IWNEST PUBLISHER

Journal of Industrial Engineering Research

(ISSN: 2077-4559)

Journal home page: http://www.iwnest.com/AACE/

Energy Efficiency and Security in Cluster Based Wireless Sensor Networks

J. Subash Chandra Bose, R. Roopa, G. Beulah, T. Saranya Devi, D. Sathya,

Department of CSE, Professional Group of Institutions Palladam, Tirupur, Tamilnadu, India

ARTICLE INFO

Article history:
Received 22 February 2015
Accepted 20 March 2015

Keywords:
Terms Used- Cluster Based WSNs, ID based digital signature, ID based online/offline digital signature

ABSTRACT

Wireless sensor networks are capable of sensing data efficiently. But, security and energy efficiency of data transmission in wireless nodes have critical issues. Clustering is an effective way for the system performance of WSNs. In this paper, we study energy efficient and secure data transmission for cluster based WSNs. We propose ID based digital signature security for transmitting the data between the cluster nodes where the clusters are formed dynamically and periodically. We make use of SET-IBS (Secure and Efficient data Transmission-Identity Based Digital Signature) and SET-IBOOS (Secure and Efficient data Transmission-Identity Based Online/Offline Digital Signature) protocols for the secure transmission of data between the nodes by asymmetric key management for encryption of data. In SET-IBS security relies on the hardness of Diffie-Hellman problem in the paring domain. SET-IBOOS further reduces the computational overhead for protocol security.

To Cite This Article: J. Subash Chandra Bose, R. Roopa, G. Beulah, T. Saranya Devi, D. Sathya, Energy Efficiency and Security in Cluster Based Wireless Sensor Networks. **J. Ind. Eng. Res.**, ***1(3),*** *1-4, 2015*

INTRODUCTION

Sensor nodes are cable of sensing their environmental conditions like sound, temperature and motion. Wireless sensor network is network system composed of spatially distributed sensor nodes by monitoring the environmental conditions. Efficient and secure data transmission is the most important issues of WSNs. WSNs of deployed in harsh neglected and adversarial physical environment for some applications like military domains. Efficient and secured data transmission is demanded for WSNs. There are many protocols have been invented for the wireless sensor nodes. Very few protocols have been invented for WSNs to obtain the security for data transmission.

Researchers go with achieving the network scalability and management for bandwidth consumption. In a cluster based WSN (CWSNs) cluster nodes have a leader called cluster head (CH) Which accumulates a data collected from the leaf nodes and sends it to base station (BS).Then BS sends the message to the destination node.

1.1 Background And Motivation:

Cluster-based WSNs has been measured to achieve the network scalability and execution, which maximizes node lifetime and reduce bandwidth consumption by using local combination among sensor nodes. In a cluster-based WSN, every cluster has a leader sensor node, named as clusterhead (CH). A CH compiles the data collected by the leaf nodes in the CWSNs, and it sends the data to the base station (BS). To anticipate the energy utilization of the set of CHs, LEACH however rotates CHs among the sensors nodes in the network circle.

Since the more CHs elected by themselves, the more total energy exhaust in the network, the orphan node problem increases the above transmission and system energy consumption by establish the number of CHs. The sensor node does share a key element with only a distant CH not a neighboring CH, it requires high energy to transmit data to the far CH.

2 Protocol Objectives:

In this section we present the network architecture and protocol objectives used in WSNs.

2.1 Network Architecture:

Cluster based WSNs subsist of a fixed BS and more number of WSNs, which are same in functionalities and capabilities. The base station (BS) is a trusted authority (TA) in this network system.

Corresponding Author: J. Subash Chandra Bose, Department of CSE, Professional Group of Institutions Palladam, Tirupur, Tamilnadu, India

Journal of Industrial Engineering Research, 1(3) March 2015, Pages: 1-4

The sensor nodes may be agreed with the attackers, and then the data transmission may be interrupted in the wireless channel. In cluster based WSNs, the sensor nodes are grouped together and form a cluster, and these clusters has a CH, which is elected enormously. The CHs perform data merging, and data transmission to the BS exactly with high energy.

2.2 Protocol Objectives:

The data transmission protocols for WSNs, including cluster-based protocols are accessible to a number of security attacks. Attacks to create a serious damage in the network of cluster based WSNs because the transmission is fully based on the CHs. But the particular forwarding attacks are disturbing the networks while transmitting the data. The proposed secure data transmission for CWSNs is secure and efficient data transmissions between leaf nodes and CHs, and also transmission between CHs and the BS.

3 ibs and iboos in cwsns:

This section shows the IBS and IBOOS protocol strategies used in CWSNs. We make the ordinary IBS scheme for cluster based WSNs by share the functions to different types of sensor nodes and also to IBOOS scheme.

3.1 Ibs Protocol Strategy:

SET-IBS is based on identity based signature scheme which has a protocol initialization prior to the network and acts in rounds. It consists of two phases called set-up phase and steady state phase in each round during communication.

For protocol initialization of SET-IBS time is subdivided into consecutive time intervals. The scheme adopts the asymmetric encryption scheme to encrypt the plaintext to ciphertext. This scheme allows aggregation of encrypted data between CHs and BS.

Security to the data that are transmitted between the cluster nodes is accomplished by the key management facility of encryption scheme. The generated signatures are verified by the encryption key and the node ID. IBS scheme has the following procedures.

Extraction- Node obtains its private key and ID from the timestamp of the node.

Signature signing- The sensor node picks the key and computes digital signature for the node and broadcasts throughout the network.

Verification- While receiving the data each nodes verifies the authenticity by checking the time stamp of time interval and finds whether the data is recent or not. If the verification is succeed it transfers the data to next node otherwise ignores it.

3.2 Iboos Protocol Strategy:

The SET-IBOOS scheme is introduced for the same principles to achieve higher efficiency in CWSNs. It acts as like the SET-IBS during communication.

In the protocol initialization the IBOOS reduces the computations and storage costs for signing process in IBS scheme for key pre-distribution the BS performs the following

- Generation of encryption key with asymmetric key management to encrypt the data information.
- It further creates the master key for the encrypted data transmission.

Security to the data that are transmitted between the cluster nodes is accomplished by the key management.

Extraction- Node obtains its private key and ID from the timestamp of the node.

Offline signature- The sensor node picks the key and computes digital offline signature for the node and keeps it as the knowledge about the active data transmissions.

Online signature- It further computes online digital signature from the offline signature and the encrypted sensed data then broadcast throughout the network.

Verification- While receiving the data each nodes verifies the authenticity by checking the time stamp of time interval and finds whether the data is recent or not. If the verification is succeed it transfers the data to next node otherwise ignores it.

4 Set-Ibs Protocol:

Security to the data that are transmitted between the cluster nodes is accomplished by the key management facility of encryption scheme. The generated signatures are verified by the encryption key and the node ID. IBS scheme has the following procedures.

Extraction- Node obtains its private key and ID from the timestamp of the node.

Signature signing- The sensor node picks the key and computes digital signature for the node and broadcasts throughout the network.

Verification- While receiving the data each nodes verifies the authenticity by checking the time stamp of time interval and finds whether the data is recent or not. If the verification is succeed it transfers the data to next node otherwise ignores it.

5 Set-Iboos Protocol:

Security to the data that are transmitted between the cluster nodes is accomplished by the key management.
Extraction- Node obtains its private key and ID from the timestamp of the node.

Offline signature- The sensor node picks the key and computes digital offline signature for the node and keeps it as the knowledge about the active data transmissions.

Online signature- It further computes online digital signature from the offline signature and the encrypted sensed data then broadcast throughout the network.

Verification- While receiving the data each nodes verifies the authenticity by checking the time stamp of time interval and finds whether the data is recent or not. If the verification is succeed it transfers the data to next node otherwise ignores it.

6 Protocol Appearances:

The SET-IBS and SET-IBOOS protocols present secure data transmission for cluster based WSNs with the ID-based settings and then we use ID information and digital signature for authentication. The SET-IBS and SET-IBOOS protocols are solve the orphan-node problem from using the asymmetric key management for cluster based WSNs. These protocols using the ID information and digital signature for verification.

Protocol Assessments:

In this section we use three types of attacks and provide security analysis of protocols of these attacks. We use the network simulation tool NS2 to simulate SET-IBS and SET-IBOOS protocols.

7.1security Investigation:

To determine the security model we have to use some of the attack models in wireless sensor networks. The types of attacks are used here to threaten the network protocols.

Passive attack on WSNs:

Passive attackers are able to perform and monitoring the points of a network. It can be communicate with other nodes in the network. They can begin with the traffic analysis or statistical analysis in the based on the network.

Active attack on WSNs:

Active attackers have more capacity than passive attackers, can change the wireless medium. The attackers can copy, reply and modify the messages in the network at the time of data transmitting between the nodes.

Node compromising attack:

The attackers can access the secret information through the sensor nodes while the attackers can physically compromise those sensor nodes. The attacker can also change the performance of the sensors in the network and the action can be varied from this originality.

7.2 Simulation Result:

The lifetime of node is more essential in SET-IBS and SET-IBOOS protocols while transmitting the data between the nodes. We ensure the performance evaluation for the node lifetime and number of moving nodes.

Network lifetime:

The network indicates the duration of the data transmission between two nodes. We can enlarge the duration of data transmission.

Number of moving nodes:

The WSNs only depends on the moving nodes in the network for sensing and collecting information in from the nodes. We can evaluate the functionality of WSNs using these moving nodes.

Conclution:

In this paper we analyses the data transmission and security in cluster based WSNs. We use two kinds of protocols like SET-IBS and SET-IBOOS for the purpose of efficient data transmission between two nodes. The protocols SET-IBS and SET-IBOOS are more efficient in communication and we apply the ID based cryptography system for secure data transmission and we solve the problems in data transmission using

asymmetric key management. Finally the result indicates the SET-IBS and SET-IBOOS protocols have better performance than other protocols in this data transmission.

REFERENCES

[1] Wang, Y., G. Attebury and B. Ramamurthy, 2006. "A Survey of Security Issues in Wireless Sensor Networks," IEEE Comm. Surveys & Tutorials, 8(2): 2-23, Second Quarter.
[2] Abbasi, A.A. and M. Younis, 2007. "A Survey on Clustering Algorithms for Wireless Sensor Networks," Computer Comm., 30(14/ 15): 2826-2841.
[3] Oliveira, L.B., 2007. "SecLEACH-On the Security of Clustered Sensor Networks," Signal Processing, 87: 2882-2895.
[4] Diffie, W. and M. Hellman, 1976. "New Directions in Cryptography," IEEE Trans. Information Theory, IT-22(6): 644-654.
[5] Even, S., O. Goldreich and S. Micali, 1990. "On-Line/Off-Line Digital Signatures," Proc. Advances in Cryptology (CRYPTO), 263-275.
[6] Xu, S., Y. Mu and W. Susilo, 2006. "Online/Offline Signatures and Multisignatures for AODV and DSR Routing Security," Proc. 11th Australasian Conf. Information Security and Privacy, 99-110.
[7] Castelluccia, C., E. Mykletun and G. Tsudik, 2005. "Efficient Aggregation of Encrypted Data in Wireless Sensor Networks," Proc. Second Ann. Int'l Conf. Mobile and Ubiquitous Systems: Networking and Services (MobiQuitous), 109-117.
[8] Huang Lu, Jie Li and Mohsen Guizani, 2014. "Secure and Efficient Data Transmission for Cluster Based Wireless Sensor Networks" IEEE transactions on parallel and distributed systems, 25(3).
[9] Hankerson, D., S. Vanstone and A. Menezes, 2004. Guide to Elliptic Curve Cryptography. Springer.
[10] Hess, F., 2003. "Efficient Identity Based Signature Schemes Based on Pairings," Proc. Ninth Ann. Int'l Workshop Selected Areas in Cryptography (SAC), 310-324.