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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

Energy Efficient and Secure Algorithm to Improve QOS of Wireless Sensor Network

Dhatri Kallur[1], Vidya.R.Pai[2]

Student, Dept. of CSE, BMSIT &M, Karnataka, India

Asst. Professor, Dept. of CSE, BMSIT&M, Karnataka, India

ABSTRACT: Wireless sensor networks (WSNs) cover for a wide group of exploitations, comprising soldierly perceiving and ensuing, empatheticprestigewitnessing, bustlerivulettesting, where tactile gadgets regularly move between various ranges. Obtaining statistics and correspondences requires reasonable encryption key conventions. A certificateless-effective key management (CL-EKM) convention for sheltered memos in element WSNs described by hub versatility. The CL-EKM bolsters effective key redesigns when a hub leaves or joins a bunch and guarantees forward and in reverse key mystery.

KEYWORDS: Wireless sensor networks, Certificateless- Effective Key Management (CL-EKM).

I. INTRODUCTION

Wireless sensor networks (WSN), are spatially seized self-decision sensors to curtain carnal or expected disorders for e.g., temperature, sound, weight, and so on and to agreeably go their statistics concluded the organism to a chief capacity.

Auxiliary radical structures are bi-directional, moreover empowering resistor of sensor feat. Enlargement of remote sensor structures was spurred by military solicitations for e.g. , front line surveillance; currently such classifications are utilized as a part of numerous modern and customer solicitations for e.g., perfunctorytechniquescrutiny and governor, machine wellbeing witnessing, etc.

In this anticipate, we proposition a certificateless successful key supervision secure convention (CL-EKM) for protected interchanges in WSNs. CL-EKM bolsters productive correspondence for key upgrades and supervision when a hub joins or leaves the bunch and subsequently in reverse and forward mystery. We furthermore utilize parallel memos for to decrease the parcel drop.

WSN focuses on statistics which bring together as well as spotlights on evidence confidence. WSN is utilized for substantial far off correspondence preparatory with one point then onto the next. Since WSN contains parcel of sensor hubs and one among these goes about as a head for the group shaped all in all.

To make unfilled secure communiqué in dynamic WSNs, we propose a CL-EKM protocol which provisions efficient communiqué for key updates and controlling when a node leaves or joins a cluster and hence ensures forward and backward key secrecy. Our scheme is resilient against node compromise, cloning and impersonation attacks and look after the data confidentiality and integrity.

II. LITERATURE REVIEW

a. **An efficient key management scheme for wireless sensor networks:** A novel key supervision plan called MAKM (measured number-crunching based key administration). The MAKM plan rest on the coinciding property of measured number juggling. Every part sensor hub just essentials to store a key seed. Key seed is consumed to register a one of a kind imparted key to its bunch head and a jamboree key instructed to different hubs in the equivalent group. MAKM minimizes the key storage room. Moreover, sensor hubs in the system can redesign their key seeds rapidly. In this technique every hub must trade the testament to set up the pairwise key and confirm

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

every one's declaration prior to utilize, the communication and calculation overhead increment significantly furthermore the base station familiarities the overhead of the endorsement supervision.

b. A novel key update protocol in mobile sensor networks: The portable remote sensor system (MWSN) is another fashion WSN among versatile sinks or sensors in the structure. The outline of a lightweight portable is a confirmation convention for versatile hub. The unruffled treaty gives forward protected pairwise key to the portable hub as it moves starting with one bunch then onto the next. The portable sensor hub can be validated by the new group head, and the security of his cause territory is ensured. It is not meant for sensors through constrained assets and can't achieve precious calculations with expansive key sizes.

c.A pairwise key predistribution scheme for wireless sensor networks: Safekeeping in remote sensor structures is imperative to have the capacity to encode and validate memos sent between sensor hubs. Because of asset rations, be that as it may, undertaking key indulgent in remote sensor structures is nontrivial. Numerous key indulgent plans utilized as a part of wide-ranging structures, for e.g, Diffie-Hellman and other release key based policy, are not reasonable for remote sensor structures because of the constrained computational capacities of the sensor hubs. Predistribution of mystery keys for all sets of hubs is not feasible because of the extensive measure of memory this necessitates when the structure size is substantial. It is not versatile against bargains and not able to bolster hub portability.

1. Existing System

The existing structure resides of two schemes and they are as follows:

- Symmetric key encryption.
- Asymmetric key based approaches have been proposed for dynamic WSNs.

Topsy-turvy key based practices found the safekeeping shortcomings of surviving ECC-based plans that these policies are defenceless against missive imitation, key bargain and known-key assaults. Furthermore, the uncomplicated safekeeping defects of the static undisclosed key are unfilled to the next when both hubs set up the gathering key. Besides, these ECC-based diplomacies with endorsements when straightforwardly connected to dynamic WSNs, experience the ill effects of the authentication supervision overhead of the whole sensor hubs as are not a handy solicitation for huge scale WSNs. The matching manoeuvre based ID-PKC plans are wasteful because of the computational overhead to pair manoeuvres.

The disadvantages of the existing system are as follows:

- Sensor devices are defenceless to malicious attacks such as impersonation, interception, capture or physical destruction, due to their unattended operational environments and lapses of connectivity in wireless communication.
- Protection is one of the most important issues in many critical dynamic WSN solicitations.

2. Proposed System

The proposed framework will upgrade your model which was slacking in some issues and which had its own particular disservices. It will receive the forefront innovation and fundamentally ponder on the issues expressed in remaining framework.

A certificateless compelling key supervision (CL-EKM) plan for element WSNs utilizes certificateless release key cryptography (CL-PKC), the client's full private key is a mix of a unfinished private key formed by a key era meeting point (KGC) and the consumers own particular mystery esteem. The extraordinary connotation of the full private/open key pair evacuates the prerequisite for testaments furthermore resolve the key escrow issue by expelling the obligation regarding the client's full private key.

Advantages of proposed system

- To maintain node mobility, the CL-EKM supports lightweight practises for cluster key updates executed when a node moves, detected as malicious or leaves the cluster everlastingly.

- CL-EKM is scalable in case of add-ons of new nodes after set of connections deployment. CL-EKM is lock against node compromise, cloning and impersonation, and ensures familiar and towards the back secrecy. The security analysis of our scheme shows its effectiveness.

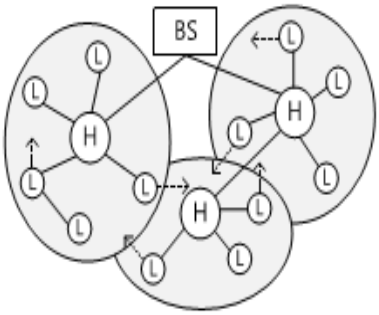
ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

III. SYSTEM ARCHITECTURE



Manner has three major components. They are:

- Senor nodes
- Cluster head
- Base station

Sensor nodes are mobile nodes which move and are not stationary. They are connected in wireless manner. They converse with the help of cluster head which is also a node one among them. They sense data like heat, temperature, fire, rain, humidity, waves, earthquakes, oceans, water level etc., and hence the name. They are deployed in solicitations wanting high mobility and sensing activities. They sense the data and send it base station via cluster head.

Cluster head is also a sensor node like other sensor node. The metamorphosis is, it has high energy equalled to its fellow nodes in the cluster and hence the name. It acts as a bridge and gateway between sensor nodes and base station. Assortment of cluster head implicates a policy and the node having high energy will be in the array to become next cluster head. It takes data from all sensor nodes of that cluster and aggregates it and sends it to base station. It virtually involves RCDA (Reconciliation and data aggregation) technique.

Base station is head of wireless sensor networks. Base station accepts the amassed data from cluster heads. There will be many clusters and each cluster will have its own head. After the data is acknowledged the base station computes the results and carries out the necessary operation.

IV. CONCLUSION AND FUTURE WORK

A. Conclusion

The certificate less effective key supervision affords a protected communiqué in live wireless sensor networks. It chains resourceful communiqué for key update and overseeing when node leaves or joins a cluster. It is flexible in opposition to node concession, cloning and masquerade attacks and protects the records secrecy and truthfulness.

B. Future Work

Surviving structure is vulnerable to adversary attacks as certificate less communiqué takes place. A node which is unknown can enter a cluster and be a part of it and can destroy the entire WSN. So data integrity and confidentiality are the driving paradigm that needs to be cared about. So future enhancements would include algorithms for secure communiqué keeping the paradigms in mind.

REFERENCES

[1] Seung-Hyun Seo, Member, IEEE , Jongho Won, Student Member, IEEE , Salmin Sultana, Member, IEEE , and Elisa Bertino, Fellow, IEEE , "Effective Key Management in Dynamic Wireless Sensor Networks" , IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 10, NO. 2, FEBRUARY 2015.

[2] D. Du, H. Xiong, and H. Wang, "An efficient key management scheme for wireless sensor networks," Int. J. Distrib. Sensor Network, vol. 15, Sep. 2014, Art. ID 406254.

[3] 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.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

[4] X. Zhang, J. He, and Q.Wei, "EDDK: Energy-efficient distributed deterministic key management for wireless sensor networks," EURASIP J. Wireless Commun. Network, vol. 2011, pp.1-11, Jan.2011.
[5] 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.
[6] 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.
[7] 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.
[8] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," in Proc. IEEE Symp. SP, May 2003, pp. 197–213.
[9] 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
[10] 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.
[11] 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.
[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] I.-H. Chuang, W.-T. Su, C.-Y. Wu, J.-P. Hsu, and Y.-H. Kuo, "Twolayered dynamic key management in mobile and long-lived clusterbased wireless sensor networks," in Proc. IEEE WCNC, Mar. 2007, pp. 4145–4150.
[14] 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.
[15] 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.
[16] P. Jiang, "A new method for node fault detection in wireless sensor networks," Sensors, vol. 9, no. 2, pp. 1282–1294, 2009.