INTERNATIONAL JOURNAL FOR TRENDS IN ENGINEERING & TECHNOLOGY
VOLUME 3 ISSUE 3 – MARCH 2015 – ISSN: 2349 – 9303

Improved Identity Based Digital Signature Scheme for Enhancing Security and Efficient Data Transmission

Abinaya J.[1]
[1]SNS College of Technology,
M.E. Communication Systems, Dept. of E.C.E.
jeenisabi5@gmail.com

Prabakaran T.[2]
[2]SNS College of Technology,
Associate professor, Dept. of E.C.E.
prabaakar.t@gmail.com

Abstract - Secure data communication is a significant issue in wireless sensor networks (WSNs). Clustering is an efficient and useful way to augment the system performance of WSNs. The secure data communication for a cluster-based wireless sensor networks (CWSNs), where the clusters are created dynamically and occasionally is considered. The Identity-Based digital Signature (IBS) scheme and the improved Identity-Based Online/Offline digital Signature (IBOOS) scheme are used for secure and efficient data transmission (SET). In SET-IBS, safety relies on the rigidity of the Diffie-Hellman problem and the SET-IBOOS additionally reduces the computational overhead for protocol safety, which is vital for WSNs. The possibility of the improved SET-IBOOS protocol with respect to the security requirements and security analysis against different attacks is analyzed. The calculations and simulations are provided to demonstrate the efficiency of the proposed protocol. It improves the security overhead and the energy conservation.

Index Terms - clustering, energy efficient, security, wireless sensor networks.

1 INTRODUCTION

1.1 Wireless Sensor Networks

A wireless sensor network (WSN) consists of randomly distributed independent sensors to observe physical or environmental conditions, such as temperature, pressure, sound, flow of liquid etc and to considerately pass their information through the network to a different node in the network. The expansion of wireless sensor networks was aggravated by military applications such as battleground examination, today such networks are used in many industrialized and customer applications, such as industrial procedure monitoring and management. The WSN is built of nodes beginning a few to several thousands, where each node is connected to a sensor. The topology of the WSNs can vary from an easy star network to a complex multi-hop wireless interconnect network. The transmission of information between the hops of the system can be routing or through flooding.

1.2 Security Vulnerabilities and Protocol Objectives

The data communication protocols for WSNs, as well as cluster-based protocols (LEACH-like protocols), are susceptible to a number of safety attacks [2], [3]. Particularly, attacks to CHs in CWSNs could affect in severe harm to the network because data communication and data summing up depend on the CHs essentially. If an aggressor manages to conciliation or pretend to be a CH, it can aggravate attacks such as sinkhole and selective forwarding attacks, hence distracting the network. On the other hand, an aggressor may intend to introduce fake sensing data into the WSN, for example, the fake node act as a leaf node sending fake information toward the CHs. Yet, LEACH-like protocols are tougher against the attacks than the other types of protocols in the network [3]. It is because CHs are revolving from nodes to nodes in the system by rounds, which makes it difficult for foreigners to recognize the routing elements as the mediatory nodes and attack them. The uniqueness of LEACH-like protocols decreases the risks of being attacked on mediatory nodes, and makes it difficult for an opponent to recognize and compromise important nodes. The purpose of the projected safe data communication for CWSNs is to assure the secure and well-organized data communication between leaf nodes and CHs, as well as communication between CHs and the BS. Temporarily, most of the presented secure communication protocols for CWSNs in the literature [8], [9], though, use the symmetric key management for safety, which suffers from the orphan node problem. In this paper, it aims to solve this orphan node problem by using the ID based cryptosystem that guarantees safety requirements, by using the IBS scheme [1].

2 EXISTING SYSTEM

2.1 Set-IBS Protocol

The SET-IBS protocol has a protocol initialization phase prior to the system exploitation and operates in rounds during communication, which consists of two phases namely a setup phase and a steady-state phase in each round.

2.2 IBS Scheme for CWSNs

A SET-IBS scheme implemented for CWSNs consists of the following steps, purposely, setup at the BS node, key extraction and signature signing at the data sending nodes, and verification at the information receiving nodes:

- *Setup phase*. The base station produces a master key *msk* and the public parameters *param* for the private key generator (PKG), and gives them to all sensor nodes.
- *Extraction phase*. Given an ID string, a sensor node produces a private key sek*ID* related with the ID using *msk*.
- *Signature signing phase*. Given a data M, t time stamp and θ a signing key, the sending node produce a signature SIG.
- *Verification phase*. Given the ID, M, and SIG, the receiving node outputs “accept” if SIG is valid, and outputs “reject” otherwise.

2.3 Protocol Operation

Following the protocol initialization phase of key distribution, SET-IBS operates in rounds during data transmission. Each round consists of a phase setup and a phase steady state. The operation of protocol SET-IBS is divided by rounds as shown in Fig.1, which is similar to other protocols similar to LEACH. Each round consists of a phase setup for forming clusters from CHs, and a phase steady state for broadcasting data from sensor nodes to the BS. In each round, the time span is separated into successive time slots by the TDMA process [4]. Sensor nodes broadcast the obtained data to the CHs in each frame of the phase steady state. For energy consumption, nodes are arbitrarily elected as CHs in each of the round, and the other non-CH sensor nodes the leaf nodes join clusters using one-hop communication, based on the maximum obtained signal strength of CHs. To select CHs in a new circle, each sensor node obtains an arbitrary number and evaluates it with a given threshold. If the value is less than the given threshold value, the sensor node becomes a CH for the current round of data transmission. In this way, the new CHs are self-elected only on their own decisions. Therefore, SET-IBS method functions without data communication with each other in the CH rotations.

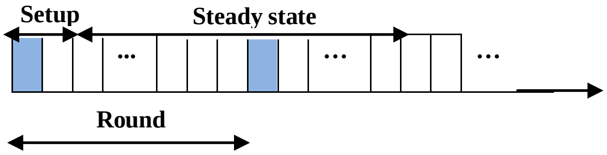

Fig.1. Operation in secure data transmission

3 PROPOSED SYSTEM

The improved SET-IBOOS protocol is planned with the same reason and method for CWSNs with superior effectiveness. The proposed SET-IBOOS operates similarly to the earlier SET-IBS, which has a protocol initialization phase prior to the network exploitation and works in rounds during communication. It describes the following steps

- Protocol initialization
- Key management
- Protocol operations

3.1 Protocol Initialization

To reduce the computation and storage costs of signature signing processing in the IBS scheme is done by introducing SET-IBOOS method. The process of the protocol initialization in SET-IBOOS is similar to that of SET-IBS method; however, the operations of key pre distribution are revised for IBOOS. The Base Station does the following operations of key pre distribution in the network

- Create an encryption key k for the homomorphic encryption scheme to encrypt data messages, where k ϵ [m -1], m is a large integer.
- Generate the pairing parameters (p,q,E/F_p,G1,G2,e)as described .Select a generator P of G1 stochastically.
- For each node j, randomly select r_j ϵ Z_q for its private key generation, and let H be a hash function.
- Preload each sensor node j with the public parameters, given by *param*j= (k,m,G,q,r,rj,H)

3.2 Protocol Features

The protocol characteristics and hierarchical clustering solutions are presented in this section. It first summarizes the features of the SET-IBS and SET-IBOOS protocols. These protocols provide secure data transmission for CWSNs with concrete ID-based settings, which uses the ID based information and digital signature for authentication. Thus the SET-IBS and SET-IBOOS protocols fully solve the orphan-node problem from using the symmetric key management for CWSNs. The proposed secure data transmission protocols are with the existing ID-based settings, which uses the ID based information and digital signature for authentication. Comparing the SET-IBS with SET-IBOOS requires less energy for computation and storage. In addition, the SET-IBOOS is more appropriate for node-to-node exchanges in CWSNs, since the computation is easier to be executed. In improved SET-IBOOS, the offline signature is executed by the CH node, thus, sensor node do not have to perform the offline algorithm before it wants to sign on a new message. Moreover, the offline signature phase does not use any sensed data or secret information for signing. This is predominantly valuable for CWSNs because leaf sensor nodes do not need auxiliary communication for renewing the off-line signature. Each metric is explained as follows:

- **Key management feature:** The key cryptographies that are used in the procedure are to attain secure data communication, which consist of the symmetric and the asymmetric key based safety.
- **Neighborhood authentication feature:** Used for safe access and data communication to the close by sensor nodes, by approving with each other. Here, “restricted” means the likelihood of neighbour authentication, where the nodes with the joint pairwise key can authenticate to each other.
- **Storage cost feature:** Which represents the condition of the safety keys stored in the sensor node’s memory.
- **Network scalability feature:** Denotes whether a safety method is able to range without compromising the safety requirements.
- **Communication overhead feature:** The safety overhead in the data packets during message.
- **Computational overhead feature.** The power cost and calculation efficiency on the production and confirmation of the certificates or signatures for safety.
- **Attack resilience feature:** The types of attacks that safety procedure can defend against.

4 SIMULATION AND RESULTS

In the Fig.2, shows the network scenario consisting of hundred nodes randomly deployed in the network. It has a fixed base station and randomly selected cluster heads. The cluster head is selected based on the node composing of the highest remaining energy.

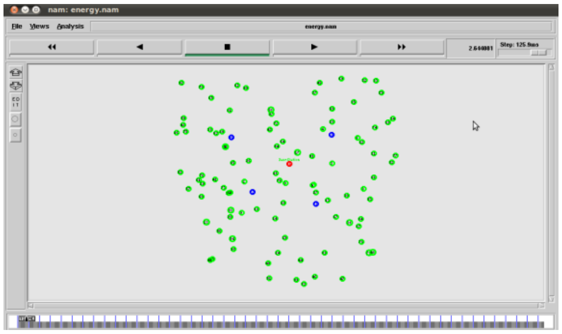

Fig. 2 Network scenario

The Fig.3 shows the nodes marked in yellow are nearing the threshold energy, here in this scenario the threshold energy is 0.3J, and nodes moving to energy below this level are termed to be dead nodes. The remaining nodes are involved in data transmission other than the dead nodes.

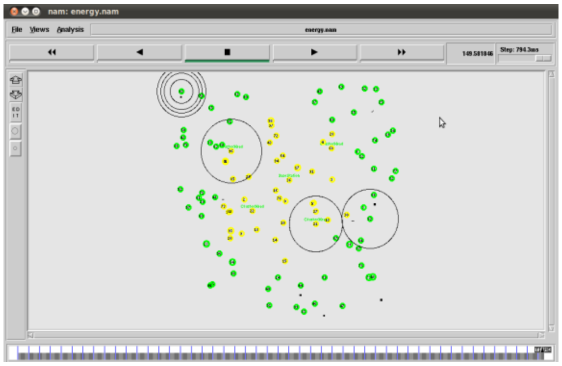

Fig.3. Nodes nearing threshold energy

The Fig.4 shows the remaining energy available at each node by using the improved IBOOS scheme. Hundred nodes are considered here for which the residual energy is calculated.

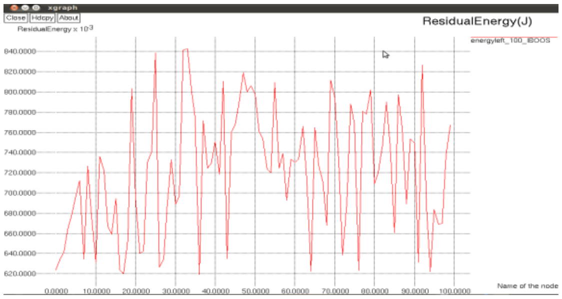

Fig. 4 Residual energy in IBOOS scheme

The Fig.5 shows the comparison about the residual energy available with the network when using the SET-IBS and SET-IBOOS scheme. Comparatively the use of IBOOS scheme shows higher remaining energy than the IBS scheme.

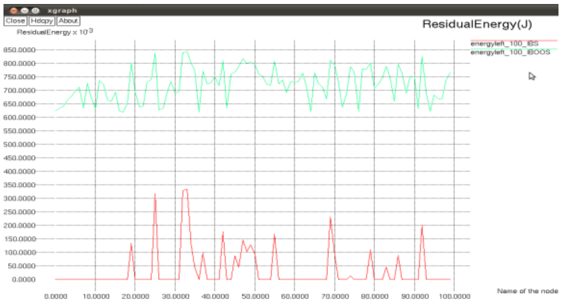

Fig.5 Residual energy comparison

The Fig.6 shows the energy consumed by the network by using the protocols SET-IBS and SET-IBOOS scheme are as shown below.

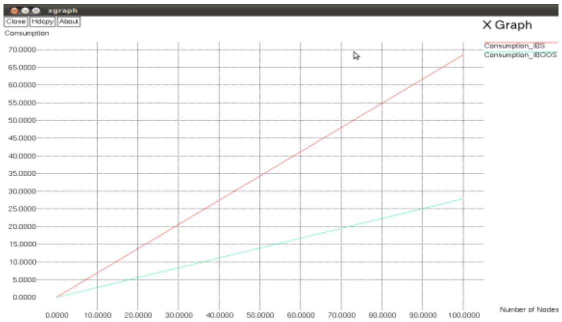

Fig.6 Energy consumed

5 CONCLUSION

The lack of the symmetric key management for safe data communication has been analyzed. This paper has been presented with two safe and efficient data communication protocols, respectively, for CWSNs, the SET-IBS, and the improved SET-IBOOS. In the assessment section, it provides the possibility of the SET-IBS and the SET-IBOOS with respect to the safety requirements and investigates against routing assaults. The SET-IBS and the SET-IBOOS are capable in the field of communication and applying for the ID based cryptosystem, which aim at safety requirements in CWSNs, as well as the solved orphan node problem present in the safe communication process with the symmetric key management. Lastly, the evaluation in the calculation and simulation results show that the SET-IBS and the improved SET-IBOOS protocols have better performance than the existing safe protocols for CWSNs. With respect to both the computation and the communication costs, it points out the qualities that using the improved SET-IBOOS with less secondary safety overhead is preferred for secure data communication in CWSNs. A new protocol have been proposed based on the existing LEACH protocol to save energy of the network. Energy efficiency was evaluated by calculating the number of alive nodes in the network by considering the number of rounds taken.

6 FUTURE WORK

As a future work the security of the network is to be improved by further enhancing the protocol.

REFERENCES

[1] Abbasi A.A.and Younis M., "A survey of clustering algorithms for wireless sensor networks", Computer Comm., Vol. 30, nos. 14/15, pp. 2826-2841, 2007.

[2] Divya C., Krishnan N. & Petchiammal A., "Increase the alive nodes based on the cluster head selection algorithm for heterogeneous wireless sensor networks", Global Journal of Computer Science and Technology Network, Web & Security, Vol. 13 Issue 9 Year 2013.

[3] Even S., Goldreich O., and Micali S., "On-line/off-line digital signatures", Proc. Advances in Cryptology (CRYPTO), pp. 263-275,1990.

[4] Heinzelman W., Chandrakasan A., and Balakrishnan H., "An application-specific protocol architecture for wireless microsensor networks", IEEE Trans. Wireless Comm., Vol. 1, no. 4, pp. 660-670, Oct. 2002.

[5] Hess F., "Efficient online/offline identity-based signature for wireless sensor network", Proc. Ninth Ann. Int'l Workshop Selected Areas in Cryptography , pp. 310-324, 2003.

[6] Huang Lu, Jie Li, Mohsen Guizani, "Secure and efficient data transmission for cluster-based wireless sensor networks", IEEE, transactions on parallel and distributed systems, Vol. 25, NO. 3, March 2014.

[7] Manjeshwar A., Zeng Q.A., and Agrawal D.P., "An analytical model for information retrieval in wireless sensor networks using enhanced apteen protocol", IEEE Trans. Parallel & Distributed Systems, Vol. 13, no. 12, Dec. 2002.

[8] Oliveira et al L.B., "Sec-leach – a random key distribution solution for securing clustered sensor networks", Signal Processing, Vol. 87, pp. 2882-2895,2007.

[9] Shamir A., "An identity-based security system for user privacy in vehicular ad hoc networks", Proc. Advances in Cryptology (CRYPTO), pp. 453, 1985.

[10] Wang Y., Atterbury G., and Ramamurthy B., "A survey on Wireless sensor network security", IEEE Comm. Surveys & Tutorials, Vol. 8, no. 2,pp.2-23,Second Quarter 2006.