IMPROVISATION OF PERFORMANCE IN CLUSTER NETWORKS

Dr. G. Charles Babu*, Mr. K. Rajeshwar Rao
* Dr. G. Charles Babu, Professor, CSE Dept, MREC (A), Secunderabad
Mr.K. Rajeshwar Rao, Asst. Professor, CSE Dept, MREC (A), Secunderabad

DOI: 10.5281/zenodo.61145

KEYWORDS: Identity-based digital signature, Wireless sensor network, Cluster, Data transmission, Identity-based cryptography.

ABSTRACT

Recently identity-based digital signature has been made available as a key management in wireless sensor networks for security. We study effective data transmission meant for cluster-basis sensor system, in our work in which clusters are created dynamically and intermittently. We aim to study the proposals regarding two Secure and Efficient data Transmission procedures for cluster-based wireless sensor networks known as secure and effective data transmission-Identity-based on digital signature and secure and effective data transmission-based on online/offline digital signature. Data transmission protocol based on Identity based online/offline digital signature is projected to further decrease computational overhead for security by means of secure and effective data transmission-based on online/offline digital signature in which security depends on hardness of discrete logarithmic complexity. Identity-based protocol of digital signature on basis of complexity of factoring integers from cryptography of identity-basis is to obtain an entity’s public key from its identity information. The important notion of proposed data transmission protocols is to authenticate encrypted sensed data, by means of application of digital signatures which are efficient in communication. Both of these schemes totally work out orphan-node problem from using symmetric key management for cluster-based wireless sensor system.

INTRODUCTION

Data transmissions based on cluster in wireless sensor networks were examined by researchers to attain management and scalability of network, which make the most of node duration and decrease bandwidth consumption by means of local collaboration between sensor nodes [1]. In cluster based wireless sensor networks sensor nodes are set into clusters, in which each cluster include a cluster head sensor node, which is selected independently. In a cluster-based wireless sensor networks every cluster enclose a leader sensor node, known as cluster head which aggregates data that is collected by leaf nodes in its cluster, and forward aggregation to base station. In cluster-based wireless sensor networks data sensing, processing, as well as transmission consume energy concerning sensor nodes. The expenditure of data transmission is extremely pricey than data processing hence system that the intermediate node aggregate data and send it to base station is preferred than technique that each sensor node openly sends data towards base station. We put forward two Secure and Efficient data Transmission procedures for cluster-based wireless sensor networks known as secure and effective data transmission-Identity-based on digital signature (SET-IBS) and secure and effective data transmission- based on online/offline digital signature (SET-IBOOS) [2][3]. These procedures make available protected data transmission meant for cluster-basis sensor system with concrete identity-based settings, which use identity information. The scheme of identity-based digital signature on basis of complexity of factoring integers from cryptography of identity-basis is to obtain an entity’s public key from its identity information. In the modern times, identity-based digital signature has been build up as key managing in wireless bandwidth consumption by means of local collaboration between sensor nodes [1]. In cluster based wireless sensor networks sensor nodes are set into clusters, in which each cluster include a cluster head sensor node, which is selected independently. Sensor networks for security. Identity-based online/offline digital signature scheme has been projected to decrease computation as well as storage costs of signature processing.

AN OVERVIEW OF PROPOSED SECURE DATA TRANSMISSION PROTOCOLS

MATERIALS AND METHODS

In literature, researchers have been extensively studied cluster-based wireless sensor networks in the past few years in literature. Operation of cluster-based architecture in real world is relatively complicated. The objective of projected secure data transmission meant for cluster-basis sensor system is to assurance and efficient data transmissions among leaf nodes and cluster heads, as well as transmission involving cluster heads and base station. For the most of traditional protocols of secure transmission for cluster-based wireless sensor networks in literature on the other hand, apply symmetric key management intended for security, which undergo from orphan node difficulty we solve orphan node setback by means of Identity based cryptosystem that assurance security requirements, and recommend secure and effective data transmission-Identity-based digital signature. Secure and efficient data transmission-Identity based on online/offline digital signature is projected to further decrease computational overhead for security by means of secure and effective data transmission-based on online/offline digital signature in which security depends on hardness of discrete logarithmic difficulty. In our work we learn secure data transmission meant for cluster-basis sensor system where clusters are created dynamically and intermittently. Secure and effective data transmission- identity based on online/offline digital signature necessitates less energy for computation and storage and is more appropriate for node-to-node communications within cluster basis sensor networks [4]. The key proposal of secure and effective data transmission-Identity-based on digital signature and secure and effective data transmission- based on online/offline digital signature is to authenticate encrypted sensed data, by means of application of digital signatures which are efficient in communication. In these proposed procedures, secret keys as well as pairing parameters are distributed and preloaded in the entire sensor nodes by base station initially, which overcome key escrow difficulty described in ID-based cryptosystems. Secure communication in secure and effective data transmission-Identity-based on digital signature relies on identity basis cryptography, in which, user public keys are their identity information consequently, and users can get hold of corresponding private keys devoid of auxiliary data. Both secure and effective data transmission-Identity-based on digital signature and secure and effective data transmission-identity based on online/offline digital signature solve orphan node difficulty in protected data transmission through symmetric key management.

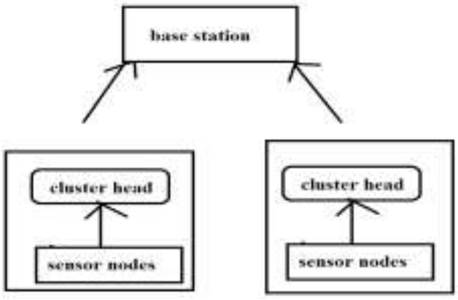

Figure 1: An overview of Cluster system.

CHARACTERISTICS OF PROPOSED PROTOCOL

Both the proposed SET-IBS and SET-IBOOS procedures make available protected data transmission meant for cluster-basis sensor system with concrete identity-based settings, which use identity information as well as digital signature for authentication. Consequently, both of these schemes completely work out orphan-node problem from using symmetric key management for cluster-based wireless sensor networks. When compared with SET-IBS, the procedure of SET-IBOOS necessitates less energy for computation and storage and is more appropriate for node-to-node communications within cluster basis sensor networks as computation is lighter to be performed [5]. In secure and effective data transmission- identity based on online/offline digital signature offline signature is executed by cluster head sensor nodes; consequently, sensor nodes do not have to implement offline algorithm before it wants to mark on a new message. Both secure and effective data transmission-Identity-based on digital signature and secure and identity based on online/offline digital signature solve orphan node difficulty in secure data transmission by means of symmetric key management. The projected SET-IBS include a protocol initialization earlier to the network consumption and operates in rounds throughout communication, which consists of a setup phase as well as a steady-state phase in each round [6]. By means of this scheme allows well-organized aggregation of encrypted data at the cluster heads and the base station, which moreover guarantees data privacy.

CONCLUSION

We introduce Secure and Efficient data Transmission procedures for cluster-based wireless sensor networks known as secure and effective data transmission-Identity-based on digital signature and secure and effective data transmission- based on online/offline digital signature. The objective of projected data transmission protocol in support of cluster-based wireless sensor networks is to assurance and efficient data transmissions among leaf nodes and cluster heads, as well as transmission involving cluster heads and base station. For conventional protocols of secure transmission for cluster-based wireless sensor networks in literature on the other hand, apply symmetric key management intended for security, which undergo from orphan node difficulty. We solve orphan node problem by means of IDbased cryptosystem that assurance security requirements, and recommend secure and effective data transmission-Identity-based digital signature. The protocol based on online/offline digital signature system has been projected to decrease computation as well as storage costs of signature processing. Both secure data transmission protocols solve orphan node difficulty in protected data transmission through symmetric key management.

REFERENCES

1. 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.
2. L.B. Oliveira et al., “SecLEACH-On the Security of Clustered Sensor Networks,” Signal Processing, vol. 87, pp. 2882-2895, 2007.
3. 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.
4. 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.
5. L.B. Oliveira et al., “SecLEACH-On the Security of Clustered Sensor Networks,” Signal Processing, vol. 87, pp. 2882-2895, 2007.
6. 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.