. In examination with existing methodologies, the proposed arrangement gives better system availability, diminishes memory overhead, increments system versatility against node capture attacks and requires least correspondence overhead amid the authentication and key establishment stages. Consequently it saves battery energy and increases the network life time.

REFERENCES

[1] Khan, Sarmad Ullah; Lavagno, Luciano; Pastrone, Claudio; Spirito, Maurizio; ,"An effective key management scheme for mobile heterogeneous sensor networks," *Information Society (i-Society), 2011 International Conference on*, vol., no., pp.98-103, 27-29 June 2011.

[2] Maerien, J.; Michiels, S.; Huygens, C.; Joosen, W.; , "MASY: MAnagement of Secret keYs for federated mobile wireless sensor networks," *Wireless and Mobile Computing, Networking and Communications (WiMob), 2010 IEEE 6th International Conference on* , vol., no., pp.121-128, 11-13 Oct. 2010.

[3] Xiaojiang Du; Yang Xiao; Song Ci; Guizani, M.; Hsiao-Hwa Chen; , "A Routing Driven Key Management Scheme for Heterogeneous Sensor Networks," *Communications, 2007. ICC07.IEEE International Conference on*,vol.,no.,pp.3407-3412,24-28June 2007.

[4] Fang Liu, Maiou Jose "Manny " Rivera, Xiuzhen Cheng, "Location-Aware Key Management in wireless sensor networks", IWCMC'06, 2006.

[5] Yarvis, M.; Kushalnagar, N.; Singh, H.; Rangarajan, A.; Liu, Y.; Singh, S.; , "Exploiting heterogeneity in sensor networks," *INFOCOM 2005. 24th Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings IEEE* , vol.2, no., pp. 878- 890 vol. 2, 13-17 March 2005.

[6] Sanchez, D.S.; Baldus, H.;"A Deterministic Pairwise Key Pre-distribution Scheme for Mobile Sensor Networks," *Security and Privacy for Emerging Areas in Communications Networks, 2005. SecureComm 2005. First International Conference on* , vol., no., pp. 277- 288, 05-09 Sept. 2005.

[7] A. Perrig, R. Szewczyk, J. Tygar, Victorwen, and D. E. Culler, "Spins: Security Protocols for Sensor Networks", ACM Wireless Networking, Sept. 2002.

[8] L. Eschenauer and V. D. Gligor, "A key management scheme for distributed sensor networks", Proc. of the 9th ACM Conference on Computer and Communication Security, Nov. 2002. pp. 41-47.

[9] Kaixin Xu; Xiaoyan Hong; Gerla, M.; , "An ad hoc network with mobile backbones," *Communications, 2002. ICC 2002. IEEE International Conference on* , vol.5, no., pp. 3138- 3143 vol.5, 2002.

[10] Eduru Hariprasad, J.S.V.R.S.Sastry, N. Subhash Chandra "Vastly Efficient Key Pre Distribution and Authentication scheme for Wireless Sensor Networks,"*International Journal of Computer Science and Engineering (SSRG-IJCSE) – volume1 issue7 September 2014.*