International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 4 | Issue 2 | ISSN : 2456-3307

Implementation of Effective Key Management Strategy with Secure Data Aggregation in Dynamic Wireless Sensor Network

Shraddha Deshmukh[1], Prof. A. R. Bhagat Patil[2], Harshad Nakade[3]

[1]M.Tech Scholar, Department of Computer Technology, Yeshwantrao Chavan College of Engineering, Nagpur, Maharashtra, India
[2]Dean(P&D) & Associate Professor, Department of Computer Technology, Yeshwantrao Chavan College of Engineering, Nagpur, Maharashtra, India
[3]Wolters Kluwer Pvt. Ltd., Pune, Maharashtra, India

ABSTRACT

Wireless sensor networks (WSNs) have been passed on for a wide assortment of uses, including military detecting and following, understanding status observing, activity flow checking, where sensory contraptions as often as possible move between various territories. Securing data and correspondences requires reasonable encryption key conventions. In this paper, we propose a Certificateless-effective key management (CL-EKM) convention for secure correspondence in unique WSNs portrayed by hub versatility. The CL-EKM underpins capable key updates when a hub leaves or joins a cluster and guarantees forward and in reverse key mystery. The convention additionally underpins efficient key renouncement for exchanged off nodes and limits the impact of a hub exchange off on the security of other correspondence joins. A security examination of our arrangement exhibits that our convention is effective in guarding against various assaults. It is effective in time, vitality, correspondence, and memory execution. Likewise, we actualize Data gathering hub for correspondence inside cluster head and base station. The DCN is valuable when the cluster head is bargained hub and information sending without separation.

Keywords: Wireless Sensor Networks (WSN), Clustering, Relay cluster heads (RCH), Key Generation Centers (KGC), Elliptical Curve Cryptography (ECC), Certificateless Partial Key Generation.

I. INTRODUCTION

A wireless sensor organize (WSN) comprises of countless nodes, which are controlled by batteries, outfitted with detecting, information preparing and short-extend radio correspondence parts. The uses of WSNs go from the most prevalent ones, similar to condition observing and home computerization, to additionally requesting ones in military or security zones, similar to combat zone observation, focusing on and target following systems. In any case, the wireless availability, the nearby connection among sensor nodes and their unattended task, and the nonappearance of physical assurance make WSNs helpless against an extensive variety of system level assaults and even physical harm. Despite the fact that sensor nodes can be furnished with worked in alter protection systems, the memory chips are as yet experiencing different memory read-out vulnerabilities. Dynamic wireless sensor networks (WSNs), which empower portability of sensor nodes, encourage more extensive system scope and more exact administration than static WSNs. In this way, dynamic WSNs are as a rule quickly embraced in observing applications, for example, target following in front line reconnaissance, medicinal services systems, movement stream and vehicle status checking, dairy cows wellbeing checking. In WNS security is a standout amongst the most essential issues in numerous basic dynamic WSN applications. Dynamic WSNs in this manner need to address key security necessities, for example, hub authentication, information Efficient Key Management in Dynamic Wireless Sensor Network secrecy and honesty, at whatever point and wherever the nodes move.

Key administration is a center system to guarantee security in organize administrations and uses of WSNs. Key administration can be characterized as an arrangement of procedures and instruments that help key foundation and the upkeep of progressing keying connections between legitimate gatherings as per a security approach. Since sensor nodes in WSNs have limitations in their computational power and memory ability, security arrangements intended for wired and specially appointed networks are not appropriate for WSNs. The objective of key administration in WSNs is to tackle the issue of making, disseminating and keeping up those mystery keys. Consequently, methods for solid circulation and administration of these keys are of key significance for the security in WSNs.

To address security, encryption key administration conventions for dynamic WSNs have been proposed in the past based on symmetric key encryption. Such kind of encryption is appropriate for sensor nodes because of their restricted vitality and handling ability. Nevertheless, it experiences high correspondence overhead and requires huge memory space to store shared pairwise keys. It is likewise not versatile and not flexible against bargains, and unfit to help hub portability. In this manner, symmetric key encryption is not appropriate for dynamic WSNs.

To defeat this issue identified with key we introduce a declaration less viable key administration (CL-EKM) conspire for dynamic WSNs. In this system, we have made utilization of Key Generation Center (KGC) for incomplete private key age. By making utilization of KGC, we likewise the shot of key escrow issue.

II. LITERATURE SURVEY

H. Chan and et. al. in [1] presents three new systems for key foundation utilizing the structure of pre-conveying an irregular arrangement of keys to every hub. In the first place, in the q-composite keys conspire, they exchange of the implausibility of an expansive scale organize assault with a specific end goal to altogether fortify arbitrary key pre-conveyance's quality against littler scale assaults. Second, in the multipath-support conspire, they demonstrate to fortify the security between any two nodes by utilizing the security of different connections. At long last, they show the arbitrary pairwise keys plot, which splendidly safeguards the mystery of whatever is left of the system when any hub is caught, and furthermore empowers hub to-hub authentication and majority based denial.

W. Du, J. Deng and et.al in [2] propose a novel irregular key pre-conveyance conspire that endeavors sending learning and maintains a strategic distance from pointless key assignments. We demonstrate that the execution (counting availability, memory use, and system versatility against hub catch) of sensor networks can be considerably enhanced with the utilization of our proposed plot.

M. R. Alagheband and M. R. Aref [3] proposes a dynamic key administration structure based on circular bend cryptography and signcryption technique for heterogeneous WSNs. The proposed plot has arrange versatility and sensor hub (SN) portability particularly in fluid situations. Besides, both intermittent authentication and another enlistment instrument are proposed through counteractive action of SN bargain. The author examinations a portion of the more original various leveled heterogeneous WSN key administration plans and contrast them and the proposed conspire.

W. Du, J. Deng, and et. al [4] proposes another key pre-dissemination conspire, which sub stantially enhances the versatility of the system contrasted with the current plans. Their plan displays a pleasant limit property: when the quantity of bargained nodes is not as much as the edge, the likelihood that any nodes other than these traded off nodes are influenced is near zero.

I. - H. Chuang and et.al [5] proposed a two-layered dynamic key administration (TDKM) approach for cluster-based WSN (CWSN) is proposed. Both combine insightful key and gathering key are circulated in three rounds for key material trade without encryption/decoding and exponentiation activities in TDKM. In hypothetical investigation, TDKM is contrasted with other key administration conventions with demonstrate its effectiveness. Finally, the connections between the quantity of gatherings and the system execution including key age overhead, arrange security, and secured information transmission overhead in CWSN are dissected.

S. Agrawal and et.al in [6] propose a key refresh convention, which safely refreshes the session key between a couple of nodes with the assistance of irregular contributions to portable sensor networks. At first, a one of a kind ace key is acquired utilizing symmetric bivariate polynomial offers. This key is additionally utilized as a part of confirming and building up the match shrewd key between a couple of nodes. Irregular contributions from both the taking an interest nodes are utilized to refresh the match astute key in the versatile WSN setup. The security investigation demonstrates that the proposed convention opposes known-key, pantomime, replay, worm and sink gap assaults. The proposed convention additionally gives forward mystery, key freshness, and shared key control.

S. U. Khan, and et.al in [7] presents a compelling common authentication and key foundation plot for heterogeneous sensor networks comprising of various portable sensor nodes and just a couple of all the more effective settled sensor nodes. In addition, OMNET++ recreations are utilized to give a complete execution assessment of the proposed conspire.

S. Web optimization and E. Bertino in [8] presents the formal security model of their CL-HSC plot. At that point, they give the security evidence of their CL-HSC conspire against both versatile picked figure content assault and existential fraud in the fitting security models for testament less mixture signcryption. Since their CL-HSC conspire does not rely upon the blending based task, it lessens the computational overhead. It is likewise received to use ECC (Elliptic Curve Cryptography). In this manner, they take the advantage of ECC keys characterized on an added substance bunch with a 160-piece length as secure as the RSA keys with 1024-piece length.

S. H. Website design enhancement, J. Won, and E. Bertino in [9] presents a novel CL-HSC conspire without blending tasks. With a specific end goal to assess its execution, they actualized our CL-HSC conspire and ordinary half and half encryption approaches. The exploratory outcomes demonstrate that our CL-HSC plot is effective and appropriate for secure interchanges in AMI networks.

Q. Huang, J. Cukier and et. al in [10] considers a productive verified key foundation conventions between a sensor and a security director in a self-arranging sensor organize. We propose a half breed verified key foundation plot, which abuses the distinction in abilities between security administrators and sensors, and put the cryptographic weight where the assets are less compelled. The distributed key distribution decreases the high cost open key activities at the sensor side and replaces them with proficient symmetric-key based tasks. In the meantime, the plan verifies the two characters based on open key authentications to stay away from the normal key administration issue in unadulterated symmetric-key based conventions and keep up a decent measure of versatility.

III. PROPOSED SYSTEM

The accompanying figure 1 indicates proposed system engineering i.e Efficient Secure Routing Data Collection Node (ESR-DCN) in unique wireless sensor arrange, in which first client produce a system by conveying the nodes and after that system make a cluster. The cluster creation is done based on the node position with the node which is accessible in clusters go is allotted as a Data Collection Node (DCN). System chooses the CH from each cluster based on vitality, separate from BS and number of neighbouring nodes, after this every node and BS creates the key. The special individual key of base station is dispersed to each node in organize.

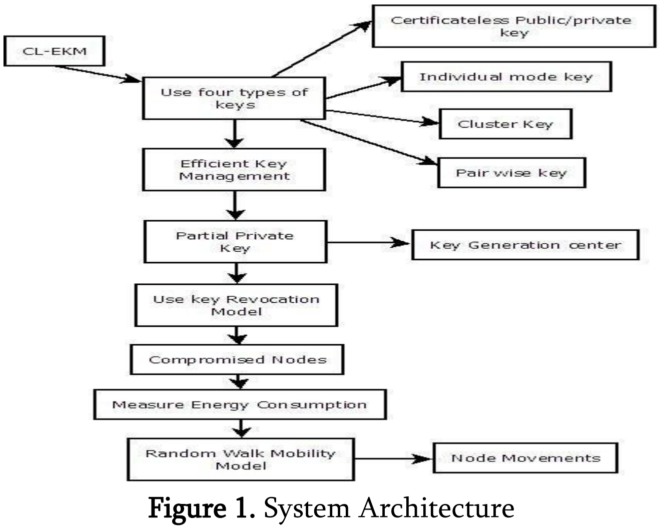

Figure 1. System Architecture

Base station has a key of every node. Additionally neighbouring nodes of every node in arrange shares different match insightful key of every node with its nearby nodes. Cluster key is created and imparted to every one of the nodes in each cluster for broadcasting reason. After that each cluster part sends the data to its CH and it totals all legitimate the data. DCN gathers information from CH and advances towards base BS. For the situation if any cluster part leaves/joins the cluster, CH will refresh the cluster key. Such node, which is leaves/joins, is alluded as an aggressor node. The new node creates open/private key and imparted it to BS, CH and neighbouring nodes. System at that point actualize forward in reverse key mystery process where in if source node forward information to the goal node and around then the nodes which happens on the way don't put away the information. The information is eradicated at in reverse node. Because of which information stay secure.

IV. IMPLEMENTATION DETAILS

A. Prerequisite System Generated Parameters

At the time of system deployment eight major parameters list < C/F_s, s, G, Z_k, k, A, B>, Q_k is kept private are established those are:

- C/F_s: Elliptical Curve function on field F_s $y^2 = x^3 + ax + b \bmod s$.
- s: It is an *m* bit prime number .
- G: Elliptical curve point generator.
- Q_k: Master Private Key of multiple PKGC.
- Z_k: Public key of multiple PKGC, generated as $Z_k = Q_k G$.
- k: Multiple PKGC .
- A: List of all existing nodes registered excluding RCH, where a_i nodes within a cluster c_j.; i = 0,1… A, j = 0, 1… C. Let C be the total number of clusters in the network.
- B: List of registered RCH.

B. Clustering and Cluster Head Selection

In this clustering based system the 'a_i' nodes within the same geographical location shares same cluster c_i and a unique attribute Att_t. Amongst the cluster members cluster head CH_i is selected which aggregates and encrypt the data with unique cluster attribute Att_t and forward it to the base station through nearest RCH with unique identity number as ID_r. Therefore, to balance the network lifetime we are selecting a CH in each round based on following three factors:

1. Maximum Residual Energy

To expand the lifetime of the system as well as to transmit data to base station uninterrupted and to balance the load of energy dissipation we must select the CH having the maximum residual energy among the cluster members. While transferring and receiving the data, nodes utilize some amount of energy based on the data length and the distance between two nodes.

Energy consumption of radio dissipation of sending data and receiving data are both expressed as E_m; the free space (a^2 power loss) and the multi-path fading (a^4 power loss) channel models with amplifying index $\in_{fs}$ and $\in_{amp}$ are used respectively; the energy consumption of data fusion is denoted by EDA.

The energy spent of a node that transmits single bits packet over distance ‘a’ is:

$$E_{Trans}(l,a) = E_{Trans-elec}(l) + E_{Trans-amp}(l,a) = \begin{cases} E_m * l + \in_{fs} a^2 * l & a < a_0 \\ E_m * l + \in_{fs} + \in_{amp} a^4 * l & a \geq a_0 \end{cases} \quad (1)$$

Where, $a_0 = \sqrt{\frac{\in_{fs}}{\in_{amp}}}$, and the energy consumption of receiving this message is:

$$E_{Rec}(l) = E_m * l \qquad (2)$$

2. Minimum distance of node to base station

To reduce the energy consumption the distance between the CH and BS should be as minimum as possible. We are introducing BS at the second level which increases one hop at the cost of increasing reach-ability to BS.

$$Distance\ between\ node\ and\ BS = \sqrt{\sum_{i=1}^{n}(X_i - Y_i)^2}$$

Where X_i, Y_i are the coordinates on x and y-axis for each node to BS

3. Maximum number of nodes in the transmission range of that node

The number of nearest nodes to the cluster head must be as possible as it can so the cluster head can collect the data from the all the members of the cluster.

In the case if the cluster head is compromised all the cluster members transmit data to the relay cluster head (RCH).

C. Key generation and Distribution

Next step of node registration is to generate pair of public / private key- Global key, and then generation of individual-BS key and lastly cluster-member key, each of which is generated with the help of PKGC as follows:

- Public/Private-Global Key – This key is global and generally used to encrypt data while communication .At the time of initialization of network ,each member node a_i choose a random secret number ‘h’ ,where h is an integer then compute P_i = h G. Then PKGC generates the partial key pair of a_i with input parameters i, and P_i. Then again a random secret number ’k’ is selected for further computation which is as bellow:

  P_{ppub} = k G

  P_{ppri} = k + Q_k . L_0(i, P_{ppub},P_i) mod s ,

  FP_{pub} = (P_i,P_{ppub})

Where L_0 is cryptographic hash function

Next < P_{ppub} , P_{ppri} , FP_{pub} > is send to node where it generate full private key as FP_{priv} =(h,P_{ppri}).

Individual Key-BS – This key pair is used to communicate individually to BS and RCH <IB_{pub},IB_{priv}>are generated in a similar way as above except that the PKGC also takes Att_t attribute of the individual node as input in L_0.
Cluster-Member Key – This key is used within cluster member communication and generated after cluster formation. This key is also generated as similar to Public/Private –Global key pair <CM_{pri},CP_{pub}>

V. CONCLUSION

This paper propose the principal Certificateless effective key administration convention (CL-EKM) for secure correspondence in unique WSNs. CL-EKM underpins proficient correspondence for key updates and administration when a node leaves or joins a cluster and consequently guarantees forward and in reverse key mystery. Our plan is strong against node trade off, cloning and pantomime assaults and secures the information secrecy and uprightness. The trial comes about exhibit the effectiveness of CL-EKM in asset compelled WSNs. Additionally this system actualize Data accumulation node for correspondence inside cluster head and base station. The DCN is valuable when the cluster head is bargained node and information sending without separation.

VI. REFERENCES

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

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

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

[4] 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.

[5] 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 clusterbased wireless sensor networks,” in Proc. IEEE WCNC, Mar. 2007, pp. 4145–4150.

[6] S. Agrawal, R. Roman, M. L. Das, A. Mathuria, and J. Lopez, “A novel key update protocol in mobile sensor networks,” in Proc. 8th Int. Conf. ICISS, vol. 7671. 2012, pp. 194–207.

[7] S. Seo and E. Bertino, “Elliptic curve cryptography based certificateless hybrid signcryption scheme without pairing,” CERIAS, West Lafayette, IN, USA, Tech.

[8] S. U. Khan, C. Pastrone, L. Lavagno, and M. A. Spirito, “An energy and memory-efficient key management scheme for mobile heterogeneous sensor networks,” in Proc. 6th Int. Conf. CRiSIS, Sep. 2011, pp. 1–8.

[9] S. H. Seo, J. Won, and E. Bertino, “POSTER: A pairing-free certificateless hybrid sign-cryption scheme for advanced metering infrastructures,” in Proc. 4th ACM CODASPY, 2014, pp. 143–146.

[10] Q. Huang, J. Cukier, H. Kobayashi, B. Liu, and J. Zhang, “Fast authenticated key establishment protocols for self-organizing sensor networks,” in Proc. 2nd ACM Int. Conf. WSNA, 2003, pp. 141–150.

[11] M. Rahman and K. El-Khatib, “Private key agreement and secure communication for heterogeneous sensor networks,” J. Parallel

Distrib. Comput., vol. 70, no. 8, pp. 858–870, 2010.

[12] D. S. Sanchez and H. Baldus, “A deterministic pairwise key predistribution scheme for mobile sensor networks,” in Proc. 1st Int. Conf. SecureComm, Sep. 2005, pp. 277–288.

[13] X. Zhang, J. He, and Q. Wei, “EDDK: Energy-efficient distributed deterministic key management for wireless sensor networks,” EURASIP J. Wireless Commun. Netw., vol. 2011, pp. 1–11, Jan. 2011.

[14] N. Gura, A. Patel, A. Wander, H. Eberle, and S. C. Shantz, “Comparing elliptic curve cryptography and RSA on 8-bit CPUs,” in Proc. 6th Int. Workshop Cryptograph. Hardw. Embedded Syst., 2004, pp. 119–132.

[15] S. S. Al-Riyami and K. G. Paterson, “Certificateless public key cryptography,” in Proc. 9th Int. Conf. ASIACRYPT, vol. 2894. 2013, pp. 452–473.

[16] Rep. CERIAS TR 2013-10, 2013. [Online]. Available: https://www.cerias.purdue.edu/apps/reports_and_papers/.Seung-Hyun

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

[18] P. Szczechowiak, L. B. Oliveira, M. Scott, M. Collier, and R. Dahab, “NanoECC: Testing the limits of elliptic curve cryptography in sensor networks,” in Proc. 5th Eur. Conf. WSN, vol. 4913. 2008, pp. 305–320.

[19] K. Chatterjee, A. De, and D. Gupta, “An improved ID-based key management scheme in wireless sensor network,” in Proc. 3rd Int. Conf. ICSI, vol. 7332. 2012, pp. 351–359.

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

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

[22] P. Jiang, “A new method for node fault detection in wireless sensor networks,” Sensors, vol. 9, no. 2, pp. 1282–1294, 2009.

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

[24] (2013). All About Battery. [Online]. Available: http://www.allaboutbatteries.com/Energy-tables. html, accessed Dec. 2014.

[25] A. Liu and P. Ning, “TinyECC: A configurable library for elliptic curve cryptography in wireless sensor networks,” in Proc. Int. Conf. IPSN, Apr. 2008, pp. 245–256.