International Journal of Electronics, Communication & Soft Computing Science and Engineering
ISSN: 2277-9477, Volume 4, Issue 2

Study on Secure Multipath Routing in Wireless Sensor Network

Madhuri Zawar **Dipali Salunke**

Abstract- **Routing and security is very important and difficult for wireless sensor networks. WSN is divided in to cluster for providing better performance for wireless sensor network. In cluster-based WSNs, the clusters are formed dynamically and periodically to secure data. For security and routing purpose, there are several cluster routing protocols. Still, there is deficiency to provide better performance to WSN. To give better performance the secure multipath routing protocol has been proposed by using cryptography and learning automata.**

Keywords - **Cluster based wireless sensor network (CWSNs), Identity-based digital signature (IBS), Identity-based online/offline digital signature (IBOOS), Cryptography.**

I. INTRODUCTION

WSN are autonomous, modern networks are bidirectional, also self organizing systems consisting of a multitude of small, inexpensive, enabling control of sensor activity, battery-powered devices deployed densities in the deployment area. The WSN is group of "nodes" – from a few to several hundreds or even thousands, where each node is connected to one sensor. The individual nodes are sensing their environments, processing the information data locally, and sending data to one or more collection points in a WSN [1].

In CWSNs sensor nodes are deployed in large numbers and they are very affordable to each others. The goal of a sensor network is to collect data from all the nodes and send the aggregated data to the base-station in to WSN [2] and the solution to this problem is clustering. The clustering protocols are used to minimize inter node communication in the WSN. The cluster heads may be predesigned by the network designer or elected by the sensors in the network. In a CWSN, each cluster has a leader sensor node, regarded as CH. A CH aggregates the data collected by the leaf nodes (non-CH sensor nodes) in its cluster, and sends aggregation to the base station (BS) into the WSN. Usually a cluster head is a node which is very rich in energy resources [2].The cluster heads are selected using different methods and based on the parameters used for CH. Clustering approaches can be categorized as deterministic, adaptive, and random ones. In CH are stored the information of neighboring CH and inter cluster node information to WSN. In deterministic schemes, special inherent attributes of the sensor nodes are considered, such as the identifier (ID), number of neighbors they have. In adaptive manners, CHs are elected from the deployed sensor nodes with higher weights, which includes such as residual energy, communication cost.

II. DATA TRANSMISSION EXISTING PROTOCOLS

Today a Secure data transmission is a critical issue for wireless sensor networks (WSNs). The data transmission protocols are operates on the clustered wireless sensor networks (CWSNs). For providing the security, performance to the network various protocols are introduced.

A. *SET-IBS Protocol*

The SET-IBS protocol operates in rounds during communication, which consists of a setup phase and a steady-state phase in each round. The SET-IBS protocols set is implemented on the BS of WSNs [3]. In the set up the network is formed with the clusters and cluster heads are selected in this state. In steady state phase, the protocol generates private key for each node, signing of the nodes. After that the data is transmitted from nodes to CH and CH to BS with the verification of private key and master key that contains in message.

Advantages:

1. It provides more security for data while it transmits message from source to destination.
2. The orphan node problem is solved.

Disadvantages:

1. There is no proper routing mechanism. Sometimes may be packet loss.
2. The computational overhead is high.

B. *SET-IBOOS Protocol*

SET-IBOOS works in rounds during communication, and the self-elected CHs of the CWSNs are decided based on their local decisions, thus it functions without data transmission in the CH rotations. It works same as IBS [4]. For the IBOOS key management in SET-IBOOS, the offline signatures are generated by the CHs, which are used for the online signing at the leaf nodes.

Advantages:

1. The storage cost is less because of the private key is the id of that node.
2. The scalability of network is high. It means number of nodes can work in network.

Disadvantages:

1. The offline is not suitable in the CWSN. Because the offline signature is computed by third party.

2. The computational overhead is high.

C. LEACH

The low-energy adaptive clustering hierarchy (LEACH) protocol is present effective one to reduce and balance the total energy consumption for CWSNs [6]. To prevent quick energy consumption of the set of CHs, LEACH randomly rotates CHs among all sensor nodes in the CWSNs, in rounds. LEACH achieves improvements in terms of network lifetime and is updated the information according to the CWSN. There are some secure data transmission protocols based on LEACH- SecLEACH, GS-LEACH, and RLEACH.

Advantages:

1. A large-scalable network without traffic overload can be deployed and by this also better energy efficient network topology can be achieved as compared to the flat-topology.
2. Single -hop routing is possible from sensor node to cluster head, and this means it is able to save the energy of the network.

Disadvantages:

1. It significantly relies on cluster heads rather than cluster members of the cluster for communicating to the sink. Due to this it incurs robustness issues like failure of the cluster heads.
2. CHs are not uniformly distributed within the cluster that means CHs can be located at the edges of the cluster.

D. APTEEN

Threshold sensitive Energy Efficient sensor Network protocol (APTEEN) [10],[12], is an extension to TEEN and aims at both transmitting periodic data and reacting to time critical events. APTEEN, on the other hand, is a hybrid protocol that changes the periodicity or threshold values. APTEEN is based on a query system which allows three types of queries: historical, on-time, and persistent which can be used in a hybrid network.

Advantages:

1. APTEEN combines both proactive policies, which is alike that of LEACH, and reactive policies, which is alike that of TEEN. Accordingly it is suitable in both proactive and reactive applications.
2. It embodies a lot of flexibility by setting the count-time interval, and the threshold values for the energy consumption.

Disadvantages:

1. There exist additional complexity required to implement the threshold functions and the count time.
2. Actually, both TEEN and APTEEN share the same drawbacks of additional overhead and complexity of cluster construction in multiple levels, implementing threshold-based functions, and dealing with attribute-based naming of queries.

E. PEACH

The PEACH is Power Efficient and Adaptive Clustering Hierarchy protocol for wireless sensor networks. PEACH can be used for both location-unaware and location-aware CWSNs. Performance of PEACH is less affected by the distribution of sensor nodes compare to other clustering protocols. The PEACH minimizes energy consumption of the nodes [7].

Advantages:

1. All nodes in network communicate easily and share data to each others.
2. PEACH has no overhead on cluster head selection and forms adaptive multi-level clustering.

Disadvantages:

1. Maximum delay is produced for searching nodes in PEACH protocol.
2. Multilevel clustering support is not fixed.

III. METHODS

A. Digital Signature

In Digital signature scheme “sign” messages and verify the resulting signature with two different keys in such a way that it is difficult to sign without the signing key. Similar to public-key cryptosystems, the verification key can be published without compromising security, and is called the public key; the signing key is called the private key. Digital signature schemes provide integrity and origin authentication. Like public-key cryptosystems, they do not require that parties first agree on a secret key, and they are generally somewhat slower than, for instance, secret-key cryptosystems and cryptographic hash functions [5]. In so-called reversible cryptography, signing in a digital signature scheme is the same as decryption in a public- key cryptosystem, while verification is the same as encryption. In irreversible cryptography, the relationships do not hold, although a given public/private-key pair may work in both a digital signature scheme and a public-key cryptosystem [11].

B. RSA Algorithm

In Digital signature scheme “sign” messages and verify the resulting signature with two different keys in such a way that it is difficult to sign without the signing key. Similar to public-key cryptosystems, the verification key can be published without compromising security, and is called the public key; the signing key is called the private key for the cryptography use RSA algorithm [8],[9]. Digital signature schemes provide integrity and origin authentication using RSA algorithm. In so-called reversible cryptography, signing in a digital signature scheme is the same as decryption in a public- key cryptosystem, while verification is the same as encryption.

In CWSNs network continuous monitoring to secure and energy aware multipath routing. Hence, a public key and private key is generated in every node and secure and energy aware multipath routing provides security to the node. In RSA, public key and private keys generated at all the nodes are assigned in a key table and put in a node which is called as the base station [13]. The base station also contains the routing table, having the exact location of all the other nodes. Based on the routing table the base station assigns two other nodes that are nearer to the base station as cluster heads. Lastly two

other nodes are assigned as a source node and destination node randomly with respect to each and every application.

C. *Learning Automata*

Sensors are redundantly deployed, a subset of sensors should be selected to actively monitor the field (referred to as a "cover"), while the rest of the sensors should be put to sleep to conserve their batteries. Despite of its potential application, wireless sensor network encounters resource restrictions such as low computational power, reduced bandwidth and specially limited power resource. In this paper we propose learning automata based algorithm for energy-efficient monitoring in wireless sensor networks. Learning Automata are used for choosing the nodes having redundant coverage contribution. The method in comparison to existing methods uses many numbers of nodes for monitoring network area.

IV. FUTURE SCOPE

Security of CWSNs is very critical job for security to data transmission. To evaluate the energy consumption of the computational overhead for security in communication, proposed work considers three metrics for the performance evaluation: Network lifetime, system energy consumption, and the number of alive nodes. Secure and energy aware multipath routing Protocols will be implemented to provide better confidentiality protection from unauthorized persons using RSA algorithm and also explains different methods.

V. CONCLUSION

In this paper, different types of data transmission protocols are discussed. The LEACH like protocols is not suitable for the security. The SET IBS and SET IBOOS protocol provides the security but there is also problem in computational overhead and it takes more time. Hence, for giving the performance, security and reduction of energy consumption in WSN, the secure energy aware multipath routing protocols is introduced.

ACKNOWLEDGMENT

I would like to thank Mrs.Madhuri Zawar Professor of Computer Department for valuable time, guidance and suggestions during the hour of paper. I accord my sincerest gratitude and profound thankfulness, for his insistent guidance, insightful opinion and constructive comments. I would like to express my special gratitude and thanks also HOD of Computer Department Prof. Dipak R. Pardhi other staff members for giving me such attention and time.

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

[3] Huang Lu, Jie Li, Mohsen Guizani,"*Secure and EfficientData Transmission for Cluster-Based Wireless Sensor Networks*",IEEE Computer Security,vol. 25, no. 3,pp. 750-761,March 2014.

[4] Xuxun Liu "*A Survey on Clustering Routing Protocols in Wireless Sensor Networks",*Sensors,pp , 11113-11153, 2012.

[5] D.W. Carman, "New Directions in Sensor Network Key Management," Int'l J. Distributed Sensor Networks, vol. 1, pp. 3-15, 2005.

[6] 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.

[7] 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.

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

[9] Hongwei Si, Youlin Cai,, Zhimei Cheng," *An Improved RSA Signature Algorithm based on Complex Numeric Operation"*, IEEE Computer Security,pp.399-400,2010.

[10] Jalil Jabari Lotfa, Mehran Hosseinzadehb,seyed hossein hosseini nazhad ghazanic,Rasim M. Alguliev "*Applications of learning automata in wireless sensor networks"*, Elsevier,Procedia Technology 1,pp. 77 – 84,2012.

[11] Gerhard Potzelsberger, B.Eng."KV Web Security: Applications of Homomorphic Encryption" ,May 2013.

[12] Karlof, C., Sastry, N., Wagner, D. (2004) '*TinySec: A Link Layer Security Architecture for Wireless Sensor Networks*', Proceedings of the 2nd International Conference on Embedded Networked Sensor Systems, Baltimore, MD, USA, 03 – 05 November 2004, New York, NY, USA: ACM Press, 162 – 175.

[13] Perrig, A., Canetti, R., Tygar, J.D. and Song, D. (2002) '*The TESLA Broadcast Authentication Protocol*', CryptoBytes, 5(2),2-1.

AUTHOR'S PROFILE

Mrs. Madhuri R. Zawar received the B.E and M.E. Degrees in Computer Science and Engineering from Dr. Babasaheb Ambedkar Marathwada University, Maharashtra, India, in 1996 and 2011 respectively. Since 2007, she has been with the GF's Godavari College of Engineering, Jalgaon, NMU University, where she is currently an Assistant Professor of Computer Engineering. Her research interests include Wireless adhoc Networking. In these areas, she has presented a paper in iCOST 2011 International Conference, Dhule and presented a paper in absence at IEEE ICCSIT 2011 International Conference, China. She has a membership of ISTE.

Ms. Dipali A. Salunke received the B.E Degree in Computer Engineering from North Maharashtra University Jalgaon, Maharashtra, India, in 2010. Currently, she is studied in ME Computer Engineering in North Maharashtra University,Jalgaon. Since Aug. 2010, she has been with the G.H.Raisoni Polytechnic, Jalgaon, where she is currently Lecturer of Computer Engineering. Her research interests include Wireless Networking. In these areas, she has presented a paper in ICACSIT 2012 International Conference, Pune, Maharashtra.