ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology
Vol. 2, Issue 6, June 2015

Achieving Security and Efficient Data Transformation for Cluster Based Wireless Sensor Networks

Phanindra Kumar Reddy.P[1], Sreenivasulu.T[2]

Assistant Professor, C.S.E, A.I.T.S, Rajampet[1]

M.Tech student, C.S.E, A.I.T.S, Rajampet[2]

Abstract: Wireless Sensor Networks (WSN) plays vital role in research field. Secure transmission of data along with efficiency is a critical issue for wireless sensor networks (WSNs). Clustering is an efficient and practical way to enhance the system performance of WSNs. In this project work, we study a secure transmission of data for cluster-based WSNs (CWSNs), where the clusters are formed dynamically and sporadically. We propose two Secure and Efficient data Transmission (SET) protocols for CWSNs, called SET-IBS and SET-IBOOs, by means of the Identity-Based digital Signature (IBS) scheme and the Identity-Based Online/Offline digital Signature (IBOOS) scheme. In SET-IBS, security relies on the hardness of the Diffie-Hellman problem in the pairing area. SET-IBOOS further reduces the computational overhead for protocol security, which is important for WSNs, though its security relies on the hardness of the discrete logarithm problem.

Keywords: CWSN, SET-IBS, SET-IBOOS.

1. INTRODUCTION

A wireless sensor network (WSN) generally consists of a gateway that can communicate with a number of wireless sensors via a radio link. Data is composed at the wireless sensor node, packed together, and transmit to the gateway directly or, if required, it uses other nodes to forward data to the gateway. The transmitted data is then transformed to the system. The function of this section is to provide a brief technical introduction to wireless sensor networks and present a few applications in which wireless sensor networks are enabling. A WSN usually consists of tens to thousands of such nodes that communicate through wireless channels for information sharing and mutual processing. WSNs can be deployed on a large-scale for environmental monitoring and environment study, over a battle-field for military surveillance and reconnaissance, in emergent environments for search and rescue, in factories for condition based maintenance, in buildings for infrastructure health monitoring, in homes to realize smart homes, or even in bodies for patient monitoring. After the initial deployment (typically ad hoc), sensor nodes are responsible for self-organizing an appropriate network infrastructure, often with multi-hop Connection between sensor nodes. Efficient transmission of data is one of the most significant issues for WSNs. Cluster-based transmissions of data in WSNs, has been examined by researchers in order to accomplish the network scalability and supervision, which maximizes node life span and reduces bandwidth utilization by using local cooperation between sensor nodes. In a cluster-based WSN (CWSN), each cluster has a leader sensor node, known as cluster-head (CH). A CH collects the data gathered by the leaf nodes (non- CH sensor nodes) in its cluster, and sends the pooled data to the base station (BS). 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 or its name.

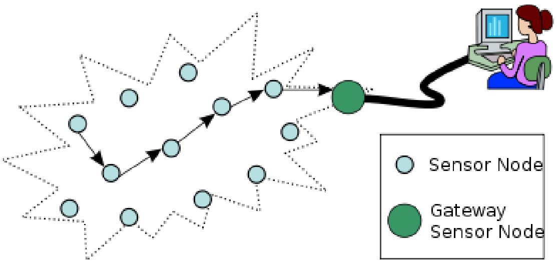

Fig : Architecture of WSN

2. BACKGROUND AND MOTIVATIONS

Cluster-based data transmission in WSNs, has been investigated by researchers in order to achieve the network scalability and management, which maximizes node lifetime and reduce bandwidth consumption by using local collaboration among sensor nodes. The LEACH (Low-Energy Adaptive Clustering Hierarchy) protocol presented by Heinzelman is a widely known and effective one to reduce and balance the total energy consumption for CWSNs. LEACH randomly rotates CHs among all sensor nodes in the network, in rounds. LEACH achieves improvements in terms of network lifetime. Following the idea of LEACH, a number of protocols have been presented such as APTEEN and PEACH, which use similar concepts of LEACH. Adding security to LEACH-like protocols is challenging, because they dynamically, randomly and periodically re-arrange the network's

DOI 10.17148/IARJSET.2015.2630

clusters and data links. There are some secure data transmission protocols based on LEACH-like protocols, such as SecLEACH, GS-LEACH and RLEACH. In WSNs recently, which compensates the shortage from applying the symmetric key management for security. Digital signature is one of the most critical security ser-vices 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. IBS has been developed asa key management in WSNs for security. Carman first combined the benefits of IBS and key pre-distribution set into WSNs. The IBOOS scheme has been proposed in order to reduce the computation and storage costs of signature processing.

3. NETWORK ARCHITECTURE

In a cluster-based WSN (CWSN), each cluster has a leader sensor node, known as cluster-head (CH). A CH collects the data gathered by the leaf nodes (non- CH sensor nodes) in its cluster, and sends the pooled data to the base station (BS).

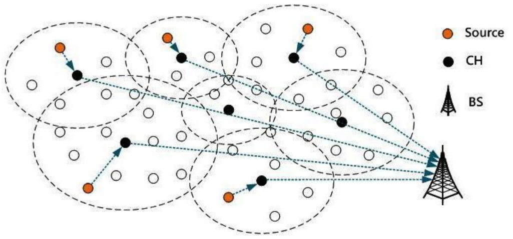

Fig: Cluster Based Wireless Sensor Network

In CWSNs, data sensing, processing and transmission consume energy of sensor nodes. The cost of data transmission is much more expensive than data processing.

4. IBS AND IBOOS For CWSNs

In this section, we introduced the IBS Scheme and IBOOS scheme used in this paper.

a. IBS Scheme for CWSNs

An IBS scheme implemented for CWSNs consists of the following operations, specifically, setup at the BS, key ex-traction and signature signing at the data sending nodes, and verification at the data receiving nodes.

Setup: The BS (as a trust authority) generates a master key msk and public parameters param for the private key generator (PKG), and gives them to all sensor nodes.

Extraction: Given an ID string, a sensor node generates a private key sekID associated with the ID using msk.

Signature signing: Given a message M, time-stamp t and a signing key θ, the sending node generates a signature SIG.

Verification: Given the ID, M and SIG, the receiving node outputs "accept" if SIG is valid, and outputs "reject" otherwise.

b. IBOOS Scheme for CWSNs

An IBOOS scheme implemented for CWSNs consists of following four operations, specifically, setup at the BS, key extraction and offline signing at the CHs, online signing at the data sending nodes, and verification at the receiving nodes.

Setup: Same as that in the IBS scheme.

Extraction: Same as that in the IBS scheme.

Offline signing: Given public parameters and time-stamp **t**, the CH sensor node generates an offline signature SIG offline and transmit it to the leaf nodes in its cluster.

Online signing: From the private key sekID, SIG offline and message M, a sending node (leaf node) generates an online signature SIGonline.

Verification: Given ID, M and SIG online, the receiving node (CH node) outputs "accept" if SIGonline is valid, and outputs "rejects" otherwise.

5. SECURITY ANALYSIS

In order to evaluate the security of the proposed protocols, we have to investigate the attack models in WSNs which threaten the proposed protocols, and the cases when an adversary (attacker) exists in the network. Afterwards, we detail the solutions and countermeasures of the proposed protocols, against various adversaries and attacks.

5.1.1 Attack Models

In this paper, we group attack models into three categories according to their attacking means as follows, and study how these attacks may be applied to affect the proposed protocols.

- ***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.

- ***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 thesecret information stored in the compromised nodes, e.g., the security keys.

The attackers also can change the inner state and behaviour of the compromised sensor node, whose actions may be varied from the premier protocol specifications.

DOI 10.17148/IARJSET.2015.2630

5.1.2 Solutions to Attacks and Adversaries

The proposed SET-IBS and SET-IBOOS provide different types of security services to the communication for CWSNs, in both setup phase and steady-state phase. Both in SET-IBS and SET-IBOOS, the encryption of the message provides confidentiality, the hash function provides integrity, the nonce and time-stamps provide freshness, and the digital signature provides authenticity and non-repudiation.

• *Solutions to passive attacks on wireless channel*:
In the proposed SET-IBS and SET-IBOOS, the sensed data is encrypted by the homo morphic encryption scheme from, which deals with eavesdropping. Thus, the passive adversaries cannot decrypt the eavesdropped message without the decryption key. Furthermore, both SET-IBS and SET-IBOOS use the key management of concrete ID-based encryption. The ID-based key management in the proposed protocols is IND-ID-CCA secure (semantic secure against an adaptive ID-based chosen cipher text attack) and IND-ID-CPA secure (semantic secure against an adaptive ID-based chosen plaintext attack). As a result, properties of the proposed secure data transmission for CWSNs settle the countermeasures to passive attacks.

• *Solutions to active attacks on wireless channel*:
Focusing on the resilience against certain attacks to CWSNs mentioned in attack models, SET-IBS and SET IBOOS work well against active attacks. Most kinds of attacks are pointed to CHs of acting as intermediary nodes, because of the limited functions by the leaf nodes in a cluster-based architecture. Since attackers do not have valid digital signature to concatenate with broadcast messages for authentication, attackers cannot pretend as the BS or CHs to trigger attacks. Therefore, SETIBS and SET-IBOOS are resilient, and robust to the sinkhole and selective forwarding attacks, because the CHs being attacked are capable to ignore all the communication packets with bogus node IDs or bogus digital signatures. Together with round-rotating mechanism and digital signature schemes, SETIBS and SET-IBOOS are resilient to the hello flood attacks involving CHs.

• *Solutions to node compromising attacks*:
In case of attacks from a node compromising attacker, the compromised sensor node cannot be trusted anymore to fulfil the security requirements by key managements. In the case that the node has been compromised but works normally, the WSN system needs an intrusion detection mechanism to detect the compromised node and has to replace the compromised node manually or abandon using it. In this part, we investigate the influence of the remaining sensor nodes, and evaluate the properties only to that part of the network.

For increasing the Security the algorithms used are:
The identity based digital signature is transformed with the hash function. Hashing is the transformation of a string of characters into a usually shorter fixed-length value or key that represents the original string. Hashing is used to index and retrieve items in a database because it is faster to find the item using the shorter hashed key than to find it using the original value. It is also used in many encryption algorithms.

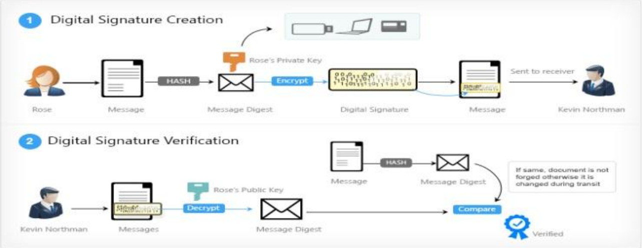

Fig: Digital Signature Creation

Hashing is also used to encrypt and decrypt digital signatures (to authenticate message senders and receivers). The digital signature is transformed with the hash function and then both the hashed value (known as a message-digest) and the signature are sent in separate transmissions to the receiver. Using the same hash function as the sender, the receiver derives a message-digest from the signature and compares it with the message-digest it also received. (They should be the same.) There are several reasons to sign such a hash (or message digest) instead of the whole document.

For efficiency: The signature will be much shorter and thus save time since hashing is generally much faster than signing in practice.

Data aggregation:
Data aggregation in WSN is one of the techniques to effectively utilize the limited resources. Generally it involves the following steps:

(i) Selection of cluster head
(ii) Formation of the cluster group
(iii) Data transfer.

The main objective of the data aggregation process is to increase the network lifetime by reducing the resource consumption of sensor node. But when network lifetime increases, there is a chance of degradation in the other performance of the network like data accuracy, latency, security and Fault tolerance. There are some protocols which can perform the data aggregation and routing simultaneously. These are classified as Tree based data aggregation protocols and Cluster based data aggregation protocols.

Source authentication:
Since wireless sensor networks use a shared wireless medium, sensor nodes need authentication mechanisms to detect maliciously injected or spoofed packets. Source authentication enables a sensor node to ensure the identity of the peer node it is communicating with. Without source authentication, an adversary could masquerade a node, thus gaining unauthorized access to resource and sensitive information and interfering with the operation of other nodes. Moreover, a compromised node may send data to its data aggregator under several fake identities so that the integrity of the aggregated data is corrupted. Faking multiple sensor node identities is called Sybil attack and it poses significant threat to data aggregation protocols. If only two nodes are communicating, authentication can be provided by symmetric key cryptography. The sender and

DOI 10.17148/IARJSET.2015.2630

the receiver share a secret key to compute the message authentication code (MAC) for all transmitted data.

6.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 thereby 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.

REFERENCES

[1] S. Sharma and S. K. Jena, "A survey on secure hierarchical routing protocols in wireless sensor networks," in Proc. ICCCS, 2011.

[2] Heinzelman W. B., Chandrakasan A. P., Balakrishnan H., "An applicationspecific protocol architecture for wireless microsensor networks," IEEE Trans on Wireless Communications, Vol. 1, No. 4, 2002, pp. 660-670, doi: 10.1109/TWC.2002.804190.

[3] X. H. Wu, S. Wang, "Performance comparison of LEACH and LEACHC protocols by NS2," Proceedings of 9th International Symposium on Distributed Computing and Applications to Business, Engineering and Science. Hong Kong, China, pp. 254-258, 2010

[4] P.T.V.Bhuvaneswari and V.Vaidehi "Enhancement techniques incorporated in LEACH- a survey"Department of Electronics Engineering, Madras Institute Technology, Anna University Chennai, India, 2009

[5] 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, doi:10.3963/j.issn.1006-2823.2011.01.019 (in Chinese).

[6] Tao, L, Zhu, QX, Zhang, L. An Improvement for LEACH Algorithm in Wireless Sensor Network.Proc.5th IEEE Conf. Indust.Electr. Appl. 2010;1:1811-4.

[7] S.K. Singh, M.P. Singh, and D.K. Singh, "A survey of Energy-Efficient Hierarchical Cluster-based Routing in Wireless Sensor Networks", International Journal of Advanced Networking and Application (IJANA), Sept.-Oct. 2010, vol. 02, issue 02, pp. 570-580.

[8] Thiemo Voigt, Hartmut Ritter, Jochen Schiller, Adam Dunkels, and Juan Alonso, ". Solar-aware Clustering in Wireless Sensor Networks", In Proceedings of the Ninth IEEE Symposium on Computers and Communications, June 2004.

BIOGRAPHIES

PHANINDRA KUMAR REDDY.P, Assistant Professor in Dept. Of Computer Science and Engineering at Annamacharya Institute of Technology, Rajampet.

SREENIVASULU. T, has received B.Tech Degree in Computer Science and Engineering From A.B.I.T, JNTU Anantapur University. And now pursuing M.Tech in Computer Science and Engineering From Annamacharya Institute of Technology, Rajampet.

DOI 10.17148/IARJSET.2015.2630