ISSN 2348 – 9928
IJAICT Volume 3, Issue 8, August 2016 Doi:01.0401/ijaict.2014.06.13 Published on 05 (8) 2016

IDENTITY BASED DIGITAL SIGNATURE SCHEME IN CLUSTER BASED WIRELESS SENSOR NETWORKS FOR SECURE AND EFFICIENT DATA TRANSMISSION – A SURVEY

Mr. S. Muthusamy
PG Scholar,
Information Technology,
Bannari Amman Institute of Technology,
Sathyamangalam, Tamilnadu, India

Dr. C. Poongodi
Associate Professor,
Information Technology,
Bannari Amman Institute of Technology,
Sathyamangalam, Tamilnadu, India

Dr. D. Deepa
Associate Professor,
Information Technology,
Bannari Amman Institute of Technology,
Sathyamangalam, Tamilnadu, India

Abstract— In wireless sensor networks (WSNs), secure data transmission is a critical problem. System performance should be increased by Clustering technique. This survey introduces two secure and efficient data transmission (SET) protocols for CWSNs, called SET-IBS and SET-IBOOS. The SET-IBS scheme using the identity-based digital signature (IBS) scheme and SET-IBOOS scheme using the identity-based online/ offline digital signature (IBOOS) scheme, respectively. In SET-IBS scheme security based on the difficulties of the Diffie-Hellman problem in the pairing domain. SET-IBOOS additionally reduces the computational overhead for protocol security, which is critical for WSNs. In SET-IBOOS security relies on the hardness of the discrete logarithm problem. The survey show that the SET-IBS SET-IBOOS protocols have better performance than the existing LEACH ,LEACH LIKE PROTOCOLS for CWSNs, 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.

I. INTRODUCTION

1.1 Wireless Sensor Network

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 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.

1.2 Cluster Based Wireless Sensor Network

Clustering protocols are often used in sensor networks. In a cluster-based WSN (CWSN), every cluster has a leader sensor node, regarded as cluster head (CH). A CH aggregates the data collected by the leaf nodes (non-CH sensor nodes) in its cluster, and sends the aggregation to the base station (BS).

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. 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.

1.3 The Goal of this Project is to

- Create the secure and efficient data transmission for cluster-based WSNs (CWSNs), where the clusters are formed dynamically and periodically.
- The SET-IBS and SET-IBOOS protocols need to consume energy faster than LEACH protocol because of the communication and computational overhead for security of either IBS or IBOOS process.

- The SET-IBOOS need to achieve a better balance of energy consumption than that of SecLEACH protocol.
- Need to Implement the SET-IBS and SET-IBOOS protocols with respect to the security requirements.
- SET-IBS and SET-IBOOS protocols need to provide
  - Solutions to passive attacks on wireless channel
  - Solutions to active attacks on wireless channel.
  - Solutions to node compromising attacks

II. LITERATURE SURVEY

In 2002 W.Heinemann, A.Chandrakasan, and H.Balakrishnan. [1] Worked on " An Application-Specific Protocol Architecture for Wireless Micro sensor Networks," .In a cluster-based WSN (CWSN), every cluster has a leader sensor node, regarded as cluster head (CH). A CH aggregates the data collected by the leaf nodes (non-CH sensor nodes) in its cluster, and sends the aggregation to the base station (BS). The low-energy adaptive clustering hierarchy (LEACH) protocol presented is a widely known and effective one to reduce and balance the total energy consumption for CWSNs.To prevent quick energy consumption of the set of CHs, LEACH randomly rotates CHs among all sensors nodes in the network, in rounds. LEACH achieves improvements in terms of network lifetime. The main advantage of the algorithm is by Data aggregation process we can enhance the secure, robustness and accuracy of information which is obtained by entire network, Another advantage is those reduces the traffic load and conserve energy of the sensor. such as LEACH (low-energy adaptive clustering hierarchy), have also advantages in terms of security

In 2007 L.B. Oliveira et al, [2] Worked on " "Sec LEACH-On the Security of Clustered Sensor Networks," This paper investigates the problem of adding security to hierarchical/cluster-based sensor networks where clusters are formed dynamically and periodically, such as LEACH. For this purpose, random key pre distribution, of flat networks, can be used to secure communications in CWNS. The main advantage of this scheme was security is concerned.

In 2007 P. Banerjee, D. Jacobson, and S. Lahiri, [3] Worked on ""Security and Performance Analysis of a Secure Clustering Protocol for Sensor Networks," The GS-LEACH (grid-based secure LEACH) protocol uses pre deployment key distribution using prior knowledge of the deployment area. The main advantage of this method is The GS-LEACH protocol is more energy efficient than any of the secure flavors of LEACH also GS-LEACH provides a longer network lifetime compared to the other flavors of LEACH.

In 2008 Zhang, C. Wang, and C. Wang, [4] Worked on ""A Secure Routing Protocol for Cluster-Based Wireless Sensor Networks Using Group Key Management," This paper, investigate adding security to cluster-based routing protocols for wireless sensor networks which consisted of sensor nodes with severely limited resources, and introduce a security solution for LEACH, a protocol in which the clusters are formed dynamically and periodically. Our solution uses improved random pair-wise keys (RPK) scheme, an optimized security scheme that relies on symmetric-key methods**.** The main advantage of this method is RLEACH Is Lightweight and Preserves the Core of the Original LEACH and also Security of RLEACH Has Been Improved. This method consumes Less Energy. The common disadvantages of leach system are:

2.1 Lack of Security Inleach Like Protocols

- Adding security to LEACH-like protocols is challenging because they dynamically, randomly, and periodically rearrange the network's clusters and data links.
- Providing steady long-lasting node-to-node trust Relationships and common key distributions are inadequate for LEACH-like protocols
- Most solutions are provided for distributed WSNs, but not for CWSNs)
- the dynamic nature of their communication makes most existing security solutions inadequate for them

2.2 Cluster Head Attack

The Cluster Head (CH) send data to the base station .This Cluster Head (CH) may be attacked by malicious attacker. If a cluster head is compromised, then the base station (sink) cannot be ensure the correctness of the aggregate data that has been send to it.

2.3 Orphan Node Problem

- There are some secure data transmission protocols based on LEACH-like protocols, such as Sec LEACH, GS-LEACH, and RLEACH. Most of them, however, 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.
- 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.
- 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.
- Since the more CHs elected by them, the more overall energy consumed of the network, the orphan

node problem increases the overhead of transmission and system energy consumption by raising the number of CHs.

2.4 Limit in Pairwise Key Sharing

Even in the case that 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.

III. IDENTITY BASED SCHEME

The feasibility of the asymmetric key management has been used in WSNs recently, which compensates the shortage from applying the symmetric key management for security. 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.

3.1 SET- IBS

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, for example, from its name or ID number. Recently, the concept of IBS has been developed as a key management in WSNs for security.

3.2 SET-IOOBS

The IBOOS scheme has been introduced to reduce the computation and storage costs of signature processing. A general method for constructing online/offline signature schemes was introduced. The IBOOS scheme could be effective for the key management in WSNs. Specifically; the offline phase can be executed on a sensor node or at the BS prior to communication, while the online phase is to be executed during communication.

The advantages of identity based scheme are:

- 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 Identity Based Scheme , 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
- Thus, users can obtain the corresponding private keys without auxiliary data transmission, which is efficient in communication and saves energy.
- SET-IBOOS is introduced to further reduce the computational overhead for security using the IBOOS scheme.
- Both SET-IBS and SET-IBOOS solve the orphan node problem in the secure data transmission with asymmetric key management.
- The Identity Based Scheme with respect to the security requirements and analysis against three attack models such as active attack, passive attack, compromising attack.

Table 1: Summary of Characteristics of the Identity Based Scheme with Other Secure Data Transmission Protocols

S. No	Methods	Secure Data Transmission Protocols	Identity Based Scheme
1	Protocol	• LEACH PROTOCOL • LEACHLIKEPROTOCOLS ➢ SECLEACH ➢ GSLEACH ➢ RLEACH	• SET IBS • SET IBOOS
2	Key	Symmetric Key	Symmetric Key
3	Storage Cost	High	Low
4	Network Scalability	Low	High
5	Communicational Overhead	Probabilistic	Deterministic
6	Computational Overhead	High	low
7	Attack	Robust Against • insider attacks • attack on intermediary nodes	Robust Against • Solutions to passive attacks on wireless channel • Solutions to active attacks on wireless channel. • Solutions to node compromising attacks

IV. ARCHITECTURE DEIGN

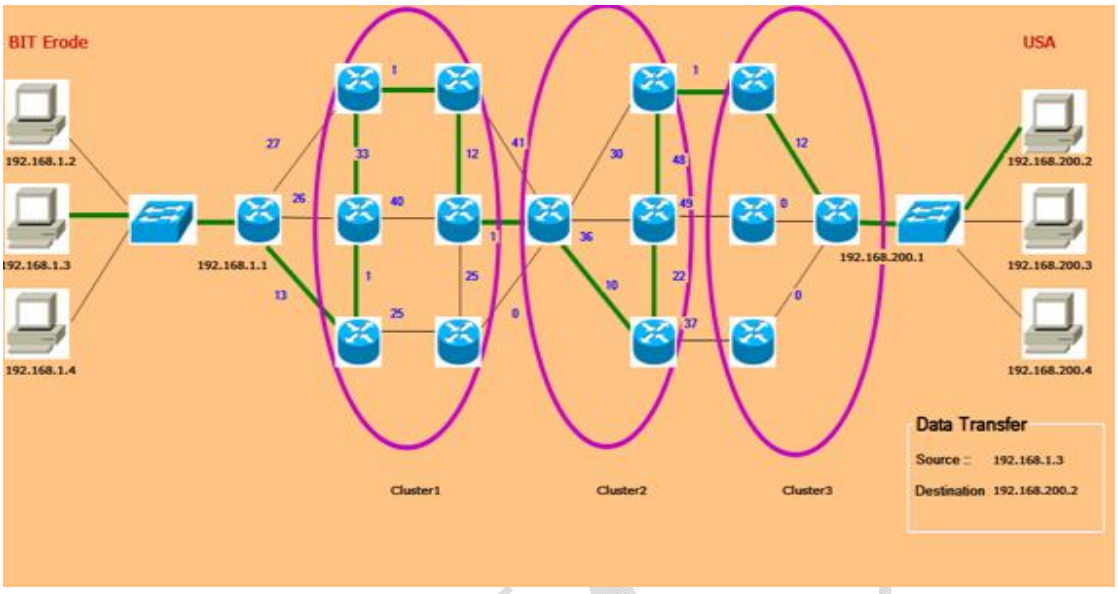

Fig 1: Architecture of proposed model

4.1 Features of SET-IBS and SET-IBOOS

- Both the SET-IBS and SET-IBOOS protocols provide secure data transmission for CWSNs with concrete ID-based settings, which use ID information and digital signature for authentication. Thus, both SET-IBS and SET-IBOOS fully solve the Orphan-node problem from using the symmetric key management for CWSNs.
- The secure data transmission protocols are with concrete ID-based settings, which use ID information and digital signature for verification.
- Comparing the SET-IBS, SET-IBOOS requires less energy for computation and storage
- Moreover, the SET-IBOOS is more suitable for node-to-node communications in CWSNs, since the computation is lighter to be executed.

Table 2: Comparison of Various Approaches

Year	Author	Title	Approach	Result
2002	W. Heinemann, A. Chandrakasan, and H. Balakrishnan	"An Application-Specific Protocol Architecture For Wireless Micro Sensor Networks"	**LEACH**- low-energy adaptive clustering hierarchy	Improvements In Terms Of Network Lifetime And Security
2007	L.B. Oliveira Et Al	" Sec LEACH-On The Security Of Clustered Sensor Networks"	**SECLEACH**-(security leach)	Improvement in Security
2007	P. Banerjee, D. Jacobson, and S. Lahiri	"Security And Performance Analysis Of A Secure Clustering Protocol For Sensor Networks ".	**GSLEACH**- (grid-based secure leach)	More energy efficient. Provides a longer network lifetime
2008	K. Zhang, C. Wang, and C. Wang	"A Secure Routing Protocol For Cluster-Based Wireless Sensor Networks Using Group Key Management"	**RLEACH**- routing leach	Consume Less Energy

V. CONCLUSION

These surveys introduce 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. The SET-IBS and SETIBOOS are efficient in communication and applying the ID based 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.

References

[1] W. Heinemann, A. Chandrakasan, and H. Balakrishnan, "An Application-Specific Protocol Architecture for Wireless Micro sensor Networks," IEEE Trans. Wireless Comm., vol. 1, no. 4, pp. 660-670, Oct. 2002.

[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. 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.

[5] Shamir, "Identity-Based Cryptosystems and Signature Schemes," Proc. Advances in Cryptology (CRYPTO), pp. 47-53,1985.

[6] J. Liu et al., "Efficient Online/Offline Identity-Based Signature for Wireless Sensor Network," Int'l J. Information Security, vol. 9, no. 4, pp. 287-296, 2010.