ISSN: 2321-7782 (Online)
Impact Factor: 6.047

Volume 4, Issue 5, May 2016

International Journal of Advance Research in Computer Science and Management Studies

Research Article / Survey Paper / Case Study

Available online at: www.ijarcsms.com

Implementation of Cluster based Wireless Sensor Network for Secure and Efficient Data Transmission

Namratha H T[1]
PG Student, dept. of CS&E
P.E.S College of Engineering
Mandya – India

Dr. Minavathi[2]
Professor and Head, dept. of IS&E
P.E.S College of Engineering
Mandya – India

Abstract: ***In the past few years secure data transmission along with efficiency is a critical issues for wireless sensor networks (WSNs).Clustering is a technique which increases network life time and reduces power consumption of sensor nodes in WSNs. We propose two protocols for authentication of data which are secure and efficient data transmission protocols namely SET-IBS and SET-IBOOS .These two make use of asymmetric key management .These protocols rely on identity based digital signature[IBS] scheme and identity based online and offline digital signature schema [IBOOS] scheme. SET-IBOOS further minimizes computational overhead.***

Keywords: wireless sensor network, LEACH, Identity based digital signature [IBS] schema, Identity based online and offline digital signature [IBOOS] schema.

I. INTRODUCTION

Wireless sensor network (WSN) is a network that consists of several sensor nodes that are randomly distributed on a geographical area. These sensor nodes are used to monitor the physical and environmental conditions like temperature, pressure, humidity etc. Cluster based Wireless Sensor Network is used to reduce the network consumption and also the increase in energy efficiency. Clustering in WSN is done to minimise the energy consumption and also to reduce the data transmission over the network required to transmit the message to the BS, as the CH becomes responsible for communication, which results into prolonged network lifetime.

WSN are used in many applications like health care monitoring, industrial monitoring, military applications, environmental and earth sensing. Due to wireless nature of sensor networks security is a critical issue in WSN.Most of the present protocols used for secure transmission of data undergo the orphan node problem. We intend to solve this orphan node problem in this paper by means of the crypto-system based on ID that gives the warranty of security requirements, and use SET-IBS by using the Identity-Based digital Signature scheme. Besides, SET-IBOOS is also used to decrease the computational operating cost in SET-IBS with the IBOOS method.

II. BACKGROUND AND MOTIVATION

The LEACH (Low Energy Adaptive Clustering Hierarchy) protocol is a widely known hierarchical protocol. It is very effectively used to reduce and balance the total energy consumption for CWSNs. LEACH achieves improvements in terms of network lifetime. Adding security to LEACH-like protocols is challenging because they dynamically, randomly, and periodically rearrange the network's clusters and data links .Therefore, 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). Nowadays asymmetric management has been found feasible for WSNs in comparison to symmetric management for security. The probability of the asymmetric key management has been revealed in WSNs in recent times, which compensates the deficiency from relating the symmetric key management for security. Digital signature is

one of the most significant security services presented by cryptography in asymmetric key management systems, where the binding between the public key and the recognition of the signer is acquired via a digital certificate. The Identity-Based digital Signature (IBS) scheme, based on the complexity of factoring integers from Identity- Based Cryptography (IBC), is to develop an entity's public key from its character information, e.g., from its identification number.

III. Related Work

A secure routing for cluster-based sensor networks is where clusters are formed periodically and dynamically. Together with the investigation of ID-based cryptography for security in WSNs, Huang Lu *et.al* proposed a new secure routing protocol with ID-based signature scheme for cluster-based WSNs within which the security is dependent on the hardness of the Diffie-Hellman problem in the random oracle model. Here the deficiency in the secure routing protocols with symmetric key pairing is pointed out by authors.

Key management methods, except many of them were planned for flat wireless sensor networks, which are not suitable for cluster-based wireless sensor networks (like LEACH). Here Kun Zhang et.al investigated adding security to cluster based routing protocols for wireless sensor networks which consist of sensor nodes with very inadequate resources, and have proposed a security solution for LEACH which is a protocol in which the clusters are created periodically and dynamically. The solution proposed by authors makes use of enhanced Random Pair-wise Keys (RPK) method, an optimized security method that depends on symmetric key methods and is a lightweight and conserves the heart of the original LEACH protocol. Simulations demonstrate that security of RLEACH has been enhanced, with reduction in energy utilization and very less operating cost.

HichemSedjelmaci*et.al* proposed an intrusion detection framework for a cluster-based WSN (CWSN) that intend to merge the advantage of anomaly and signature detection which are high discovery rate and low false positive ,correspondingly. Wireless sensor networks (WSNs) have a enormous potential to be used in vital circumstances like armed forces and commercial applications. On the other hand, these applications are mostly frequently to be deployed in hostile surroundings, where nodes and communication are smart targets to intruders. This makes WSNs susceptible to a range of possible attacks. Because of their characteristics, conservative security methods are not appropriate. So here the authors have proposed an intrusion detection framework for a cluster-based WSN (CWSN) that aims to merge the advantage of signature detection and anomaly which are high detection rate and low false positive.

Tingyao Jiang *et.al* presented a new dynamic intrusion detection method for cluster-based wireless sensor networks (CWSN). The nodes in a wireless sensor network are assembled into clusters depending on the particular relationships with a cluster head (CH) in every cluster. The projected scheme initially makes use of a clustering algorithm to construct a model of standard traffic behavior, and then uses this model of standard traffic to detect anomalous traffic patterns. Along with the diverse network conditions of clusters, this method might also dynamically set different detection factors for different clusters to accomplish a more proper detection algorithm. The performance study showed that the projected intrusion detection method can progress the detection accuracy and decrease the false positive rate, and is extremely efficient of the energy preservation.

IV. System Objectives

The goal of the proposed secure data transmission for CWSNs is to guarantee a secure and efficient data transmission between leaf nodes and CHs, as well as transmission between CHs and the BS. Meanwhile, most of existing secure transmission protocols for CWSNs in the literature, however, applies the symmetric key management for security, which suffers from the orphan node problem. In this paper, we aim to solve this orphan node problem by using the ID-based crypto-system that guarantees security requirements, and propose SET-IBS by using the IBS scheme. Furthermore, SET-IBOOS is proposed to reduce the computational overhead by using IBOOS scheme.

V. System Architecture

This system has base station and set of clusters as shown in fig.1.The purpose of the base station is to provide common key parameters to all the nodes in the system. Every node in the system can form their encryption key by following notations Node ID + Common Parameter For each transaction base station creates new common parameter, so that for every transaction new key is generated.

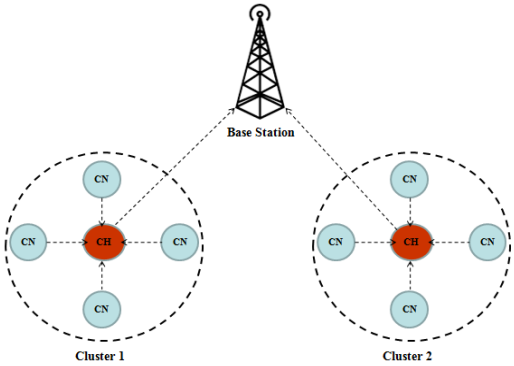

Fig.1 system architecture

VI. Proposed Schemas and Protocols

A. *IBS schema*

IBS is based on IBS scheme. It has four phases like setup at the BS, key extraction, signature signing and verification.

1. Setup at the BS: The BS generates master key and public parameters and broadcast these to all sensor nodes in the network.

2. Key extraction: Sensor nodes generates private key by using ID of the node and master key transmitted by the base station.

3. Signing of signature: Signature is created by using a, signing key and message

4. Verification of the data receiving nodes: Verification is done at the receiving end by using the digital signature, ID of the node and message. The receiving node accepts the message if sign is legal, otherwise rejects the message.

B. *Workflow of IBS protocol*

SET-IBS is based on ID-based cryptography in which identification of the node is used as their public key and private key can be generated without auxiliary data transmission. It creates digital signature and attach this digital signature to the sensed encrypted data. This process is done at the sending node. At receiver, node uses public key to decrypt the transmitted message. Then node test the validity of the digital signature of received message. If the digital signature is valid it accepts the message and transmits to base station (BS). If the digital signature is invalid, it shows that the transmitted message is altered or modified. Then it rejects that message.

C. *IBOOS Schema*

An IBOOS scheme has five phases. IBOOS scheme is similar to IBS scheme. In IBOOS scheme signature is generated in two phases. Those are online signature and offline signature. The IBOOS scheme has five phases those are:

1. Setup at the BS: The BS generates master key and public parameters similar to IBS scheme.

2. Key extraction: Sensor nodes generates private key by using ID of the node and master key transmitted by the base station.

3. Offline signing: Offline signing (offline sign) is done at the receiver node by using given parameters .The cluster head transmit offline sign to leaf node.

4. Online signing: Online signature (online sign) is generated at sending node by using private key, offline sign and message.

5. Verification: Verification is done at the receiver end by using the digital signature, ID of the node and message.

The receiving node accepts the message if sign is legal, otherwise rejects the message.

D. Workflow of SET-IBOOS Protocol

SET-IBOOS is proposed to minimize the computational overhead and to improve the performance of the network. Working of IBOOS is similar to IBS protocol. In IBOOS protocol to reduce computational overhead, signature signing is divided into two phases. i.e. online and offline. Offline signing is done at the receiver before message has been known. Advantage offline sign is it can be performed easily. By using this offline sign online signature is generated at sender node. Online sign is computed after message is known. This process is much faster than the IBS protocol.

VII. CONCLUSION

The Protocols like LEACH which are cluster based data transmission protocols suffer from variety of security threats. Adding security to such protocols is little bit tricky since they arbitrarily, occasionally and vigorously rearrange the network's clusters and data links there by threatening the security and vulnerability of the CWSNs. To overcome the drawback of orphan node problem which is experienced by LEACH, we intend to use the two methods of Identity Based Digital Signature namely the SET-IBS and SET-IBOOS, thus providing efficiency as well as security in the transmission of data among nodes in CWSNs. We intend to increase the efficiency with respect to both communication and computation cost.

ACKNOWLEDGEMENT

It's my immense pleasure to express my indebtedness to my guide Dr.Minavathi, professor and head, department of Information Science & Engineering, who guided me at various stages and I also thank the principal and management P.E.S. College of Engineering, Mandya.

References

1. Wu Xinhua and Huang Li"Research and Improvement of the LEACH Protocol to Reduce the Marginalization of Cluster Head" Journal of Wuhan University of Technology Vol. 35, No. 1, Feb. 2011, pp. 79-82.
2. Tao, L, Zhu, QX, Zhang, L. An Improvement for LEACH Algorithm in Wireless Sensor Network.Proc.5th IEEE Conf. Indust .Electr. Appl. 2010.
3. Heinzelman W. B., Chandrakasan A. P., Balakrishnan H., "An application specific protocol architecture for wireless micro sensor networks," IEEE Trans on Wireless Communications, Vol. 1, No. 4, 2002, pp. 660-670.
4. Tingyao Jiang, Gangliang Wang, Heng Yu, "A dynamic intrusion detection scheme for cluster-based wireless sensor networks", World Automation Congress (WAC), Page(s): 259- 261, Publication Year: 2012.
5. Yasmin, R., Ritter, E.;" An Authentication Framework for Wireless Sensor Networks using Identity-Based Signatures", Guilin Wang Computer and Information Technology (CIT), 2010 IEEE 10th International Conference, Page(s): 882- 889, PublicationYear: 2010.
6. Nguyen Xuan Quy, Mingi Kyun, Dugki Min, "Security-enhanced energy-efficient data aggregation for cluster-based wireless sensor networks", Internet, 2008. ICI 2008. 4th IEEE/IFIP International Conference, Page(s): 1- 5, Publication Year: 2008.

