THE INTERNATIONAL JOURNAL OF SCIENCE & TECHNOLEDGE

Secure and Efficient Data Transmission Cluster Based Wireless Sensor Network

Sachin Gavhane
Professor, Information Technology Department
Atharva College of Engineering, Mumbai, Maharashtra, India
Priyanka Patil
B.E. Information Technology Department
Atharva College of Engineering, Mumbai, Maharashtra, India
Anjana Patil
B.E. Information Technology Department
Atharva College of Engineering, Mumbai, Maharashtra, India
Suchita Gadekar
B.E. Information Technology Department
Atharva College of Engineering, Mumbai, Maharashtra, India

Abstract:
In wireless sensor networks (WSN), transmission of secure data is a difficult issue. So we implement protocols that are secure and efficient for cluster based wireless sensor network. Those two protocols are SET-IBS and SET-IBOOS.

Keywords: *LEACH, SET-IBS, SET-IBOOS*

1. Introduction

A wireless sensor network (WSN) is a network system is a collection of different devices using sensor nodes that monitor environmental or physical conditions like motion, temperature, and sound [1].
In cluster based WSNs (CWSNs), we study a secure transmission of data, so in that clusters are formed periodically and dynamically.
We use two Secure and Efficient data Transmission (SET) protocols for CWSNs, called SET-IBS and SET-IBOOS.
SET-IBS- Identity-Based digital Signature (IBS) scheme.
SET-IBOOS- Identity-Based Online/Offline digital Signature. The key idea of both SET-IBS and SET-IBOOS is to authenticate the encrypted data, by applying digital signatures to message packets [5].
Cluster-based data transmission in WSNs has been investigated to achieve the network scalability and management, which is used to reduce bandwidth and maximizes node lifetime [2].

2. Literature Survey

Source	Purpose	Results
A. Chandrakasan, and H. Balakrishnan, "An Application-Specific Protocol Architecture for Wireless Microsensor Networks," IEEE Trans. Wireless Comm., vol. 1, no. 4, pp. 660- 670, Oct. 2002.	LEACH protocol is implemented To reduce the total energy consumption for Cluster based WSNs. In network, LEACH randomly rotates CHs among all sensor nodes, in rounds, to prevent quick energy consumption of the set of CHs.	In terms of network lifetime LEACH achieves improvements.

S. Even, O. Goldreich, and S. Micali, "On-Line/Off-Line Digital Signatures," Proc. Advances in Cryptology (CRYPTO), pp. 263-275, 1990.	The signing of a message in this scheme is broken into two phases. Off –line is the first phase in this scheme. But it also requires a moderate amount of computation; it presents the advantage that it can be performed easily, before the message to be signed is even known. The second phase is on-line. It starts after the message becomes known, it utilizes the pre-computation of the first phase and is much faster.	The schemes which was introduced is a general method for constructing online/offline singnature

Table 1

3. Diagrams

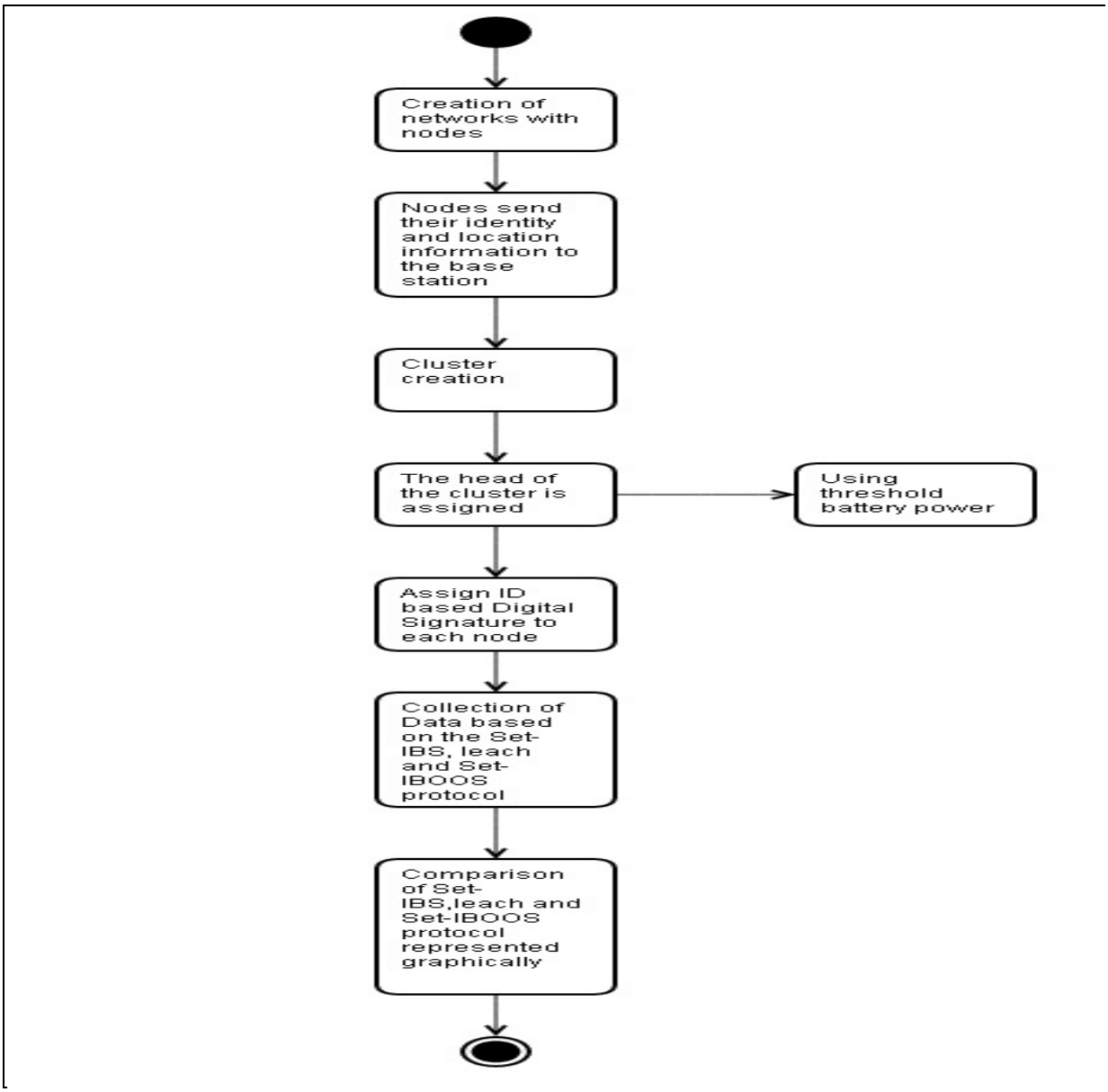

Figure 1: Block Diagram for the System

3.1. Data Flow Diagram for the System

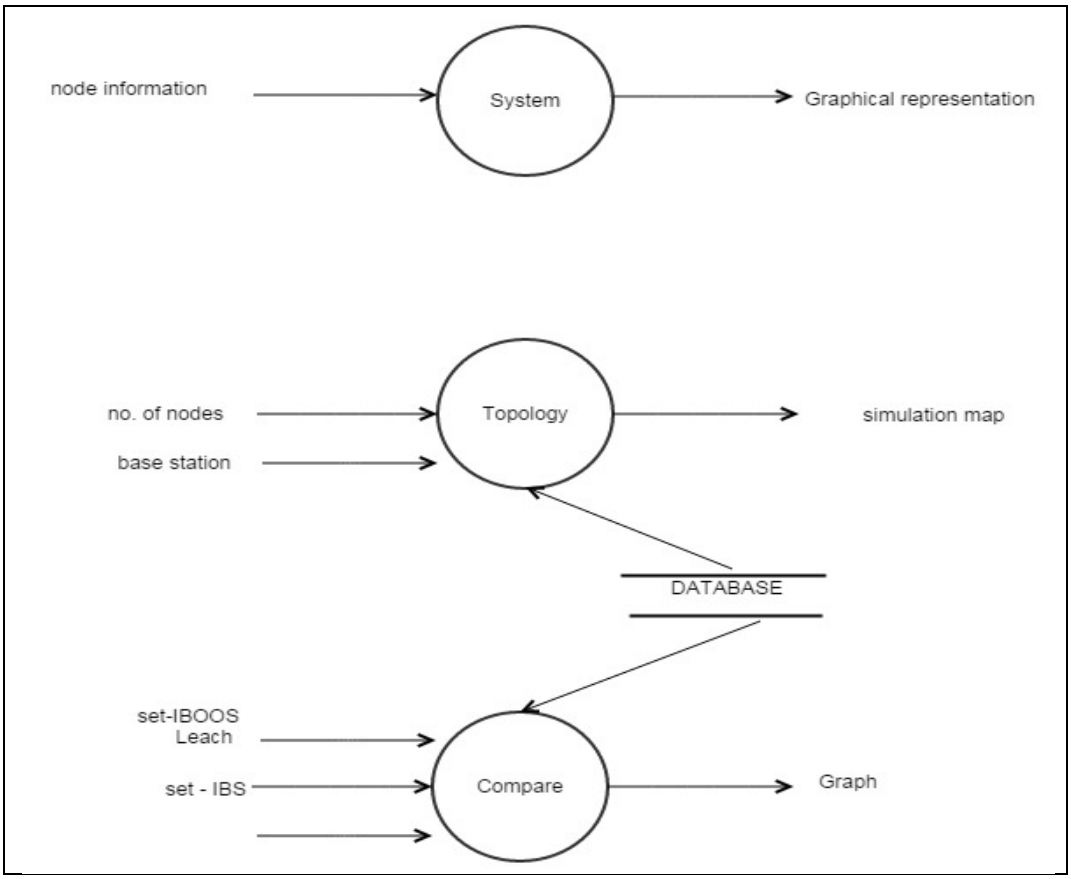

Figure 2: Data flow diagram

4. Methodology

We are using LEACH, SET-IBS and SET-IBOOS algorithm.

- LEACH stands for Lower Energy Adaptive Clustering Hierarchy which is presented by Heinzelman et al[3]. This protocol is effectively used to balance and reduce the total energy consumption for cluster based WSNs [4].
- In LEACH algorithm, the cluster heads are elected randomly, so the optimal number and distribution of cluster heads cannot be ensured. The nodes with low remnant energy have the same priority to be a cluster head as the node with high remnant energy. Therefore, those nodes with less remaining energy may be chosen as the cluster heads which will result that these nodes may die first. The cluster heads communicate with the base station in single-hop mode which makes LEACH cannot be used in large-scale wireless sensor networks for the limit effective communication range of the sensor nodes
- Both the protocols i.e. SET-IBS and SET-IBOOS provide secure data transmission for CWSNs with concrete ID-based settings that use ID information and digital signature for authentication.
- Thus, both the protocols SET-IBS and SET-IBOOS fully solve the orphan-node problem by using the symmetric key management for CWSNs.
- So the proposed protocols for secure data transmission are with concrete ID-based settings, which use digital signature and ID information for verification.
- Comparing the SET-IBS, SET-IBOOS requires less energy for storage and computation. Moreover, the SET-IBOOS is more suitable for node-to-node communication in CWSNs, since the computation is lighter to be executed.

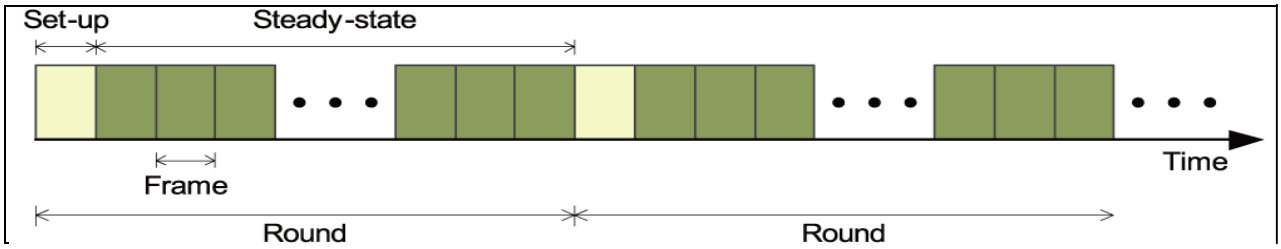

Figure 3: Operation in secure data transmission

5. Other Recommendations

- In this System, Secure and efficient data transmission is necessary and is demanded in many practical of WSNs. So, we propose two Secure and Efficient data Transmission (SET) protocols for CWSNs, which are SET-IBS and SET-IBOOS, IBS stands for Identity-Based digital Signature (IBS) scheme and IBOOS stands for Identity-Based Online/Offline digital Signature (IBOOS) scheme.
- It has been proposed in order to reduce the storage and computation and costs to authenticate the encrypted data, by using digital signatures to message packets, which are efficient in communication and applying the key management for security.
- In these protocols pairing parameters are distributed and preloaded in all sensor nodes by the BS initially.

6. Discussion & Conclusion

We presented two secure and efficient data transmission protocols for CWSNs, SET-IBS, and SET-IBOOS, respectively. In the evaluation section, we provided feasibility of the protocols SET-IBS and SET-IBOOS with respect to the security requirements and analysis against routing attacks. Lastly, the comparison in the calculation and simulation results show that for cluster based WSNs the SET-IBS and SET-IBOOS protocols have better performance than existing secure protocols for cluster based WSNs. With respect to both communication and computation costs, we notice the merits that using SET-IBOOS with less auxiliary security overhead is preferred for secure data transmission in Cluster based WSNs.

7. 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. 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.
3. W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "An Application-Specific Protocol Architecture for Wireless Microsensor Networks," IEEE Trans. Wireless Comm., vol. 1, no. 4, pp. 660-670, Oct. 2002.
4. 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.
5. D. Boneh and M. Franklin, "Identity-Based Encryption from the Weil Pairing," Proc. 21st Ann. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO '01), pp. 213-229, 2001.
6. 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.
7. L.B. Oliveira et al., "SecLEACH-On the Security of Clustered Sensor Networks," Signal Processing, vol. 87, pp. 2882-2895, 2007.
8. P. Banerjee, D. Jacobson, and S. Lahiri, "Security and Performance Analysis of a Secure Clustering Protocol for Sensor Networks," Proc. IEEE Sixth Int'l Symp. Network Computing and Applications (NCA), pp. 145-152, 2007.
9. S. Sharma and S.K. Jena, "A Survey on Secure Hierarchical Routing Protocols in Wireless Sensor Networks," Proc. Int'l Conf. Comm., Computing & Security (ICCCS), pp. 146-151, 2011.
10. G. Gaubatz et al., "State of the Art in Ultra-Low Power Public Key Cryptography for Wireless Sensor Networks," Proc. IEEE Third Int'l Conf. Pervasive Computing and Comm. Workshops (PerCom), pp. 146-150, 2005.
11. W. Diffie and M. Hellman, "New Directions in Cryptography," IEEE Trans. Information Theory, vol. IT-22, no. 6, pp. 644-654, Nov.1976.