Transmission of Data for Cluster based Wireless Sensor Networks in More Secure and Efficient Manner

Madhushree R[1], Megha K Bhairanatti[2,] Saravana Perumal[3]
[1,2]UG Student, department of computer science, rajarajeswari college of engineering India
[3]Assistant professor, department of computer science, rajarajeswari college of engineering India

***Abstract*— Secure data transmission is a critical issue for wireless sensor networks (WSNs). So we use Clustering to enhance WSN's performance. Here, we study a secure data transmission for cluster-based WSNs (CWSNs), pairing domain. where the clusters are formed dynamically and frequently. We use two efficient and secure data transmission (SET) protocols for CWSNs, Hashing algorithm for signature, RSA for generating the keys and Homomorphism for encryption and decryption. We show the better performance using these protocols and algorithm.**

Keywords-WSN, Clusters,homomorphism, hash algorithm

I . INTRODUCTION

A WIRELESS sensor network (WSN) is a network consisting of various devices that are distributed spatially using wireless sensor nodes in order to monitor physical or environmental conditions. Each node is capable of sensing their environments and process the information and send data to one or more nodes in the network .

Transmitting the data efficiently is one of the most critical issues for WSNs. Since many WSNs are established in harsh, neglected, and often in different physical environments for certain applications, such as military environment and tasks such as sensing with trustless surroundings. Secure and efficient data transmission (SET) is, thus, especially necessary and is demanded in many such practical WSNs.

II. RELATED WORKS

In this Existing System of wireless sensor network comprised of spatially distributed devices using wireless sensor nodes to monitor physical or environmental conditions, such as sound, temperature, and motion. The individual nodes are capable of sensing their environments, processing the information data locally, and sending data to one or more collection points in a WSN.

Efficient data transmission is one of the most important issues for WSNs. Meanwhile, many WSNs are deployed in harsh, neglected and often adversarial physical environments for certain applications, such as military domains and sensing tasks with trustless surroundings

The LEACH (Low-Energy Adaptive Clustering Hierarchy) protocol is a widely known and effective one to reduce and balance the total energy consumption for CWSNs. In order to prevent quick energy consumption of the set of CHs, LEACH randomly rotates CHs among all sensor nodes in the network, in rounds. LEACH achieves improvements in terms of network lifetime.

Following LEACH, a number of protocols have been presented such as APTEEN and PEACH

Digital signature is one of the most critical security services offered by cryptography in asymmetric key management systems, where the binding between the public key and the identification of the signer is obtained via a digital certificate.

The Identity-Based digital Signature (IBS) scheme, based on the difficulty of factoring integers from Identity- Based Cryptography (IBC), is to derive an entity's public key from its identity information, e.g., from its name or ID number

Disadvantage

Adding security to LEACH-like protocols is challenging, because they dynamically, randomly and periodically rearrange the network's clusters and data links.

Node-to-node trust relationships and common key distributions are inadequate for LEACH-like protocols

Apply the symmetric key management for security, which suffers from a so-called orphan node problem. 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, the key ring in a node is not sufficient for it to share pair wise symmetric keys with all of the nodes in a network. In such a case, it cannot participate in any cluster, and therefore, has to elect itself as a CH. Furthermore, the orphan node problem reduces the possibility of a node joining with a CH, when the number of alive nodes owning pair wise keys decreases after a long term operation of the network

PROPOSED SYSTEM

In this Proposed System, Secure and Efficient data transmission is thus especially necessary and is demanded in many such practical WSNs. So, we 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.

It has been proposed in order to reduce the computation and storage costs to authenticate the encrypted sensed data, by applying digital signatures to message packets, which are efficient in communication and applying the key management for security.

In the proposed protocols pairing parameters are distributed and preloaded in all sensor nodes by the BS initially.

Secure and Efficient data Transmission (SET) protocols for CWSNs is proposed, 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, which are efficient in communication and applying the key management for security.

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-basedcrypto-systems.

Advantages

Less computation and communication

High security

III. DESIGN

A . Network Architecture

Consider a CWSN consisting of a fixed BS and a large number of wireless sensor nodes, which are homogeneous in functionalities and capabilities. We assume that the BS is always reliable, i.e., the BS is a trusted authority (TA). Meanwhile, the sensor nodes may be compromised by attackers, and the data transmission may be interrupted from attacks on wireless channel. In a CWSN, sensor nodes are grouped into clusters, and each cluster has a 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.

In CWSNs, data sensing, processing, and transmission consume energy of sensor nodes. The cost of data transmission is much more expensive than that of data processing. Thus, the method that the intermediate node (e.g., a CH) aggregates data and sends it to the BS is preferred than the method that each sensor node directly sends data to the BS [1], [3]. A sensor node switches into sleep mode for energy saving when it does not sense or transmit data, depending on the time-division multiple access (TDMA) control used for data transmission. In this paper, the proposed SET-IBS and SET-IBOOS are both designed for the same scenarios of CWSNs above.

B . Contributions and Organization

we have applied and evaluated the key management of IBS to routing in CWSNs [17]. In this paper, we extend our previous work and focus on providing an efficient secure data communication for CWSNs. The contributions of this work are as follows:

We propose two Secure and Efficient data Transmission protocols for CWSNs, called SET-IBS and SET-IBOOS, 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, which are efficient in communication and applying the key management for security. In 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 cryptosystems [22].

Secure communication in SET-IBS relies on the ID based cryptography, in which, user public keys are their ID information. Thus, users can obtain the corresponding private keys without auxiliary data transmission, which is efficient in communication and saves energy.

SET-IBOOS is proposed to further reduce the computational overhead for security using the IBOOS scheme, in which security relies on the hardness of the discrete logarithmic problem. Both SET-IBS and SET-IBOOS solve the orphan node problem in the secure data transmission with a symmetric key management.

We show the feasibility of the proposed protocols with respect to the security requirements and analysis against three attack models. Moreover, we compare the proposed protocols with the existing secure protocols for efficiency by calculations and simulations, respectively, with respect to both computation and communication.

IV. CONCLUSION

In this paper, we first reviewed the data transmission issues and the security issues in CWSNs. The deficiency of the symmetric key management for secure data transmission has been discussed. We then presented two secure and efficient data transmission protocols, respectively, for CWSNs, SET-IBS, and SET-IBOOS. In the evaluation section, we provided feasibility of the proposed SET-IBS and SET-IBOOS with respect to the security requirements and analysis against routing attacks. SET-IBS and SETIBOOS are efficient in communication and applying the IDbased cryptosystem, which achieves security requirements in CWSNs, as well as solved the orphan node problem in the secure transmission protocols with the symmetric key management. Lastly, the comparison in the calculation and simulation results show that the proposed SET-IBS and SET-IBOOS protocols have better performance than existing secure protocols for CWSNs. With respect to both computation and communication costs, we pointed out the merits that using SET-IBOOS with less auxiliary security overhead is preferred for secure data transmission in CWSNs.

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] Y. Wang, G. Attebury, and B. Ramamurthy, "A Survey of Security Issues in Wireless Sensor Networks," IEEE Comm. Surveys & Tutorials, vol. 8, no. 2, pp. 2-23, Second Quarter 2006

[3] 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

[4] 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.

[5] A. 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 & Distributed Systems, vol. 13, no. 12, pp. 1290-1302, Dec. 2002.

[6] 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.

[7] 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.

[8] L.B. Oliveira et al., "SecLEACH-On the Security of Clustered Sensor Networks," Signal Processing, vol. 87, pp. 2882-2895, 2007.

[9] 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.

[10] K. Zhang, C. Wang, and C. Wang, "A Secure Routing Protocol for Cluster-Based Wireless Sensor Networks Using Group Key Management," Proc. Fourth Int'l Conf. Wireless Comm., Networking and Mobile Computing (WiCOM), pp. 1-5, 2008.