ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 9, September 2015

A Survey On Secure Data Transmission Over Cluster Based Wireless Sensor Networks

Amsapriya.S[1], Geetha.D[2]

PG Scholar, Dept. of Computer Science & Engineering, Adhiyamaan College of Engineering, Hosur, India[1]

Assistant Professor, Dept. of Computer Science & Engg., Adhiyamaan College of Engineering, Hosur India[2]

Abstract: Clustering is an effective and practical way to enhance the system performance of Wireless Sensor Networks (WSNs). In WSNs, it is highly a difficult task to achieve secure data transmission. In existing system, some of the protocols such as SecLEACH, GS-LEACH, and RLEACH were used, but orphan node problem exists. Thus by using these protocols, the orphan node problem is solved due to Node-to-node communication. Secure data transmission for Cluster –based WSNs (CWSNs) can be provided with help of protocols. In existing system, two secure and efficient Data transmission protocols namely SET-IBS and SET-IBOOS scheme were proposed SET-IBS has a protocol initialization prior to the deployment and operates in round communication. SET-IBOOS operates similarly to the previous SET-IBS. The feasibility of the SET-IBS and SET-IBOOS protocols with respect to the security requirement and security analysis various attacks. In this paper, a modified protocol SET-IBS has proposed that formed dynamically, randomly and periodically. Thus the probability of two nodes will share a key to orphan rate of the orphan node problem. SET-IBOOS system lifetime will be increased. The time of FND in both SET-IBS is shorter than that of LEACH protocol due to the security overhead on computation cost of the IBS process.

Keywords: WSNs, SecLEACH, GS-LEACH, RLEACH, CWSNs, SET-IBS, SET-IBOOS.

I. INTRODUCTION

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 [1]. 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 [2]. Secure and efficient data transmission (SET) is, thus, especially necessary and is demanded in many such practical WSNs.

Cluster-based data transmission in WSNs has been investigated by researchers to achieve the network scalability and management, which maximizes node lifetime and reduce bandwidth consumption by using local collaboration among sensor nodes [3]. In a cluster-based WSN (CWSN), every cluster has a leader sensor node, regarded as clusterhead (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). 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.

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.

II. RELATED WORK

The low-energy adaptive clustering hierarchy (LEACH) protocol presented by Heinzelman et al. [4] 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 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 [5] and PEACH [6], which use similar concepts of LEACH. In this paper, for convenience, we call this sort of cluster-based protocols as LEACH-like protocols.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 9, September 2015

Researchers have been widely studying CWSNs in the last decade in the literature. However, the implementation of the cluster-based architecture in the real world is rather complicated [7]. Adding security to LEACH-like protocols is challenging because they dynamically, randomly, and periodically rearrange the network's clusters and data links [8]. 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). There are some secure data transmission protocols based on LEACH-like protocols, such as SecLEACH [8], GS-LEACH [9], and RLEACH [10]. Most of them, however, apply the symmetric key management for security, which suffers from a so-called orphan node problem [11]. This problem occurs when a node does not share a pairwise 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 pairwise 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 pairwise keys decreases after a long-term operation of the network. Since the more CHs elected by themselves, the more overall energy consumed of the network [4], the orphan node problem increases the overhead of transmission and system energy consumption by raising the number of CHs. Even in the case that a sensor node does share a pairwise key with a distant CH but not a nearby CH, it requires comparatively high energy to transmit data to the distant CH.

The feasibility of the asymmetric key management has been shown in WSNs recently, which compensates the shortage from applying the symmetric key management for security [12]. 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 [13]. The identity-based digital signature (IBS) scheme [14], 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.

Carman [15] first combined the benefits of IBS and key predistribution set into WSNs, and some papers appeared in recent years [16], [17], [18]. The IBOOS scheme has been proposed to reduce the computation and storage costs of signature processing. A general method for constructing online/offline signature schemes was introduced by Even et al. [19]. 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. Some IBOOS schemes are designed for WSNs afterwards, such as [20].

The offline signature in these schemes, however, is pre-computed by a third party and lacks reusability, thus they are not suitable for CWSNs. Recently, 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.

III. SYSTEM DESCRIPTION AND PROTOCOL OBJECTIVES

1.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.

2) Security Vulnerabilities and Protocol Objectives

The goal of the proposed secure data transmission for CWSNs is to guarantee the secure and efficient data transmissions 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 [8], [9], [10], however, apply the symmetric key management for security, which suffers from the orphan node problem that is introduced in Section 1. In this paper, we aim to solve this orphan node problem by using the IDbased cryptosystem that guarantees security requirements, and propose SET-IBS by using the IBS scheme. Furthermore, SET-IBOOS is proposed to reduce the computational overhead in SET-IBS with the IBOOS scheme

IV. IBS AND IBOOS FOR CWSNS

In this section, we introduce the IBS scheme and IBOOS scheme used in the paper. Note that the conventional

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 9, September 2015

schemes are not specifically designed for CWSNs. We adapt the conventional IBS scheme for CWSNs by distributing functions to different kinds of sensor nodes, based on first. To further reduce the computational overhead in the signing and verification process of the IBS scheme, we adapt the conventional IBOOS scheme for CWSNs.

1. *Pairing for IBS*

For self-contained, we briefly review the characteristics of pairing. Boneh and Franklin introduced the first functional and efficient ID-based encryption scheme based on bilinear pairings on elliptic curves. Specifically, randomly select two large primes p and q, and let E/Fp indicate an elliptic curve $y2 = x3 + ax + b$ $(4a3 + 27b2 \neq 0)$ over a finite field Fp. We denote by G1 a q-order subgroup of the additive group of points in E/Fp, and G2 a q-order subgroup of the multiplicative group in the finite field Fp. The pairing is a mapping $e : G1 \times G2 \rightarrow G2$, which is a bilinear map with the following properties:

1. Bilinear. P, Q, R, S € G1, e (P + Q , R + S) = e(P,R) e(P,S) e(Q,R) e(Q,S).
2. Nondegeneracy. If P is a generator of G1, then e(P;P) is a generator of G2.
3. Computability. There is an efficient algorithm to compute e(P,Q) in G2, P,Q G1.

The security in the IBS scheme is based on the bilinear Diffie-Hellman Problem (DHP) in the pairing domain [13], and the hardness of DHP is defined. A bilinear map e is secure if, given g; G;H € G1, it is hard to find h € G1 such that e(h,H) = e(g,G). Weil pairing and Tate pairing are the examples of such bilinear mapping, which present comprehensive descriptions of how pairing parameters can be selected for security.

2. IBS Scheme for CWSNs

An IBS scheme implemented for CWSNs consists of the following operations, specifically, setup at the BS, key extraction 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 _, 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.

3. IBOOS Scheme for CWSN*s*

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 SIGoffline, and transmit it to the leaf nodes in its cluster.
- Online signing. From the private key sekID, SIGoffline and message M, a sending node (leaf node) generates an online signature SIGonline.
- Verification. Given ID, M, and SIGonline, the receiving node (CH node) outputs "accept" if SIGonline is valid, and outputs "reject" otherwise.

V. THE PROPOSED SET IBOOS PROTOCOL

We present the SET protocol for CWSNs by using IBOOS (SET-IBOOS) in this section. The SET-IBOOS protocol is designed with the same purpose and scenarios for CWSNs with higher efficiency. The proposed SET-IBOOS operates similarly to the previous SET-IBS, which has a protocol initialization prior to the network deployment and operates in rounds during communication.

VI. CONCLUSION

In this paper, we study a secure data transmission for cluster-based WSNs (CWSNs), where the clusters are formed dynamically and periodically. 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.

In SET-IBS, security relies on the hardness of the Diffie-Hellman problem in the pairing domain. SET-IBOOS further reduces the computational overhead for protocol security, which is crucial for WSNs, while its security relies on the hardness of the discrete logarithm problem. We show the feasibility of the SET-IBS and SET-IBOOS protocols with respect to the security requirements and security analysis against various attacks.

The results show that the proposed protocols have better performance than the existing secure protocols for CWSNs, in terms of security overhead and energy consumption.

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.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 9, September 2015

[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.
[11] S. Sharma and S.K. Jena, "A Survey on Secure Hierarchical Routing Protocols in Wireless Sensor Networks," Proc. Int'l Conf.Comm., Computing & Security (ICCCS), pp. 146-151, 2011.
[12] Gaubatz et al., "State of the Art in Ultra-Low Power Public Key Cryptography for Wireless Sensor Networks," Proc. IEEE Third Int'l Conf. Pervasive Computing and Comm. Workshops (PerCom), pp. 146-150, 2005.
[13] Diffie and M. Hellman, "New Directions in Cryptography," IEEE Trans. Information Theory, vol. IT-22, no. 6, pp. 644-654, Nov. 1976.
[14] A.Shamir,"Identity-Based Cryptosystems and Signature Schemes," Proc. Advances in Cryptology (CRYPTO), pp. 47-53, 1985.
[15] D.W. Carman, "New Directions in Sensor Network Key Management," Int'l J. Distributed Sensor Networks, vol. 1, pp. 3-15, 2005.
[16] R. Yasmin, E. Ritter, and G. Wang, "An Authentication Framework for Wireless Sensor Networks Using Identity-Based Signatures," Proc. IEEE Int'l Conf. Computer and Information Technology (CIT), pp. 882-889, 2010.
[17] H. Lu, J. Li, and H. Kameda, "A Secure Routing Protocol for Cluster-Based Wireless Sensor Networks Using ID-Based Digital Signature," Proc. IEEE GLOBECOM, pp. 1-5, 2010.
[18] J. Sun et al., "An Identity-Based Security System for User Privacy in Vehicular Ad Hoc Networks," IEEE Trans. Parallel & Distributed Systems, vol. 21, no. 9, pp. 1227-1239, Sept. 2010.
[19] S. Even, O. Goldreich, and S. Micali, "On-Line/Off-Line Digital Signatures," Proc. Advances in Cryptology (CRYPTO), pp. 263-275, 1990.
[20] S. Xu, Y. Mu, and W. Susilo, "Online/Offline Signatures and Multisignatures for AODV and DSR Routing Security," Proc. 11th Australasian Conf. Information Security and Privacy, pp. 99-110, 2006.