Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 3, March 2015, pg.16 – 20

SURVEY ARTICLE

Survey on Secure & Efficient Data Transmission in Cluster Based Wireless Sensor Network

Anup Pawar[1], Divya K V[2]

[1]M. Tech (Software Engineering), New Horizon College of Engineering, Bangalore, India

[2]Asst. Professor, Department of Information Science & Engineering, New Horizon College of Engineering, Bangalore, India

[1] anupbdr@gmail.com, [2] divya.k.vasudevan@gmail.com

Abstract- Wireless Sensor Network is a collection of homogeneous/heterogeneous wireless devices used to monitor the changes in the surrounding of the wireless device. Each wireless device present in the network has the capability of sensing the changes in the surrounding environment. Homogeneous sensors are those which have same computational power, energy etc. Each node is battery powered which is used to transmit the sensed data over the network. So efficient transmission of data in Wireless Sensor Network is important and to transmit the data unaltered over the network to the receiver security is important. Clustering of Wireless Sensor Network is important to increase the network scalability. Cluster Based Wireless sensor Network (CWSN) are organised in hierarchical manner. In CWSN a leader node called Cluster Head (CH) is responsible for aggregation of data from the leaf nodes which are present in the Cluster. In this paper we will discuss how to transmit the data securely and efficiently over the network.

Keywords- Cluster based Wireless Sensor Network (CWSN), Low Energy Adaptive Clustering Hierarchy (LEACH), Identity Based digital Signature, Identity Based Online/Offline Signature, Digital Signature

I. INTRODUCTION

Cluster based Wireless Sensor Network (CWSN) has been researched in order to minimize the network consumption for transmitting data and increasing the wireless devices lifetime by maximizing the battery lifetime of the device. In CWSN the nodes are arranged in a cluster, based on algorithms which may or may not take into account energy depending on the algorithm. In CWSN each cluster has a node which is responsible for aggregation of data from the other nodes in cluster such a node is called Cluster Head (CH). CH collects the sensed data from the other nodes in the network and transmits it to one or more collection points which can be a Base Station (BS). CH's are selected using the same algorithms which are used for formation of clusters. Hierarchical Clustering is the efficient way to utilize the node energy. Low Energy Adaptive Clustering Hierarchy (LEACH) is an application specific hierarchical routing protocol. In LEACH each and every node in the cluster act as

a Cluster Head. In order to reduce the energy consumption of the nodes every cluster is selected as CH randomly from the cluster so as to stop the energy consumption of a CH. If only one node act as CH then the whole energy of the particular CH is consumed and the node is of no use for further collection of data which leads to ambiguity to the other nodes in the cluster and the communication within the cluster is terminated. The LEACH operation is divided in two rounds.

- **Setup State Phase:** Each round initiates with the setup state phase where the cluster are formed.
- **Steady State Phase**: In this phase all the leaf node of the cluster senses the data processes it locally and these data is collected by the CH which transmits it to the BS.

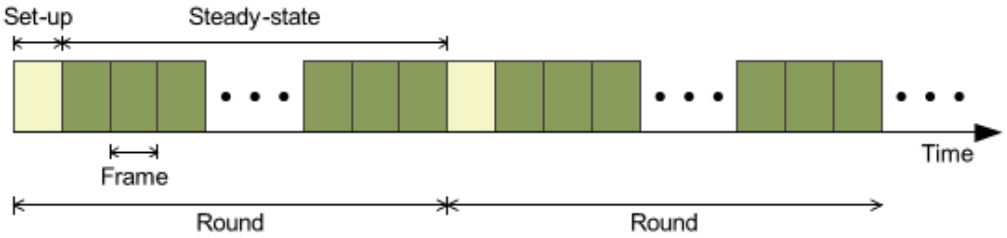

Fig. 1 The phases of a LEACH protocol in a round.

Few other protocols such as SRPSN, LHA-SP, SHEER, FLEACH are used for secure routing of data which use different mechanisms. These protocols use symmetric key cryptography for generating a group key. It is generated by taking the partial key of each node present in the cluster to generate a group key which is distributed among the nodes. The problem with this group key is if the CH changes then to generate a group key the private key of every node associated with the cluster have to be generated. When a CH consumes all energy it goes down and becomes unavailable so all the nodes associated to the particular CH suffer from a problem called orphan node problem as the leaf node does not share their pairwise key to join another cluster. So the node itself elects as a CH. As more CH is elected by itself the network transmission increases.

Symmetric key cryptography is replaced by Asymmetric key cryptography to increase the security. For asymmetric key cryptography Digital Signatures are employed for authentication which uses the binding between public key and the identification of signer using digital certificate. The two problems associated with authentication are authenticated broadcast by sensor nodes and the outside user identification. The solution to this problem is provided by using Identity Based digital Signature (IBS) scheme and Identity Based digital Online/Offline Signature (IBOOS). IBS allows computing the public key using the unique identity information such as from name, address, ID etc. IBS is used for broadcasting the message with every other node in the network without the help of BS. IBOOS scheme allows the valid user to access the data in a secure way. IBOOS partition the process of signing the message into two parts, offline phase and online phase. A partial signature is generated in the offline phase which is generated when the message to be signed is known and the complete signature is generated by making minor computations to the partial signature when the message is available online. It is assumed that online phase is faster than the offline phase. In this scheme the private key is generated by Private Key Generator (PKG) by using the signer's ID. To enhance the security two new Secure and Efficient Transmission (SET) schemes are used called SET-IBS and SET-IBOOS which are basically based on IBS and IBOOS scheme respectively. SET-IBS and SET-IBOOS use time stamps to add more security to IBS and IBOOS.

II. LITERATURE SURVEY

The below mentioned papers are survey includes the related to the Secure and Efficient Data Transmission in Cluster based Wireless Sensor Network.

- **"EEHC: Energy Efficient Heterogeneous Clustered scheme for wireless sensor networks[1]"**

(1) Dilip Kumar, Trilok C. Aseri, R.B. Patel described LEACH as a Low Energy Adaptive Clustering Hierarchy which is an application specific protocol used to reduce the energy consumption of the node in WSN. In CWSN the LEACH rotates the CH selection from one node to another node in the cluster so as to reduce the energy consumption of a single node in the cluster. LEACH is distributed into two parts, Setup phase and Steady State Phase. It uses symmetric key management for secure transmission of data which suffers from an orphan node problem which occurs when the CH of a particular cluster goes down due to total energy consumed for transmitting the data and using of symmetric keys does not provide required security level. Cluster formation and CH selection has also been discussed. It uses Symmetric key management. It leads to orphan node problem when the total energy of the CH is consumed. The orphan node problem occurs when the nodes in the cluster do not share their pairwise key with the other CH and elect themselves as the CH which leads to formation of more CH and the network congestion increases. When the CH changes the nodes associated with the cluster have to compute their public key again.

- **"An authentication framework for Wireless Sensor Networks using identity based signatures[2]"**

(2) by Rehana Yasmin, Eike Ritter and Guilin Wang discussed asymmetric key cryptography scheme Identity Based digital Signature. It uses Digital Signature for authentication of data. It uses unique ID of the signer to generate a public key. The main objective of this framework is to provide a authentication framework which solves the problem efficiently in terms of power consumption, storage overhead and processing time. It allows every node present in the network to broadcast the message with every other node in the network without considering the BS. The IBS scheme performs following four operations.

i. Setup: This operation is performed at the base station. Here the base station generates a master key and public parameter for Private Key Generator and these are distributes to all the nodes.
ii. Extraction: This operation is performed at each sensor node. In this operation a private key is generated by using the sensor ID and the master key generated at the base station.
iii. Signature Signing: This operation is performed at the sensor node The sending node generates a Signature with the help of message, time stamp and a signing key.
iv. Verification: This operation is performed at the receiver node. On receiving the message, ID and signature the receiving node accepts if the signature is valid or else the message is discarded.

- **"Practical ID-based Encryption for Wireless Sensor Network[3]"**

(3) by Cheng-Kang Chu, Joseph K. Liu, Jianying Zhou, Feng Bao and Robert H. Deng have discussed Identity Based Online/Offline Signature which is used to reduce the storage and computation cost of the signature. This scheme also makes use of asymmetric key cryptography. This scheme is divided into two parts, online scheme and offline scheme. In offline scheme

the signature is generated partially when the message is known, complete key is generated when the message becomes available online. Online scheme is considered to be faster than offline scheme. It is used for outside user authentication i.e.., it allows only valid user to access the data from sensor nodes. The following five operations involved in the IBOOS scheme.

i. Setup: This operation is performed at the base station. It generates master key and public parameter for the Private Key Generator and these are distributed to all the sensor nodes.
ii. Extraction: This operation is performed at the sensor node. It generates a private key using the master key and ID.
iii. Offline Signing: This operation is performed at the Cluster Head. By using public parameters and the time stamp an offline signature is generated and transmitted to every node present in the cluster.
iv. Online Signing: This operation is performed at the sensor node. An online signature is generated with the help of Offline Signature, Message and private key of the sensor.
v. Verification: By taking the ID, message and online signature. The receiver node accepts if the online signature is valid or else rejects.

- **"A Low-Energy Security Algorithm for Exchanging Information in Wireless Sensor Networks[4]"**

(4) by Mohammad AL-Rousan , A. Rjoub and Ahmad Baset have described about symmetric key cryptography which is used in LEACH protocol as it consumes low energy and simple hardware requirement, but usage of symmetric key cryptography leads to orphan node problem and most of them do not provide enough security. Usage of symmetric key leads to a problem when a cluster head of a cluster degrades all its energy in transferring data from cluster head to the base station. Entire energy consumption of cluster head leads to a problem known as orphan node problem. This problem occurs when a node doesn't share its pairwise key so as to reduce the storage cost. Further it increases the possibility of node not joining a cluster which leads to independent election of cluster as cluster head by themselves which further leads to more consumption of network energy and also increase in the transmission overhead.

- **"Identity based Digital Signature Scheme in Cluster Based Wireless Sensor Networks for Secure and Efficient Data Transmission – A Survey[5]"**

(5) by Mr. S. Muthusamy, Dr. C. Poongodi, Dr. D. Deepa have discussed about Secure and Efficient data Transmission (SET) IBS and SET-IBOOS. The two schemes are used to overcome the orphan node problem by using asymmetric keys. This scheme also overcomes the key escrow problem by the pre-distribution of pairing parameter and secret key in every node. As the pairing parameter and secret key are already distributed the private keys are generated without additional transmission of data which reduces the computational cost. The SET-IBS and SET-IBOOS are based on IBS and IBOOS scheme respectively. In this SET scheme two time stamps are used first time stamp is used to transmit the master key from BS to nodes and second time stamp is used to transmit the encrypted data from the nodes to the cluster head.

III. CONCLUSION

Wireless Sensor Networks are important for monitoring the changes in the environmental conditions so that preliminary cautions can be taken to deal with the problem. Moreover Cluster based Wireless Sensor Network are hierarchical networks where the data is aggregated by the CH from all the nodes present in the cluster which has to be sent to be sent to the BS. Hence secure and efficient transmission of data in CWSN is important.

REFERENCES

[1]. Dilip Kumar, Department of Product Design & Technology, Centre for Development of Advanced Computing (CDAC), A Scientific Society of the Ministry of Communication & Information Technology, A-34, Phase-8, Industrial Area, Mohali, India, Trilok C. Aseri, Department of Computer Science & Engineering, Punjab Engineering College (PEC), Deemed University, Sector-12, Chandigarh 160 012, India & R.B. Patel Department of Computer Science & Engineering, Maharishi Markandeshwar University (MMU), Mullana, Ambala 133 203, India, "*EEHC: Energy efficient heterogeneous clustered scheme for wireless sensor networks*", Computer Communications, 2009.

[2] Rehana Yasmin, University of Birmingham, Eike Ritter, University of Birmingham, Guilin Wang, University of Birmingham *"An authentication framework for Wireless Sensor Networks using identity-based signatures: Implementation and Evaluation*", IEICE, 2012.

[3] Cheng-Kang Chu, Singapore Management University, Joseph K. Liu, Institute for Infocomm Research, Jianying Zhou, Institute for Infocomm Research, Feng Bao, Institute for Infocomm Research, Robert H. Deng, Singapore Management University, "*Practical ID-based Encryption for Wireless Sensor Network*", ASIACSS, 2010.

[4] Mohammad AL-Rousan , A. Rjoub and Ahmad Baset, Jordan University of Science and technology, School of Computer and Information Technology, Irbid, Jordan "*A Low-Energy Security Algorithm for Exchanging Information in Wireless Sensor Networks*" Journal of Information Assurance and Security, 48-59, 2009.

[5] S. Muthusamy PG Scholar, Dr. C. Poongodi Associate Professor, Dr. D. Deepa Associate Professor, Information Technology, Bannari Amman Institute of Technology, Sathyamangalam, Tamilnadu, India "*Identity Based Digital Signature Scheme in Cluster Based Wireless Sensor Networks for Secure and Efficient data Transmission – A Survey*" IJAICT Volume 1, Issue 6, October 2014.

[6] Suchismita Chinara, Santanu Kumar Rath, "*A Survey on One-Hop Clustering Algorithms in MobileAd Hoc Networks*", Journal of Systems and Networks Management, 2009.

[7] Suraj Sharma and Sanjay Kumar Jena, Department of Computer Science and Engineering, National Institute of Technology, Rourkela, Odisha, India, " *A Survey on Secure Hierarchical Routing Protocols in Wireless Sensor Network*", ICCCS, 2011.

