ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

Secure and Efficient Data Transmission for Cluster-based Wireless Technology Networks

Mohd Yousuf *1, Rasheeda Begum 2, Arshiya Begum 3

[*1] Dept. of Computer science Engineering, Maulana Azad National Urdu University, Hyderabad, India
[2] Dept. of Computer science Engineering, Shadan Women's College of Engineering & Technology, Hyderabad, India
[3] Dept. of Computer science Engineering, Dr. VRK Women's College of Engineering & Technology, Hyderabad, India
yousuf.asifia@gmail.com

Abstract

Secure data transmission network is a decisive issue for wireless technology networks (WTNs). Clustering is an effective and practical way to enhance the system performance & methods of WTNs. In this respective paper, we study a secure data transmitted for cluster-based method of WTNs (CWTNs), where the clusters are formed dynamically and periodically. We propose two Secure and Efficient data Transmission (SET) protocols for CWTNs, 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 WTNs, 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 CWTNs, in terms of security performance overhead and energy consumption.

Keywords: Cluster-based WTNs, ID-based digital signature, & online/offline digital signature, secure data n/w.

Introduction

A wireless technology network (WTN) 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 WTN [1]. Efficient data transmission is one of the most important issues for WTNs. meanwhile, many WTNs 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 is thus especially necessary and is demanded in many such practical WTNs.

Background and motivations

Cluster-based data transmission in WTNs has been investi- gated 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 [3]. In a cluster-based WTN (CWTN), 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 LEACH (Low-Energy Adaptive Clustering Hierarchy) protocol presented by Heinzelman *et al*. [4] is a widely known and effective one to reduce and balance the total energy consumption for CWTNs. 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 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

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

protocols. Researchers have been widely studying CWTNs 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 re- arrange 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 WTNs, but not for CWTNs). 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 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 . 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 pair wise 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 WTNs recently, which compensates the shortage from applying the symmetric key management for security [12]. 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 [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, e.g., from its name or ID number. Recently, the concept of IBS has been developed as a key management in WTNs for security. Carman [15] first combined the benefits of IBS and key pre-distribution set into WTNs, and some papers appeared in recent years [16–18]. The IBOOS scheme has been proposed in order 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 WTNs. 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 WTNs afterwards, such as [20] and [21]. The offline signature in these schemes, however, is precomputed by a third party and lacks reusability, thus they are not suitable for CWTNs.

System description and protocol objectives

This section presents the network architecture, security vulnerabilities and protocol objectives.

Network Architecture

Consider a CWTN consisting of a fixed base station (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 CWTN, sensor nodes are grouped into clusters, and each cluster has a cluster-head (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 CWTNs, data sensing, processing and transmission con- sume 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 TDMA (time division multiple access) control used for

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

data transmission. In this paper, the proposed SET-IBS and SET-IBOOS are both designed for the same scenarios of CWTNs above.

Security Vulnerabilities and Protocol Objectives

The data transmission protocols for WTNs, including cluster- based protocols (LEACH-like protocols), are vulnerable to a number of security attacks [2, 23]. Especially, attacks to CHs in CWTNs could result in serious damage to the network, because data transmission and data aggregation depend on the CHs fundamentally. If an attacker manages to compromise or pretend to be a CH, it can provoke attacks such as sinkhole and selective forwarding attacks, hence disrupting the network. On the other hand, an attacker may intend to inject bogus sensing data into the WTN, e.g., pretend as a leaf node sending bogus information towards the CHs. Nevertheless, LEACH- like protocols are more robust against insider attacks than other types of protocols in WTNs [23]. It is because CHs are rotating from nodes to nodes in the network by rounds, which makes it harder for intruders to identify the routing elements as the intermediary nodes and attack them. The characteristics of LEACH-like protocols reduce the risks of being attacked on intermediary nodes, and make it harder for an adversary to identify and compromise important nodes (CH nodes).

The goal of the proposed secure data transmission for CWTNs is to guarantee a secure and efficient data transmis- sion between leaf nodes and CHs, as well as transmission between CHs and the BS. Meanwhile, most of existing secure transmission protocols for CWTNs in the literature [8–10], 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 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 in SET-IBS with the IBOOS scheme.

IBS and IBOOS for CWTNS

In this section, we introduce the IBS scheme and IBOOS scheme used in the paper. Note that the conventional schemes are not specifically designed for CWTNs. We adapt the conventional IBS scheme for CWTNs by distributing functions to different kinds of sensor nodes, based on [24] at first. In order to further reduce the computational overhead in the signing and verification process of the IBS scheme, we adapt the conventional IBOOS scheme for CWTNs, based on [21].

Protocol evaluation

In this section, we first introduce the three attack models of the adversaries, and provide the security analysis of the Proposed protocols against these attacks. We then present results obtained from calculations and simulations. For the network simulations, we use the network simulator OMNeT++ 3.0 [33] to simulate SET-IBS and SET-IBOOS, and we focus on the energy consumption spent on message propagation and computation.

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 mcountermeasures of the proposed protocols, against various adversaries and attacks.

Attack Models

In this paper, we group attack models into three categoriesaccording 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 mcan 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 [2, 23].

• *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 the secret information stored in the compromised nodes, e.g., the security keys. The attackers also can change the inner state

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

and behavior of the compromised sensor node, whose actions may be varied from the premier protocol specifications.

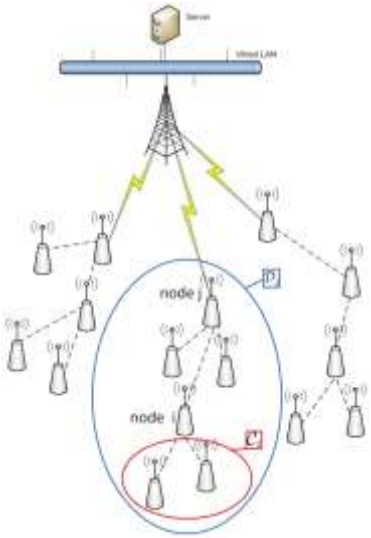
Solutions to Attacks and Adversaries

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 SETIBS 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 homomorphic encryption scheme from [30], 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 Based on the DHP assumption mentioned in Section 3, the ID-based key management in the proposed protocols is INDID- CCA secure (semantic secure against an adaptive ID-based chosen ciphertext 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 [34], 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. Since each round in the protocol operations terminates in a pre-defined time, SET-IBS and SET-IBOOS satisfy the property of protocol execution termination, depending on the local timer of the sensor nodes. The CH nodes are elected based only on their local decisions, therefore, both SET-IBS and SET-IBOOS operate if there exists an active or compromising attacker. In order to eliminate the compromised sensor node in the network, all the revoked IDs of compromised nodes will be broadcast by the BS at the beginning of the current round. In this way, the compromised nodes can be prevented from either electing as CHs or joining clusters in this round. Furthermore, using either the IBS scheme or the IBOOS scheme has at least two advantages. First, it eliminates the utilization of certificates and auxiliary authentication information. Therefore, the message overhead for security can be reduced, especially with IBOOS. Also, because only the compromised node IDs have to be stored, it requires very small storage space for the node revocation. Since the length of a user's ID is usually only 1~2 *bytes*, the storage of compromised user's IDs do not require much storage space.



ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

Conclusion

In this paper, we first reviewed the data transmission issues and the security issues in CWTNs. 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 SET-IBOOS are efficient in communication and applying the ID-based crypto-system, 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 CWTNs.

Acknowledgment

The authors would like to thank the Associate Editor and the anonymous reviewers, for their valuable suggestions and Comments that improved this paper.

References

1. T. Hara, V. I. Zadorozhny, and E. Buchmann, *Wireless Sensor Network Technologies for the Information Explosion Era*, *Stud. Comput. Intell.* Springer-Verlag, 2010, vol. 278.
2. Y. Wang, G. Attebury, and B. Ramamurthy, "A Survey of Security Issues in Wireless Sensor Networks," *IEEE Commun. Surveys Tuts.*, vol. 8, no. 2, pp. 2–23, 2006.
3. A. A. Abbasi and M. Younis, "A survey on clustering algorithms for wireless sensor networks," *Comput. Commun.*, vol. 30, no. 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 Commun.*, vol. 1, no. 4, pp. 660–670, 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 Distrib. Syst.*, vol. 13, pp. 1290–1302, 2002.
6. S. Yi, J. Heo, Y. Cho *et al.*, "PEACH: Power-efficient and adaptive clustering hierarchy protocol for wireless sensor networks," *Comput. Commun.*, vol. 30, no. 14-15, pp. 2842–2852, 2007.
7. K. Pradeepa, W. R. Anne, and S. Duraisamy, "Design and Implementa- tion Issues of Clustering in Wireless Sensor Networks," *Int. J. Comput. Applications*, vol. 47, no. 11, pp. 23–28, 2012.
8. L. B. Oliveira, A. Ferreira, M. A. Vilaça *et al.*, "SecLEACH-On the security of clustered sensor networks," *Signal Process.*, 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," in *Proc. IEEE NCA*, 2007, pp. 145–152.
10. K. Zhang, C. Wang, and C. Wang, "A Secure Routing Protocol for Cluster-Based Wireless Sensor Networks Using Group Key Manage- ment," in *Proc. WiCOM*, 2008, pp. 1–5.
11. S. Sharma and S. K. Jena, "A Survey on Secure Hierarchical Routing Protocols in Wireless Sensor Networks," in *Proc. ICCCS*, 2011, pp. 146–151.
12. G. Gaubatz, J. P. Kaps, E. Ozturk *et al.*, "State of the Art in Ultra- Low Power Public Key Cryptography for Wireless Sensor Networks," in *Proc. IEEE PerCom Workshops*, 2005, pp. 146–150.
13. W. Diffie and M. Hellman, "New Directions in Cryptography," *IEEE Trans. Inf. Theory*, vol. 22, no. 6, pp. 644–654, 1976.
14. A. Shamir, "Identity-Based Cryptosystems and Signature Schemes," in *Lect. Notes. Comput. Sc. - CRYPTO*, 1985, vol. 196, pp. 47–53.
15. D. W. Carman, "New Directions in Sensor Network Key Management," *Int. J. Distrib. Sens. Netw.*, vol. 1, pp. 3–15, 2005