International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 11, November 2015
Available at http://internationaljournalofresearch.org

Ensuring Secure and Efficient Data Transmission in Cluster-based Wireless Sensor Networks

Shaik Naseema Begum[1]; Lakshmanarao[2]& Sayeed Yasin[3]

[1] M.Tech (CSE), Nimra College of Engineering & Technology, A.P., India.
[2]Asst. Professor, Dept. of Computer Science & Engineering, Nimra College of Engineering & Technology, A.P., India
[3]Head of the Department, Dept. of Computer Science & Engineering, Nimra College of Engineering & Technology, A.P., India.

Abstract *—*
The most critical issue in wireless sensor networks is Secure data transmission. The system performance of WSNs can be improved by Clustering which is an effective and practical way to. 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 calculations and simulations are provided to illustrate the efficiency of the proposed protocols. 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.

Keywords —Cluster-based WSNs; ID-based digital signature; ID-based online/offline digital signature; secure data transmission protocol

I. Introduction

Efficient data transmission is one of the most important issues in wireless sensor networks. In a network system wireless sensor networks 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]. 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 is thus especially necessary and is demanded in many such practical WSNs.
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 [3]. 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 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 CWSNs. 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

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 11, November 2015
Available at http://internationaljournalofresearch.org

sort of cluster-based protocols as LEACH-like protocols. 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 earrange 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 Sec-LEACH [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. In order 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 [13], 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 WSNs for security. Carman [13] first combined the benefits of IBS and key pre-distribution set into
WSNs and some papers appeared in recent years [11–13]. 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 were introduced by Even et al. [10]. 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 [2] and [6]. The offline signature in these schemes, however, is precomputed by a third party and lacks reusability, thus they are not suitable for CWSNs

II .PROBLEM STATEMENT

Recently, we have applied and evaluated the key management Of IBS to routing in CWSNs [7]. In this paper, we extend Our previous work and focus on providing efficient secure data communication for CWSNs. The contributions of this work are as follows.

- We propose two Secure and Efficient data Transmission (SET) protocols for CWSNs, called SET-IBS and SETIBOOS, 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 crypto-systems [2].

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 11, November 2015
Available at http://internationaljournalofresearch.org

- 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 in order 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 SETIBOOS 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. Moreover, we compare the proposed protocols with the existing secure protocols for efficiency by calculations and simulations respectively, with respect to both computation and communication.

III .RELATED WORK

Protocol Characteristics

In this part, we summarize the characteristics of the proposed SET-IBS and SET-IBOOS protocols. Table I shows a general summary of comparison of the characteristics of SET-IBS and SET-IBOOS with prior ones, in which metrics are used to evaluate whether a security protocol is appropriate for CWSNs. We explain each metric as follows.

TABLE I: **Comparison of characteristics of the proposed protocols with other secure data transmission protocols**

	SET-IBS / SET-IBOOS	Prior protocols [8–10]
Key management	Asymmetric	Symmetric
Neighborhood authentication	Yes	Limited
Storage cost	Comparative low	Comparative high
Network scalability	Comparative high	Comparative low
Communication overhead	Deterministic	Probabilistic
computational overhead	Comparative high	Low ~ high
Attack resilience	Passive and active attacks on wireless channel	

Key management: The key cryptographies used in the protocol to achieve secure data transmission, which consist of symmetric and asymmetric key based security.

• ***Neighborhood authentication***: used for secure access and data transmission to nearby sensor nodes, by authenticating with each other. Here, "limited" means the probability of neighborhood authentication, where only the nodes with the shared pairwise key can authenticate each other.

• ***Storage cost***: represents the requirement of the security keys stored in sensor node's memory.

• ***Network scalability***: indicates whether a security protocol is able to scale without compromising the security requirements.
Here, "comparative low" means that, compared with SET-IBS and SET-IBOOS, in the secure data transmission with a symmetric key management, the larger network scale increases, the more orphan nodes appear in the network, and vice versa [2].

• ***Communication overhead***: the security overhead in the data packets during communication.

• ***Computational overhead***: the energy cost and computation efficiency on the generation and verification of the certificates or signatures for security.

• ***Attack resilience***: the types of attacks that security protocol can protect against.

Protocol operation

After the protocol initialization, SET-IBS operates in rounds during communication. Each round consists of a setup phase and a steady-state phase. We suppose that, all sensor nodes

The operation of SET-IBS is divided by rounds as shown in Figure1, which is similar to other LEACH-like protocols. Each round includes a setup phase for constructing clusters from CHs, and a steady-state phase for transmitting data from sensor nodes to the BS. In each round, the timeline is divided into

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 11, November 2015
Available at http://internationaljournalofresearch.org

consecutive time slots by the TDMA (time division multiple access) control [4]. Sensor nodes transmit the sensed data to the CHs in each frame of the steady state phase. For fair energy consumption, nodes are randomly selected as CHs in each round, and other non-CH sensor nodes join clusters using one-hop transmission, depending on the highest received signal strength of CHs. In order to elect CHs in a new round, each sensor node determines a random number and compares it with a threshold. If the value is less than the threshold, the sensor node becomes a CH for the current round. In this way, the new CHs are self-elected based by the sensor nodes themselves only on their local decisions, therefore, SETIBS functions without data transmission with each other in the CH rotations.

TABLE II: Operations in SET-IBS

Setup phase				
Step 1.	$BS \Rightarrow G_z$	:	$\langle ID_{bz}, T_z, nonce \rangle$	/* The BS broadcasts its information to all nodes. */
Step 2.	$CH_i \Rightarrow G_z$	:	$\langle ID_i, T_z, adv, \sigma_i, c_i \rangle$	/* The elected CHs broadcast their information. */
Step 3.	$L_j \rightarrow CH_i$	:	$\langle ID_i, ID_j, T_z, join, \sigma_j, c_j \rangle$	/* A leaf node joins a cluster of the CH i. */
Step 4.	$CH_i \Rightarrow G_z$	:	$\langle ID_i, T_z, sched(\ldots, ID_j/t_j, \ldots), \sigma_i, c_i \rangle$	/* A CH i broadcasts the schedule message to its members. */
Steady-state phase				
Step 5.	$L_j \rightarrow CH_i$	:	$\langle ID_i, ID_j, t_j, C_j, \sigma_j, c_j \rangle$	/* A leaf node j transmits the sensed data to its CH i. */
Step 6.	$CH_i \rightarrow BS$	:	$\langle ID_{bz}, ID_i, T_z, F_i, \sigma_i, c_i \rangle$	/* A CH i transmits the aggregated data to the BS. */

- *Notations* -	$\Rightarrow, \rightarrow$	:	Broadcast and unicast transmission.
	L_j, CH_i, G_z	:	A leaf node, a cluster head, and the set of sensor nodes in the network.
	T_z, t_j	:	Time-stamps denoting the time slot for transmission in setup and steady-state phases.
	ID_i, ID_{bz}	:	The IDs of a sensor node i and the BS.
	C_j, F_i	:	The encrypted sensed data of node j and the aggregated data of CH i.
	adv,join,sched	:	Message string types which denote the advertisement, join request, and schedule messages.
	$\langle \sigma_i, c_i \rangle$	:	The ID-based digital signature concatenated with data from node i.

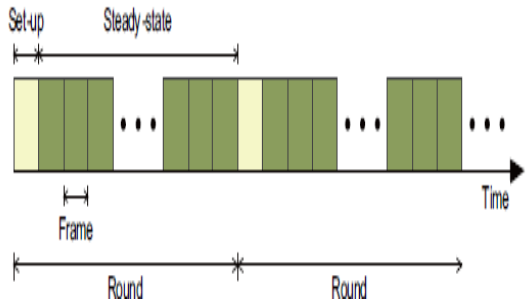

Fig.1. **Operation in the proposed secure data transmission**

know the starting and ending time of each round, because of the time synchronization.

Secure Data Transmission with Hierarchical Clustering

In large scale CWSNs, multi-hop data transmission is used for transmission between the CHs to the BS, where the direct communication is not possible due to the distance or obstacles
between them. The version of the proposed SET-IBS and SETIBOOS protocols for CWSNs can be extended using multi-hop routing algorithms, to form secure data transmission protocols for hierarchical clusters. The solutions to this extension could be achieved by applying the following two routing models.

1) The multi-hop planar model: A CH node transmits data to the BS by forwarding its data to its neighbor nodes, in turn the data is sent to the BS. We have proposed an energy efficient routing algorithm for hierarchically clustered WSNs in [1], and it is suitable for the proposed secure data transmission protocols.

2) The cluster-based hierarchical method: The network is broken into clustered layers, and the data packages travel from a lower cluster head to a higher one, in turn to the BS, e.g., [2].

PROTOCOL EVALUATION

In this we propose, and 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++ 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 countermeasures of the proposed protocols, against various adversaries and attacks.

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.

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 11, November 2015
Available at http://internationaljournalofresearch.org

• *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, 13].

• *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 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, the ID-based key management in the proposed protocols is INDID-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 fulfill 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 [5], 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 has 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.

IV. Conclusion

In this paper, we first reviewed 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. We provided feasibility of the proposed ET-IB Sand 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 CWSNs.

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 Implementation 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. Vilac¸a 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 Management," 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..