SECURE AND EFFICIENT DATA TRANSMISSION FOR CLUSTER-BASED WIRELESS SENSOR NETWORKS

PRIYANKAA.B[1], SINDHUJA.M[2]

[1]*STUDENT, INFORMATION TECHNOLOGY, NEW PRINCE SHRI BHAVANI COLLEGE OF ENGINEERING AND TECHNOLOGY, TAMILNADU, INDIA*

[2]*ASSISTANT PROFESSOR, INFORMATION TECHNOLOGY, NEW PRINCE SHRI BHAVANI COLLEGE OF ENGINEERING AND TECHNOLOGY, TAMILNADU, INDIA*

ABSTRACT

Secure data transmission is a critical issue for wireless sensor networks wireless sensor networks. Clustering is an effective and practical way to enhance the system performance of wireless sensor networks. In this paper, we study a secure data transmission for cluster-based wireless sensor networks, where the clusters are formed dynamically and periodically. We propose two Secure and Efficient data Transmission (SET) protocols for cluster based wireless sensor networks, called SET-IBS and SET-IBOOS, by using the Identity-Based digital Signature (IBS) scheme and the Identity-Based Online/Offline digital Signature (IBOOS) scheme, respectively. In SET-IBS, security relies on the hardness of the Diffie-Hellman problem in the pairing domain. SET-IBOOS further reduces the computational overhead for protocol security, which is crucial for wireless sensor networks, while its security relies on the hardness of the discrete logarithm problem. We show the feasibility of the SET-IBS and SET-IBOOS protocols with respect to the security requirements and security analysis against various attacks. The calculations and simulations are provided to illustrate the efficiency of the proposed protocols. The results show that, the proposed protocols have better performance than the existing secure protocols for cluster based wireless sensor networks, in terms of security overhead and energy consumption.

Keywords: *Cluster-based WSNs, ID-based digital signature, ID-based online/offline digital signature, secure data transmission protocol.*

1.INTRODUCTION

A wireless sensor network (WSN) is a network system comprised of spatially distributed devices using wireless sensor nodes to monitor physical or environmental conditions, such as sound, temperature, and motion. The SET is a critical issue for wireless sensor networks (WSNs). Clustering is an effective and practical way to enhance the system performance of WSNs. Propose two Secure and Efficient data Transmission (SET) protocols for CWSNs, called SET-IBS and SET-IBOOS, by using the Identity-Based digital Signature (IBS) scheme and the Identity-Based Online/Offline digital Signature (IBOOS) scheme, respectively. In SET-IBS, security relies on the hardness of the cryptography problem in the pairing domain. SET-IBOOS further reduces the computational overhead for protocol security, which is crucial for WSNs, while its security relies on the hardness of the discrete logarithm problem. The SET-IBS and SET-IBOOS protocols with respect to the security requirements and security analysis against various attacks. The SET protocol to implement for one way hah function enhances the security and also provide random key generation algorithm. The results show that, the proposed protocols have better performance than the existing secure protocols for CWSNs, in terms of security overhead and energy consumption.

2.EXISTING SYSTEM

Existing LEACH-like protocols is challenging, because they dynamically, randomly and periodically rearrange the network's clusters and data links. There are providing steady long-lasting node-to-node trust relationships and common key distributions are inadequate for LEACH-like protocols (most existing solutions are provided for distributed WSNs, but not for CWSNs). This problem occurs when a node does not share a pair-wise key with others in its preloaded key ring, in order to mitigate the storage cost of symmetric keys, and the key ring is not sufficient for the node to share pair-wise symmetric keys with all of the nodes in a network. It cannot participate in any cluster, and therefore, has to elect itself as a CH. The orphan node problem reduces the possibility of a node joining a CH, when the number of alive nodes owning pair-wise keys decreases after a long term operation of the network. The orphan node problem increases the overhead of transmission and system energy consumption by raising the number of CHs. A sensor node does share a pair-wise key with a distant CH but not a nearby CH; it requires comparatively high energy to transmit data to the distant CH.

3.DISADVANTAGES:

- Very high key Management storage, use symmetric algorithm.
- Lot of Cryptography problem occur in Cluster Based Wireless Sensor Network
- Require high Energy to transmit data to the GH.

4. PROPOSED SYSTEM:

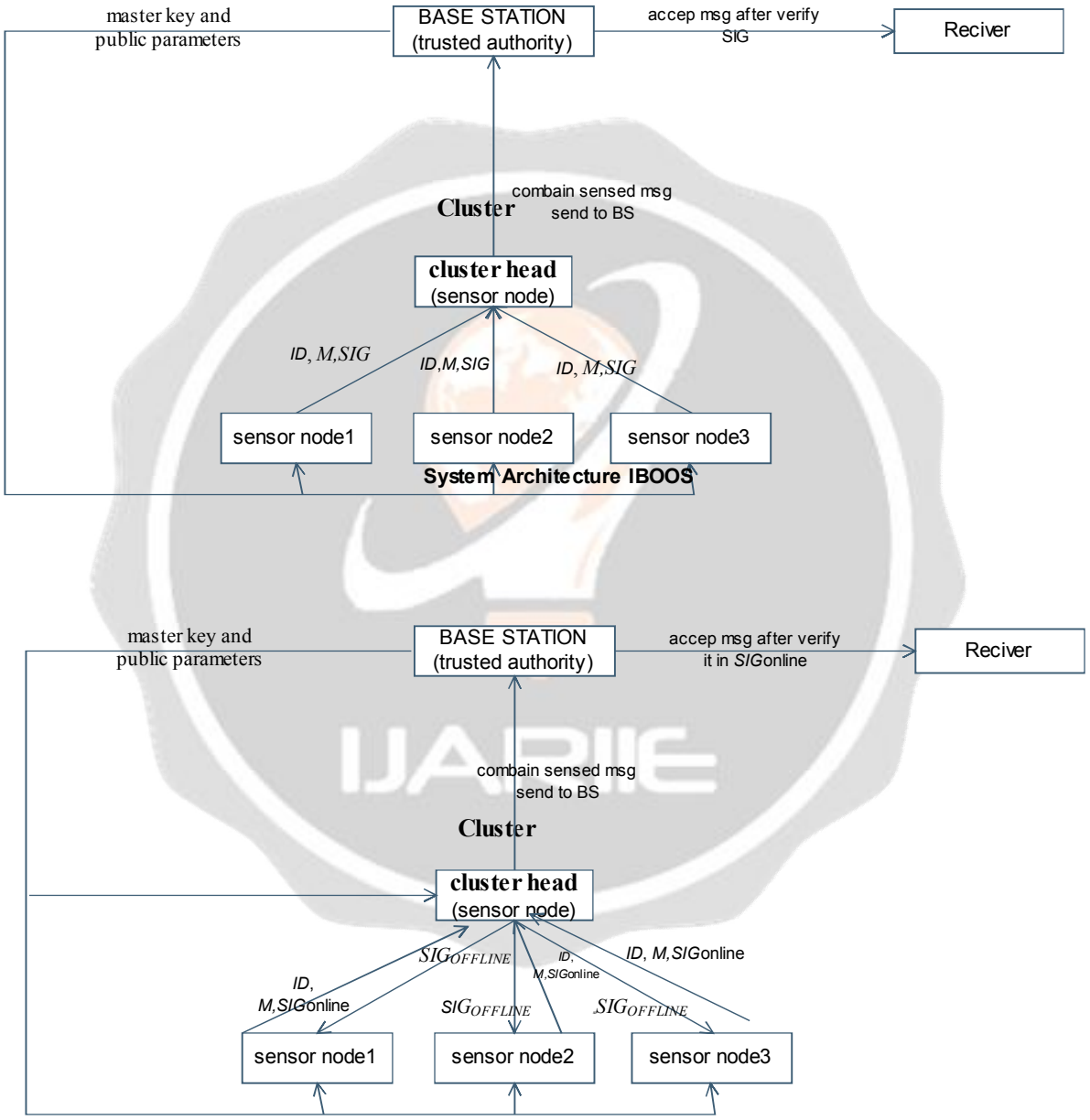
New approach applied and evaluated the key management of IBS to routing in CWSNs. In this project, to extend our previous work and focus on providing efficient secure data communication for CWSNs. Propose two **S**ecure and **E**fficient data **T**ransmission (SET) protocols for CWSNs, called **SET-IBS** and **SETIBOOS**, by using the **IBS** scheme and the **IBOOS** scheme, respectively. The key idea of both **SET-IBS** and **SET-IBOOS** is to authenticate the encrypted sensed data, by applying digital signatures to message packets. The proposed protocols, secret keys and pairing parameters are distributed and preloaded in all sensor nodes by the **BS** initially, which overcomes the key escrow problem described in **ID-based crypto-systems**. Secure communication in **SET-IBS** relies on the **ID-based cryptography**, in which, user public keys are their **ID** information. **SET-IBOOS** is proposed in order to further reduce the computational overhead for security using the IBOOS scheme, in which security relies on the hardness of the discrete logarithmic problem. The proposed protocols with respect to the security requirements and analysis against three attack models. Compare the proposed protocols with the existing secure protocols for efficiency by calculations respectively, with respect to both computation and communication.

5.ADVANTAGES:

- Efficient in communication and applying the key management for security.
- Efficient in communication and saves energy
- Solve the orphan node problem in the secure data transmission with a symmetric key management.

6. SYSTEM ARCHITECTURE

System Architecture IBS



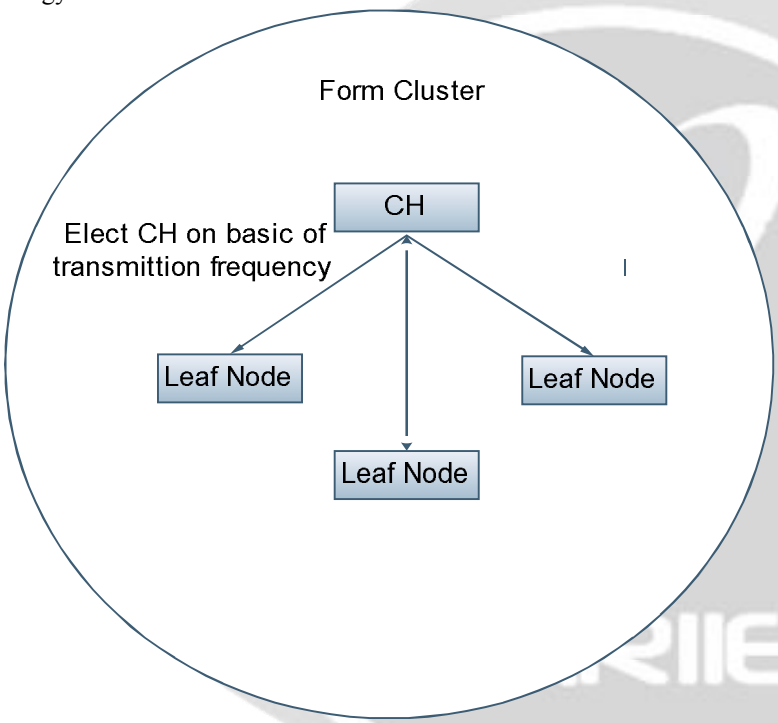
7.MODULES

- Cluster
- BASE STATION(trusted authority)

- SET-IBS
- SET-IBOOS
- Security Analysis

7.1CLUSTER

In this module we construct CWSN. In which sensor nodes are grouped into clusters, and each cluster has a cluster-head (CH) sensor node, which is elected autonomously. Leaf (non-CH) sensor nodes, join a cluster depending on the receiving signal strength and transmit the sensed data to the BS via CHs to save energy. The CHs perform data fusion, and transmit data to the BS directly with comparatively high energy. In addition, we assume that, all sensor nodes and the BS are time synchronized with symmetric radio channels, nodes are distributed randomly, and their energy is constrained



7.2 BASE STATION

In this module we fixed base station for cluster-base wireless sensor network. Base station responsibility to give authority (certificate and key) for every node in cluster.

7.3 SET-IBS

In this module we construct SET-IBS which expand as Identity-Based digital Signature (IBS) scheme in this module base station generates a master key and public parameter for private key generator and give that all to sensor node in cluster. Then sensor node generate private key use a private string after that send message along with timestamp and signature. Here signature is generated by signing key. In receiver side message accepted if verification of signature is valid otherwise reject.

7.4 SET-IBOOS

In this module we construct SET-IBOOS which expand as Identity-Based Online/Offline digital Signature (IBOOS) scheme in this module base station generates a master key and public parameter for private key generator and give that all sensor node in cluster. Then sensor node generate private key use a private string after that a cluster head use that sting id and time stamp cluster head generate offline signature send it to the leaf node. And then use the private of sensor node, offline signature and message every sensor node generate online signature .In receiver side cluster head accepted message if signature is online otherwise reject.

7.5 SECURITY ANALYSIS

Passive attack on wireless channel: Passive attackers are able to perform eavesdropping at any point of the network, or even the whole communication of the network. Thus, they can undertake traffic analysis or statistical analysis based on the monitored or eavesdropped messages.

Active attack on wireless channel: Active attackers have greater ability than passive adversaries, which can tamper with the wireless channels. Therefore, the attackers can forge, reply and modify messages. Especially in WSNs, various types of active attacks can be triggered by attackers, such as bogus and replayed routing information attack, sinkhole and wormhole attack, selective forwarding attack, HELLO flood attack, and Sybil attack [2, 21].

***Node compromising attack*:** Node compromising Attackers are the most powerful adversaries against the proposed protocols as we considered. The attackers can physically compromise sensor nodes, by which they can access the secret information stored in the compromised nodes, e.g., the security keys. The attackers also can change the inner state and behavior of the compromised sensor node, whose actions may be varied from the premier protocol specifications.

8.CONCLUSION:

In the evaluation section, provided feasibility of the proposed SET-IBS and SET-IBOOS with respect to the security requirements and analysis against routing attacks. SET-IBS and SET-IBOOS are efficient in communication and applying the ID-based crypto-system, which achieves security requirements in CWSNs, as well as solved the orphan node problem in the secure transmission protocols with the symmetric key management.

9.REFERENCES:

[1]. T. Hara, V. I. Zadorozhny, and E. Buchmann, *Wireless Sensor Network Technologies for the Info. Explosion Era*, *Stud. Comput. Intell.* Springer-Verlag, 2010, vol. 278.

[2]. Y.Wang, G. Attebury, and B. Ramamurthy, "A Survey of Security Issues in Wireless Sensor Networks," *IEEE Commun. Surveys Tuts.*, vol. 8, no. 2, 2006.

[3]. A. Abbasi and M. Younis, "A survey on clustering algorithms for wireless sensor networks," *Comput. Commun.*, vol. 30, no. 14-15, 2007.

[4]. W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "An application-specific protocol architecture for wireless microsensor networks," *IEEE Trans. Wireless Commun.*, vol. 1, no. 4, 2002.

[5]. Manjeshwar, Q.-A.Zeng, and D. P. Agrawal, "An analytical model for information retrieval in wireless sensor networks using enhanced APTEEN protocol," *IEEE Trans. Parallel Distrib. Syst.*, vol. 13, 2002.