AN AUTHENTICATIVE WAY TO DATA TRANSMISSION FOR CLUSTER BASED WIRELESS SENSOR NETWORK

Sandhyarani B H[1], Nagnath Biradar[2], T.S.Vishwanath[3]

[1]PG Scholar (DCN), ECE Dept, BKIT Bhalki.
[2]ECE Dept, BKIT, Bhalki.
[3]Prof. and head ECE Dept BKIT Bhalki.

Abstract

Due to wireless nature of sensor network, secure data transmission is a major issue for wireless sensor network. Clustering is a technique which increases network lifetime and reduces power consumption of sensor nodes in WSN. In this paper, we study an authenticative way to data transmission for cluster based WSN. We propose two protocols for authentication of data, those are secure and efficient data transmission protocols SET-IBS and SET-IBOOS, by using identity-based digital signature (IBS) scheme and identity-based online and offline digital signature (IBOOS) scheme. This protocol relies on ID-based cryptography. SET-IBOOS further minimize the computational overhead. Our result show that performance of proposed protocols are better than existing secure protocols.

Keywords- *Cluster-based WSNs, K-medoid, Identity-based digital signature, Identity-based online and offline digital signature, secure data transmission protocol.*

----------***----------

1. INTRODUCTION

Wireless sensor network (WSN) is a network that consists of several sensor nodes that are randomly distributed on a geographical area. These sensor nodes are used to monitor the physical and environmental conditions like temperature, pressure, humidity etc. WSN consist of hundreds or even thousands of sensor devices. Each node is capable of data sensing, processing and communicating [1]. Sensor nodes relay the sensed data to the Base station (BS).BS transmits that data to the users as shown in figure 1. Users can get the information from base station through satellite or internet. BS in WSN acts as an interface between sensor nodes and user [2]. WSN are used in many applications like health care monitoring, industrial monitoring, military applications, environmental and earth sensing.

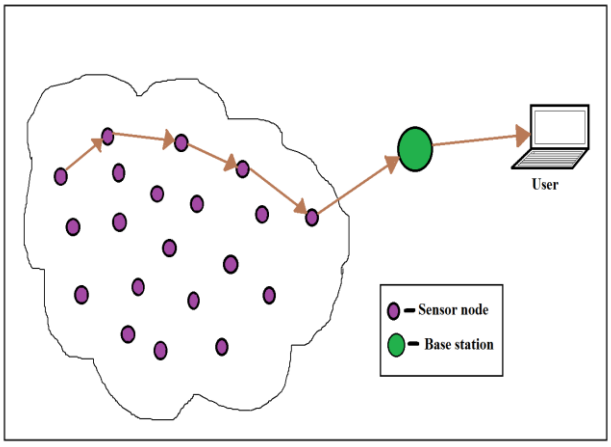

Fig 1: Overview of Wireless sensor network

Each sensor node consist of sensors, transreceiver, microcontroller and power unit [3]. Sensor nodes are mainly operated on batteries. Battery of sensor devices are limited. Sensor nodes are deployed in hard to reach locations or remote areas. So replacing or recharging of battery is inconvenient. resource constraints of sensor nodes are limited battery power, limited memory and energy [4]. Energy and communication bandwidth are the two key challenges of WSN. Sensor nodes require more energy for communication than data processing. To increase network scalability, network lifetime and to reduce the power consumption of sensor nodes, we introduced clustering technique [5]. For forming the clustering of sensor nodes, we proposed K-medoid protocol which is more efficient for large WSN.

Sensor nodes in WSN communicates through wireless link. So, WSN are more vulnerable to attacks. Due to wireless nature of sensor networks security is a critical issue in WSN. In this paper, for transmitting the data securely in a wireless network, we proposed two secure and efficient data transmission protocols called SET-IBS (Identity-based digital signature) and SET-IBOOS (Identity-based online and offline digital signature). These protocols are based on ID-based cryptography [6]. The main objectives of these protocols are to provide authentication to data. The remainder of this paper is organized as: Network architecture is presented section 2. In section 3, cluster network model is discussed. Section 4 presents the proposed protocols. Section 5 shows simulation results. Section 6 represents the conclusion of paper.

2. NETWORK ARCHITECTURE

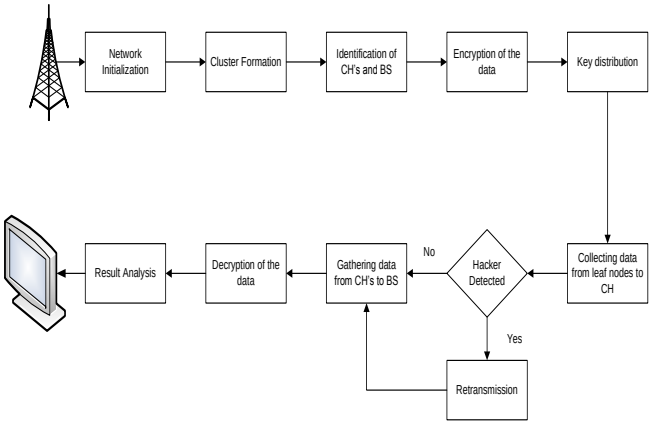

Fig 2: Network architecture

Consider a WSN consist of a fixed BS and several sensor nodes which are interconnectd wirelessly. Each sensor node has same functionalities and capabilities. network is initiated by deploying the number of nodes randomly on a geographical area. To reduce power consumption of each node and to increase the lifetime of the network we proposing a cluster network model. here we grouping nodes into a cluster. After formation of clusters one node is selected as cluster head (CH) in each cluster. And other nodes are leaf nodes. Leaf nodes sense the data, process the data and transmit to the CH. before transmission of data, leaf node apply encryption method on data by which it convert plain text of data into the cipher text. for encryption and decryption method key is pre distributed to all sensor nodes by the BS. The CH aggregates all the data from leaf nodes and check the authenticity of data. If the data is valid then CH transmit these data to BS. Otherwise it rejects that data and inform the leaf node to retransmit that data.

3. CLUSTER NETWORK MODEL

Clustering is a technique by which the sensor nodes are grouped into clusters [5]. In each cluster there is one cluster head (CH) i.e. the leader of the cluster. Each sensor node sense the data, process it and transmit this data to the CH. Then CH aggregates the data from sensor nodes which lies in its cluster and transmit this data to the base station (BS). BS is a master node in the network which has unlimited power.BS acts as a gateway between sensor nodes and user.BS transmit that data to the user through internet or satellite. Cluster network model is shown in figure 3.

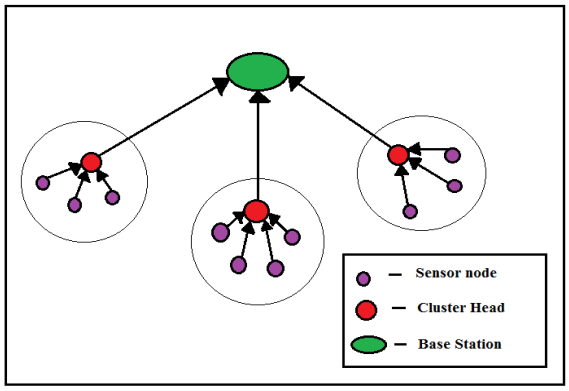

Fig 3: Cluster network model

In this paper, we are using K-medoid clustering algorithm for the formation of clusters. K-medoid algorithm is an adaptation of K-means algorithm. K-medoid protocol chooses that sensor node as a cluster head (CH) which lies almost centre of the cluster. Where as in K-means [7] protocol cluster head (CH) can be anywhere. K-medoid protocols are better than the K-means protocol. K-medoid is more robust to the attackers than K-Means. Therefore performance of K-medoid in clustering is better than K-means. K-medoid protocol is more efficient for large WSN [8].K-medoid protocol is better than LEACH [9], HEED [10] and K-means protocol.

3.1 Algorithm of K-medoid

K-medoid protocol calculates the distance matrix of each sensor node in WSN. In distance matrix, it stores distance between each sensor node and other nodes that lies in the network. K-medoid randomly chooses K cluster heads from the network. then it adds each sensor nodes to the nearest cluster head based on the minimum distance. It forms K clusters by looking distance matrix. After formation of clusters, it re-elect cluster head (CH) ,which lies almost centroid of the cluster. By having centroid node as a CH sensor nodes can have better communication and lower packet delay.

Algorithm of K-medoid :
1. Choose K initial cluster heads randomly.
2. Adds each sensor nodes to the initial cluster heads based on minimum distance.
3. Formation of K clusters in the network.
4. Re-election of central cluster heads in the clusters.

4. PROPOSED PROTOCOLS

To provide authentication to the transmitted data two secure and efficient data transmission protocols are proposed called Identity-based digital signature (SET-IBS) and Identity-based online and offline digital signature (SET-IBOOS). These two protocols uses ID-based cryptography in which identification of the node (ID) is used as their public key and private key can be generated without auxiliary data transmission. Therefore, the secure protocol is efficient in communication. These two protocols are applied on cluster

based wireless sensor network (CWSN) for the better performance of the network. IBS protocol is proposed to transmit the data securely in the wireless network and to make the network robust against the attackers like passive attacks, active attacks and compromised nodes. The IBOOS scheme has been proposed to minimize the computational overhead and storage costs of signature processing. Generation of offline signature in IBOOS is more faster. The main objective of these protocols is to secure and efficient data transmission between leaf node and CH and between CH and base station (BS). The existing system uses symmetric key management,which leads to orphan node problem. This can be solved by using proposed protocols.

4.1 IBS Scheme

IBS is based on IBS scheme. It has four phases like setup at the BS, key extraction, signature signing and verification.
1. Setup at the BS: The BS generates master key (msk) and public parameters (param) and broadcast these to all sensor nodes in the network.
2. Key extraction: Sensor nodes generates private key by using ID of the node and master key (msk) transmitted by the base station.
3. Signing of signature: Signature (sign) is created by using a time-stamp (t), signing key (θ) and message (M).
4. Verification of the data receiving nodes: Verification is done at the receiving nodes by using the digital signature (sign), ID of the node and message (M). the receiving node accepts the message (M) if sign is legal, otherwise rejects the message (M).

Workflow of SET-IBS Protocol

SET-IBS is based on ID-based cryptography in which identification of the node (ID) is used as their public key and private key can be generated without auxiliary data transmission. It creates digital signature [11] and attach this digital signature to the sensed encrypted data. This process is done at the sending node. At receiver, node uses public key to decrypt the transmitted message. Then node test the validity of the digital signature of received message. If the digital signature is valid it accepts the message and transmit to base station (BS). If the digital signature is invalid, it shows that the transmitted message is altered or modified. Then it reject that message and inform sending node to retransmit that message again.

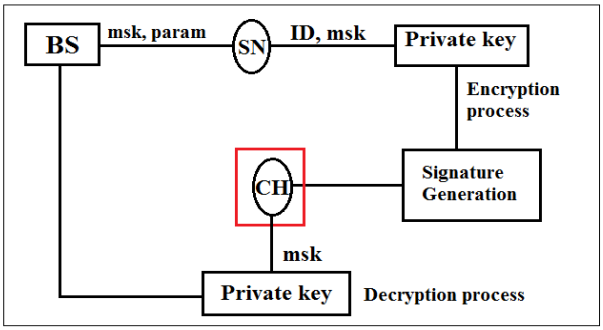

Fig 4: Workflow of SET-IBS protocol

4.2 IBOOS Scheme

An IBOOS scheme has five phases. IBOOS scheme is similar to IBS scheme. In IBOOS scheme signature is generated in two phases. Those are online signature and offline signature. The IBOOS scheme has five phases those are:
1. Setup at the BS: The BS generates master key (msk) and public parameters (param) similar to IBS scheme.
2. Key extraction: Sensor nodes generates private key by using ID of the node and master key (msk) transmitted by the base station.
3. Offline signing: Offline signing (offline sign) is done at the receiver node by using given parameters and time stamp (t).The cluster head transmit offline sign to leaf node.
4. Online signing: Online signature (online sign) is generated at sending node by using private key, offline sign and message (M).
5. Verification: Verification is done at the receiving nodes by using the digital signature (sign), ID of the node and message (M). the receiving node accepts the message (M) if sign is legal, otherwise rejects the message (M).

Workflow of SET-IBOOS Protocol

SET-IBOOS is proposed to minimize the computational overhead and to improve the performance of the network. Working of IBOOS is similar to IBS protocol. In IBOOS protocol to reduce computational overhead, signature signing is divided into two phases. i.e. online and offline. Offline signing is done at the receiver before message has been known. Advantage offline sign is it can be performed easily. By using this offline sign online signature is generated at sender node. Online sign is computed after message is known. This process is much faster than the IBS protocol. Workflow of IBOOS protocol is shown in fig 4.

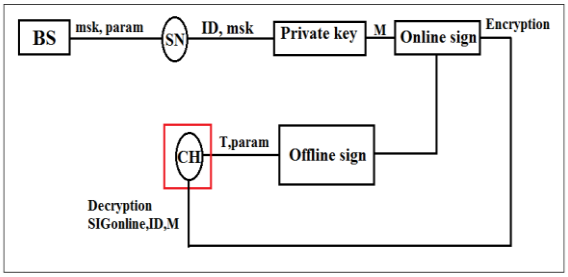

Fig 5: Workflow of IBOOS protocol

5. SIMULATION RESULT

MATLAB software is used for simulation. Performance of proposed protocols is measured in terms of network lifetime, energy consumption. Average end to end delay increases as no. of nodes increases, then overhead increases as shown in figure 6. By using proposed protocols IBS and IBOOS, sensor nodes consume less energy as compared to existing protocols as shown in figure 7. Figure 8 shows probability of success v/s no .of nodes. In this figure probability of success of proposed protocols is compared with existing protocols. As shown in figure performance of proposed protocol is better than existing protocol.

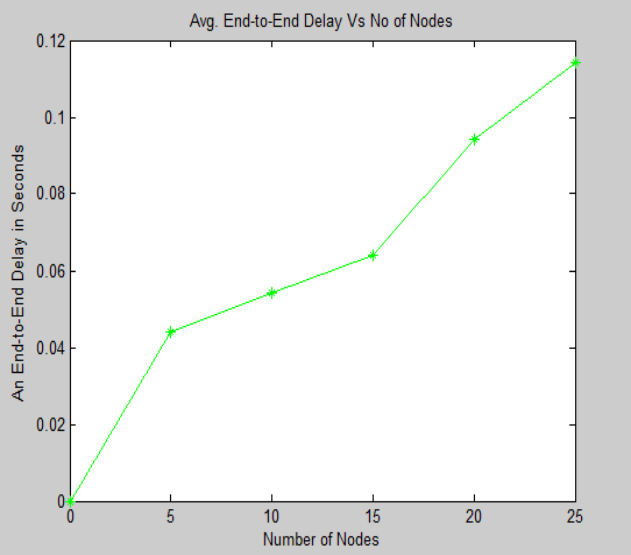

Fig 6: Average end to end delay v/s No of nodes

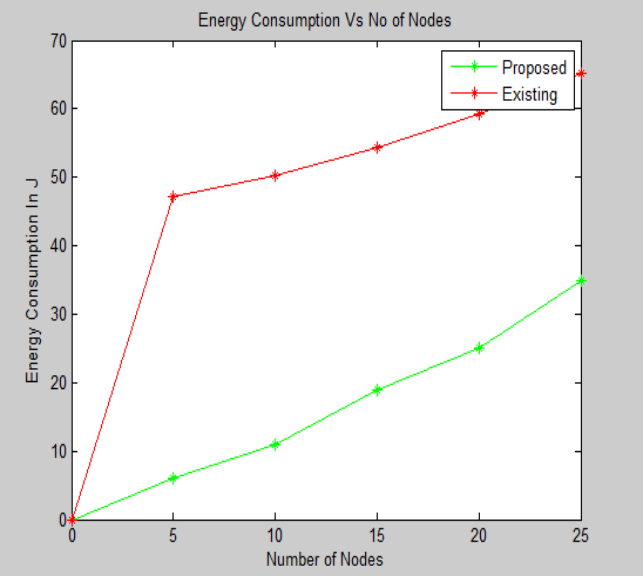

Fig 7: Energy consumption v/s No. of nodes

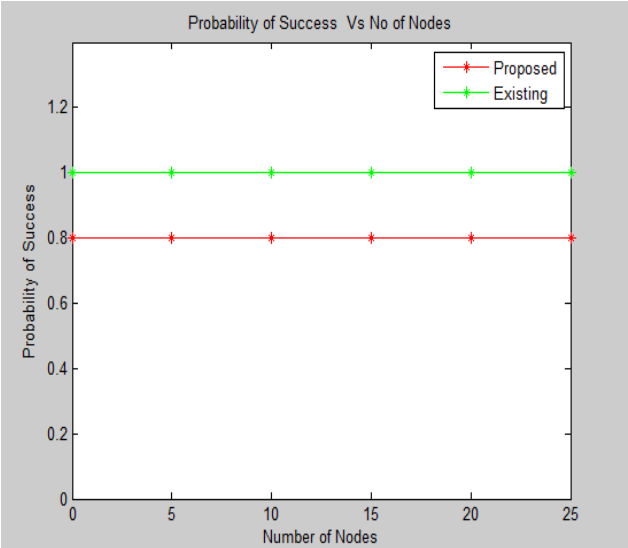

Fig 8: Probability of success v/s No. of nodes

6. CONCLUSION

In this paper, we discussed about security issues of wireless sensor network. To increase network lifetime and to reduce the power consumption of nodes, clustering of nodes is formed. K-medoid protocol used for clustering is more robust against attackers and efficient for large WSNs. SET-IBS and SET-IBOOS protocols are proposed to provide security and to provide authentication to the data. These protocols solve orphan node problem and have better performance in the network. IBOOS protocol minimizes the overhead that occurs in IBS protocol.

REFERENCES

[1]. K.Sohraby, D.,Minoli, T.,Znati, "Wireless sensor network: technology, protocols, and applications" ,John Wiley and sons, 2007 ISBN 978-0-471-74300-2,pp.203-209.
[2]. Pratibha, Dr. Prem Chand vashist, "A Detail Survey on Wireless Sensor Networks (WSNs) Security Issues" International Journal of Computer Science and Mobile Computing, Vol.3 Issues. 7, July-2014, pg. 111-118.
[3]. I.F. Akyildiz et al., "A Survey on Sensor Networks," IEEE Commun. Mag., vol. 40, no. 8, Aug. 2002, pp, 102-114.
[4]. D.W.Carman, P.S.Krus, and B..Matt, "Constraints and approaches for distributed sensor network security", Technical Report 00-010, NAI Labs, Network Associates Inc., Glenwood, MD, 2000.
[5]. Basilis Mamalis, Damianos Gavalas, Charalampos Konstantopoulos and Grammati Pantziou "Clustering in Wireless Sensor Networks" pp. 326. 2009-06-24.
[6]. M. Boujelben, H. Youssef, R. Mzid and M. Abid, "IKM - An Identity based Key Management Scheme for Heterogeneous Sensor Networks", Journal of Communications, vol. 6, no. 2, April 2011.
[7]. Geon Yong Park, Heeseong Kim, Hwi Woon Jeong, and Hee Yong Youn, "A Novel Cluster Head Selection Method based on K-Means Algorithm for Energy Efficient Wireless Sensor Network" AINAW, vol.1,pp.910-915,IEEE,2013.
[8]. Priyanka Devi, Khushneet Kaur, Doaba Institute of Engineering and Technology "A Robust Cluster head Selection Method Based on K-medoids Algorithm To Maximise Network Lifetime and Energy Efficiency For Large WSNs" Vol. 3 Issues 5, May–2014.
[9]. Heinzelman W, Chandrakasan A, Balakrishnan H. Energy Eficient Communication Protocol for Wireless Microsensor Networks, In Proceedings of the 33rd Hawaii International Conference on Systerm Sciences. Maui: IEEE Computer Society, 2000, vol. 2:3005-3014.
[10]. Ossama Younis and Sonia Fahmy. 2004.Distributed Clustering in Ad-hoc Sensor Networks: A Hybrid, Energy-Efficient Approach.In Proceedings of IEEE INFOCOM, Hong Kong, an extended version appeared in IEEE Transactions on Mobile Computing, 3(4).
[11]. E.S,Ismail, N.M.Tahat and R.R.Ahmad, Anew digital signature scheme based on factoring and discrete algorithms. Journal of Mathematics and Statistics, 4(4) 2008, pp:222-225.