ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 2, pp: (734-738), Month: April - June 2015, Available at: www.researchpublish.com

Secure Data Transmission by Using IBS and IBOOS Protocols

GEETHANJALI .S.G[1], Dr. B. R. PRASAD BABU[2]

[1]M.Tech Student, [2]Prof & Head (PG) [1,2]Department of CSE SEACET, BANGALORE – 560049, INDIA

Abstract: **secure data transmission difficult matter for wireless sensor network. Clustering is a practical method to improve the system performance. Cluster can be formed dynamically. we propose two protocol for cluster based wireless sensor network, called IBS and IBOOS and these protocol using two scheme called Identity Based digital signature schema and identity based online-offline signature scheme, respectively. We can provide security for various attacks. The results show that these two protocol give better performance than the existing protocol.**

Keywords: **Cluster based WSNs, ID based digital signature, ID based online-offline digital signature, CH, CH selection base station.**

I. INTRODUCTION

WSN consists of different distributed gadgets using sensor nodules to monitor physical state such as sound and temperature. Each and every nodes sensing their environments and processing the data and send these data into base station. Secure data transmission is demanded for many such practical wireless sensor network.

II. RELATED WORK

Cluster based data transmission in WSNs can be used to achieve the network scalability. In a cluster based technique consists of leader sensor node called cluster head. Cluster head collects the data from leaf node and send these data to the base station. It can be used to prevent LEACH problem.

A. Cluster head capabilities:

Mobility: CH can be stationary or mobile. But movements are limited within the region for better network performance. *Node types*: Deployed sensor nodes equipped with more computation and communication resources are selected as CHs. *Role*: CHs relay the traffic, fuse or aggregate the sense data.

B. Selection criteria for CH:

Initial energy**:** When any algorithm starts it considers the initial energy of the CH and the initial energy must be high. ***Residual energy:*** After few rounds of selection, the CH election should be based on remaining energy of the node. ***Energy consumption rate*****:** This rate is defined as VI (t) = [Initial– Ei (t)] / r Where Initial is the initial energy, Ei (t) is the residual energy and r is the current round of CH selection. ***Average energy of the network:*** It is the reference energy (ideal energy) of each node in current round to keep the network alive.

III. SYSTEM DESCRIPTION AND PROTOCOL OBJECTIVES

This section shows the network architecture and protocol objectives.

3.1 network architecture:

In cluster based WSN consists of base station and number of sensor nodes which are same functionalities. We have you provide security for WSN from attaks.in a cluster based wireless sensor network sensor nodes are grouped into cluster.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 2, pp: (734-738), Month: April - June 2015, Available at: www.researchpublish.com

Cluster head can be selected based on threshold .all other node can be joined the cluster head based on receipt indicator power and spread the detected information to BS. In CWSN data processing and data communication consume some energy of sensor nodule. The cost of information transmission is more expensive than data processing.CH can collect the data and it send into base station. A sensor node cannot perform any sense and the data transmission that time it can be switched into sleep mode and it's depend on time-division multiple access control can be used for data transmission, the both protocol used above technique.

3.2 protocol objectives:

WSN can be including the cluster based protocol. LEACH Like protocol most robust against insider attack than other types of protocol and it can be reduces some risk against some attack. Both the protocol can provide the secure data transmission for CH to sensor node and also CH to base station compare to existing protocol.

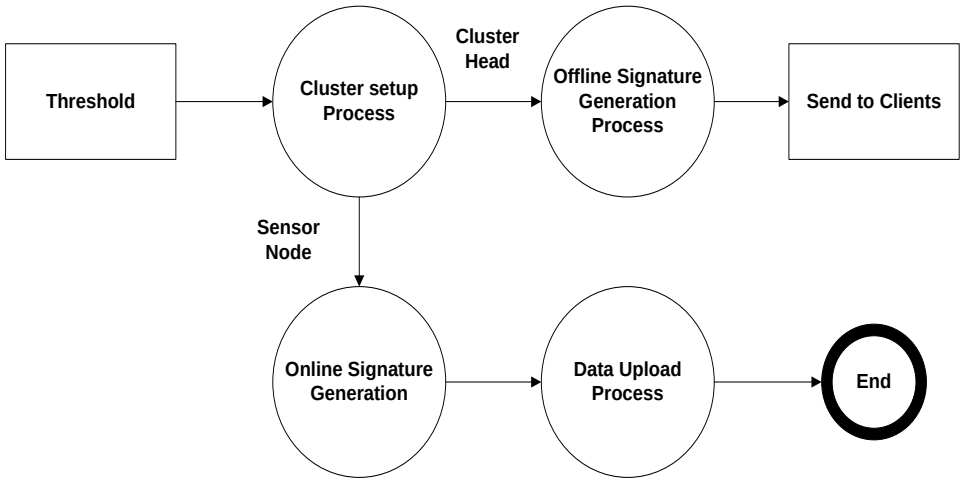

Fig: Data flow diagram

3.3 IBS AND IBOOS Scheme for cluster WSNs:

The IBS scheme consists of four operation, that is, setup, extraction, signature and signing, verification .setup can be done at the base station and base station can generate pair of public key and private key and it send into all sensor node. In the extraction sensor node generate the private key and signature signing in which sending device can generate signature. In the verification operation can accept the output if signature is valid otherwise is rejected.

The IBOOS scheme also consists of four operation, setup, extraction, offline signing, verification and online signing. Setup and extraction same as IBS scheme. In the offline signing the cluster head can generate the offline signature using public parameters and timestamp and sending these signatures into BS. In online signature generate the online signature using message, secret key and offline signature. In verification operation both online and offline signature are equal the output can be accepted otherwise it can be rejected.

3.4 THE PROPOSED IBS AND IBOOS PROTOCOL:

Both the protocol having same procedure for protocol initialization and key management.

1) Protocol initialization: In way to decrees the calculation and loading charge of signature signing handling in the IBS pattern, we advance IBS protocol by introducing IBOOS scheme for security in IBOOS protocol. The operation of the protocol initialization in IBOOS is similar to IBS. The base station can make lower process.

Make an encryption key k for the holomorphic encryption structure to encode documents messages.

Let G be a multiplicative finite cyclic group per order q. The PKG chooses a random producer g for group G generation, and chooses x ¡ô Z. q at random as the master secret key.

Arbitrarily select r ¡ô Z. q for each nodule secret key group, and let H be a hash function.

Preload each sensor nodule with the public parameters, given by param2= (k, m, G, q, g, x, r, H).

2) Key management for security: Assume that a sensor node *j* transmit a message *M*, and we denote the cipher-text of the encrypted message as *C*, which is encrypted by the same encryption scheme in both IBS and IBOOS.

The equivalent reserved pairing factors are preloaded in the sensor nodules for the duration of the protocol initialization. The IBOOS scheme in the future IBOOS consists of following four operations, extraction, offline signing, online signing and verification.

Extraction: Earlier the signature procedure, it first extracts secret keys from the master secret key *x* and its identity *ID*, as *sek* =(*R*, *si*), where

$R = g^r$,

$S_i = r + H(R, ID_i)$ x modq.

Offline signing: It generates the offline signature σ_i with the time-stamp of its time slot for transmission, and store the knowledge for signing online signature when it directs the communication. Notice that, this offline signature can be done by the sensor node itself or by the trustful third party, e.g., the BS or the CH sensor node. Let X = gx, then,

$g^{si} = g^r g^{H(R, IDi)x \ modq} = RX^{H(R, IDi)modq}$.

$\sigma_i = g^{-ti}$

Online signing: At this stage, node *Ai* computes the online signature $\_\sigma_i, z_i\_$ based on the encrypted data *C* and the offline signature σ_i.

$h_i = H (C\backslash\backslash\sigma_i)$.

$Z_i = \sigma_i + h_i s_i$ modq,

$\sigma_i = g^{\sigma i}$.

Then node Ai sends the encrypted message to its destination with the signature ID, C.

Verification: Upon accepting the message, each sensor nodule validates the validity in the ensuing method. It checks the current time-stamp for freshness. Then, if the time-stamp is right, the sensor nodule additional calculates the value of R^{hi} $X^{hiH(R, IDi) \ modq}$ using the online signature then check if

$g^{zi} = \sigma_i R^{hi} X^{hiH(R, IDi)modq}$.

If it is equal to the equation above in the accepted message, the sensor node considers the received communication accurate, receives it, and broadcasts the communication to the next hop or operator. If the confirmation overhead miscarries, the sensor nodule reflects the message as either false or a substituted one, even a wrong one, at that point discards or disregards it.

3.5 PROTOCOL OPERATION:

Once the protocol initialization complete IBS can be operate in round during conversation. Every round consists of two phase that is setup phase and steady-state phase. In which base station can allocate the time slots to every nodes. Each and every sensor node having start time and ending time for each round. In first step base station can send the it's ID and timeslots and in the second step can select the cluster head. The cluster head can be selected based on threshold and it's compared with numbers from 0 to 1. The proposed IBOOS operates similarly to that of IBS. IBOOS works in rounds during communication, and the self-voted cluster head are fixed established on their native conclusions, therefore it purposes without documents broadcast in the CH turnings. For the IBOOS key management in IBOOS, the offline signatures are generated by the CHs, which are used for the online signing at the leaf sensor nodes.

IV. PROPOSED SYSTEM

In this paper we propose two secure protocols for CWSNs, called IBS and IBOOS, by expending the IBS scheme and the IBOOS scheme, correspondingly. The in cooperation protocol validate the converted sensed documents, by put on digital signatures to message .The initially BS can distribute keys to all sensor node. The IBOOS can reduce computation overhead. Both IBS and IBOOS solve the orphan node problem in data broadcast by means of a symmetric key administration. We extends the above to add secure node mobility for allowing nodes to move from one cluster to another

by obtaining the secure token to the existing cluster and the new cluster head receives the token and validates the joining node, this allows mobility of nodes between cluster and prevents unauthenticated node to enter network. To achieve this we will use the hash based token generation approach.

V. IMPLEMENTATION

In cluster based wireless sensor network multi-hop information transmission it can be used for the transmission between the cluster head and to the Base Station, where the straight conversation is not possible due to the distance between them. The proposed IBS and IBOOS protocols for cluster based wireless sensor network can be improved using multi-hop routing algorithms, to form secure data transmission protocols for hierarchical clusters. The solutions to this extension could be achieved by applying the following two routing models.

1) The multi-hop planar model: A CH nodule spreads documents to the BS by progressing its data toward its foreigner nodules, in turn the documents is sent to the BS. We have anticipated a liveliness efficient routing algorithm for hierarchically clustered WSNs and it is suitable for the proposed secure documents transmission protocols.

2) The cluster-based hierarchical method: The network is fragmented into clustered layers, and the documents bundles travel from a lower cluster head to a higher one, in turn to the BS.

VI. CONCLUSION

In this paper, we reviewed the security for cluster based wireless sensor network in secure data transmission. Clustering is a good technique to reduce energy consumption and to provide stability in wireless sensor network. IBS & IBOOS are efficient in communication and put on the ID established cryptosystem. Which achieves security requirement is CWSNs. The result show that the proposed IBS and the IBOOS protocols have better performance than existing secure protocols.

ACKNOWLEDGEMENT

Geethanjali S G, BE, (MTech) student of Master of Technology in South East Asian College of Engineering, I did my Bachelor of Engineering Degree from the GEC, K. R. Pet. This is the First Work Carried Out by me under the Guidance of Prof. Dr. Prasad Babu.

Dr. B. R. Prasad Babu ME, PhD, MIE, MISTE is the Professor and Head Of the Department Of CSE (PG) and R&D in SEA College Of Engineering and Technology. He has a teaching experience of more than 30 years and over 5 years of experience in R&D. He has specialized in the area of Mobile Ad HOC Networks. He has been awarded with several awards including the certificate awarded by IISC Bangalore. He has published more than 30 papers in national and international publications.

REFERENCES

[1] T. Hara, V.I. Zadorozhny, and E. Buchmann, Wireless Sensor Network Technologies for the Information Explosion Era, Studies in Computational Intelligence, vol. 278. Springer-Verlag, 2010.

[2] Y. Wang, G. Attebury, and B. Ramamurthy, "A Survey of Security Issues in Wireless Sensor Networks," IEEE Comm. Surveys & Tutorials, vol. 8, no. 2, pp. 2-23, Second Quarter 2006.

[3] A.A. Abbasi and M. Younis, "A Survey on Clustering Algorithms for Wireless Sensor Networks," Computer Comm., vol. 30, nos. 14/15, pp. 2826-2841, 2007.

[4] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "An Application-Specific Protocol Architecture for Wireless Microsen-sor Networks," IEEE Trans. Wireless Comm., vol. 1, no. 4, pp. 660-670, Oct. 2002.

[5] A. Manjeshwar, Q.-A. Zeng, and D.P. Agrawal, "An Analytical Model for Information Retrieval in Wireless Sensor Networks Using Enhanced APTEEN Protocol," IEEE Trans. Parallel & Distributed Systems, vol. 13, no. 12, pp. 1290-1302, Dec. 2002.

[6] S. Yi et al., "PEACH: Power-Efficient and Adaptive Clustering Hierarchy Protocol for Wireless Sensor Networks," Computer Comm., vol. 30, nos. 14/15, pp. 2842-2852, 2007.

[7] K. Pradeepa, W. R .Anne, and. Duraisamy, "Design and Implementation Issues of Clustering in Wireless Sensor Net-works," Int'l J. Computer Applications, vol. 47, no. 11, pp. 23-28, 2012.

[8] L.B. Oliveira et al., "Sec LEACH-On the Security of Clustered Sensor Networks," Signal Processing, vol. 87, pp. 2882-2895, 2007.

[9] P. Banerjee, D. Jacobson, and S. Lahiri, "Security and Performance Analysis of a Secure Clustering Protocol for Sensor Networks," Proc. IEEE Sixth Int'l Symp. Network Computing and Applications (NCA), pp. 145-152, 2007.

[10] K. Zhang, C. Wang, and C. Wang, "A Secure Routing Protocol for Cluster-Based Wireless Sensor Networks Using Group Key Management,"Proc. Fourth Int'l Conf. Wireless Comm., Networking and Mobile Computing (WiCOM),pp. 1-5, 2008.

[11] S. Sharma and S.K. Jena, "A Survey on Secure Hierarchical Routing Protocols in Wireless Sensor Networks, "Proc. Int'l Conf. Comm., Computing & Security (ICCCS),pp. 146-151, 2011.

[12] Huang, JieLi, Mohsen GuizaniLu''secure and efficient data transmission for cluster based wireless sensor network.2014

[13] H. Lu, J. Li, and H. Kameda, "A Secure Routing Protocol for Cluster-Based Wireless Sensor Networks Using ID-Based Digital Signature,"Proc. IEEE GLOBECOM, pp. 1-5, 2010.

[14] J. Sun et al., "An Identity-Based Security System for User Privacy in Vehicular Ad Hoc Networks,"IEEE Trans. Parallel & Distributed Systems, vol. 21, no. 9, pp. 1227-1239, Sept. 2010.

[15] S. Even, O. Goldreich, and S. Micali, "On-Line/Off-Line Digital Signatures,"Proc. Advances in Cryptology (CRYPTO), pp. 263-275, 1990.

[16] S. Xu, Y. Mu, and W. Susilo, "Online/Offline Signatures and Multi signatures for AODV and DSR Routing Security,"Proc. 11th Australasian Conf. Information Security and Privacy, pp. 99-110, 2006.

[17] P. Barreto et al., "Efficient Algorithms for Pairing-Based Crypto-systems," Proc. 22nd Ann. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO),pp. 354-369, 2002.

[18] Y. Jia, L. Zhao, and B. Ma, "A Hierarchical Clustering-Based Routing Protocol for Wireless Sensor Networks Supporting

[19] Multiple Data Aggregation Qualities,"IEEE Trans. Parallel & Distributed Systems, vol. 4, nos. 1/2, pp. 79-91, 2008.