Proficient Identity-Based Online/Offline Signature Schemes For Cluster-Based Wireless Sensor Networks

K. Ananthakumar[#1] ,N. Gowthaman[*2], S. Nalini Devi[#3],A.Saranya[*4] ,K.Venkatesh Guru*[5](Assistant Professor)

[#]*Department of Computer Science and Engineering, Anna University*
K.S.R.College of Engineering, Tiruchengode-637 215,
Namakkal district, Tamil Nadu,India
[1]sureshananth03 @gmail.com
[3]nsnalini86@gmail.com[3]

[*] *K.S.R.College of Engineering, Tiruchengode-637 215,*
Namakkal district, Tamil Nadu,India
[2]n.gowthaman98@gmail.com

[4] sanjanasara333@gmail.com

[5]*guru2ksr@gmail.com*

.

Abstract--In (WSN)s secure data transmission is critical issue. One of the effective and practical way to enhance the system performance in WSNs is clustering.In a secure and effecient data transmission for (CWSNs), the clusters are formed dynamical and periodically. With the help of (IBS) and (IBOOS) two secure and effecient data transmission(SET) protocols are introduced for CWSNs, are SET-IBS and SET-IBOOS respectively. In SET-IBS, the process is not well secured due to Diffie-Helman problem in the pairing domain. In SET-IBOOS, it again reduces the computational overhead for protocol security, which is critical for WSNs, in which its security reduces due to discrete logarithmic problem. 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-Data transmission-SET-IBS-SET-IBOOS-Energy consumption

I. INTRODUCTION

A efficient data transmission is one of the most important issues for wireless sensor network(WSN).It is a network system that have the WSN to monitor the condition about temperature, sound, motion and any other physical or environmental condition. The each nodes are having the ability of sensing their environments, processing the information data locally, and the information of the data will be send to one or more collection points by the each and every individual nodes in a WSN. It will be used for military domains and sensing tasks with trust less surroundings. In practical, WSN used for secure and efficient data transmission.

II. BACKGROUND AND MOTIVATIONS

Cluster-based data transmission in WSNs, to achieve the network scalability and

management, in which maximizes node lifetime and reduce bandwidth consumption by using the sensor nodes. In a cluster-based WSN (CWSN), every cluster have a leader sensor node, that is named as cluster-head (CH). A CH collected the data from the remaining leaf nodes (non- CH sensor nodes) in its cluster, and it sends the base station (BS).In this concept the protocol which is used named ,as LEACH protocol ,presented by Heinzelman *etal*.It is one of the effective technique, which is used to reduce and balance the total energy consumption for CWSNs. It prevent quick energy consumption of the set of CHs, LEACH randomly rotates CHs among all sensor nodes in the network, in rounds. In this protocol to achieve the network lifetime. LEACH, a number of protocols are presented such as APTEEN [5] and PEACH [6], which use similar concepts of LEACH. In this paper we call this sort of cluster-based protocol as LEACH-like protocols. The implementation of the cluster-based architecture in the real world is rather complicated [7].Rearrangement of the network cluster and data link is challenging while adding security to LEACH-like protocols. Therefore, providing steady long-lasting node-to-node trust relationships and common key distributions are not sufficient 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].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, and the key ring is not sufficient for the node 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 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.In this 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 capable of being accomplished asymmetric key management has been shown in WSNs recently, which combine 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, 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 [15] first combined the benefits of IBS and key pre-distribution set into WSNs, and some papers appeared in recent years. 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. 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. The offline signature in these schemes, however, is precomputed by a third party and lacks reusability, thus they are not suitable for CWSNs.

III. CONTRIBUTIONS AND ORGANIZATION

Not long ago, we have evaluated and applied the key management of IBS to routing in CWSNs.In this concept we are mainly focus on providing efficient secure data communication for CWSNs. The contributions of this work are below as,

• By applying digital signatures Both of the key ideas in SET-IBS and SET-IBOOS is to authenticate the encrypted sensed data, to message packets, which are efficient in communication by using **IBS** and the **IBOOS** scheme and applying the key management for security purpose. In the proposed protocols, pairing parameters and secret keys are distributed and preloaded in all sensor nodes by the BS initially, which overcomes the key escrow problem described in ID-based

•To obtain the secure and effective communication, the SET-IBS using the technique as ID based cryptography and which enhances the energy to be saved.

•Both SET-IBS and SETIBOOS solve the orphan node problem in the secure data transmission with a symmetric key management. 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.

System **D**escription and **P**rotocol **O**bjectives

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

IV. NETWORK ARCHITECTURE

In this CWSN consisting of a fixed base station (BS) and a large number of wireless sensor nodes, which are homogeneous in functionalities and capabilities. Then We assume that the Base Station is always reliable, i.e., the BS is a trusted authority(TA).The data transmission is interrupted while the sensor nodes are compromised by attackers. The cluster are join depending on the receiving signal strength and transmit the sensed data to the BS via CHS to save the energy. The CHs perform, transmit data and data fusion to the BS directly with comparatively high energy. All BS and the sensor nodes 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 Data transmission is much more expensive than that of data processing. The intermediate node (e.g., a CH) collect the 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 data transmission.

V. SECURITY VULNERABILITIES AND PROTOCOL OBJECTIVES

Especially, attacks to CHs in CWSNs 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 WSN, 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 WSNs [21]. 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 in 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.

VI. KEY MANAGEMENT FOR SECURITY

Let assuming that encryption scheme in SET-IBS encrypt the message M,which is transmitted by the sensor node j,we denote that cipher text as C. Observed from the concept of an IBOOS scheme based on the DLP in the multiplicative group, and develop a novel secure data transmission protocol with IBOOS especially for CWSNs(SET-IBOOS).During the protocol initialization the corresponding private pairing parameters were loaded initially in the sensor nodes. The IBOOS scheme in the proposed SET-IBOOS may include following four operations, like extraction, offline signing, online signing and verification.

Extraction : Previous to the signature process, it first extracts private keys from the master secret key x and its identity ID as sek=(R,s_i)where

$$R = gr, \quad si=r+H(R,IDi)x \bmod q. \qquad (6)$$

Offline signing: During the transmission of message it creates the offline signature(σ_i)with the time stamp of its time slot t_i for transmission, after that it store the knowledge for signing online signature. Notice that, this offline signature can also be performed by sensor node itself or else by trusted third party. For example., the BS or the CH sensor node. Let $X=g^x$,then,

$$g^s{}_i = g^r g^{H(R,IDi)x \bmod q} = RX^{H(R,IDi) \bmod q.}, \quad \sigma_i=g^{-ti}. \qquad (7)$$

Online signing: Here, node A_i computes the online signature(σi, zi) by encrypted data C and the offline signature

$$h_i = H(C||\sigma_i), \quad z_i = \sigma_i + h_i s_i \bmod q, \quad \sigma_i=g^{\sigma i}. \qquad (8)$$

Then the encrypted message was send by A_i to its destination with signature(ID_i,,zi,C).

Verification: After receiving the message, every sensor node checks the authenticity by the following manner. Then it verifies the current time-stamp t_i for freshness. If that time-stamp is correct, the sensor node may further computes the value of g^{zi} and $\sigma_i RhiX^{hiH(R,IDi)} \bmod q$ using the online signature (σ_i, z_i),then verify if,

$$gz^i = \sigma^i Rh^i Xh^{iH(R,IDi)} \bmod q.$$

For correctness, we have the equation in the CH node as shown below,

If it is equal to the above equation in received message, then the sensor node considers that the received message is authentic ,and accepts it, then transmits the message to the next hop or user. If suppose that the above verification fails, the sensor node will considers the message either as bogus or as a replaced one, even if mistaken one, then it will reject it or ignore it.

VII. PROTOCOL OPERATION

Like SET-IBS, proposed SET-IBOOS operates similarly to it. During communication SET-IBOOS works in rounds, and based on the local decisions of CHs they are self-elected, hence it functions without data transmission in the CH rotations. The offline signatures are generated by the CHs, for the IBOOS key management in SET-IBOOS ,at the leaf nodes they are used for online signing. The full steps of SET-IBOOS in one round is shown in Table II, where the setup phase is from step 1 to 4,and the steady-state phase consist of Step 5 and 6.

Step1 in table II is similar that of Table I .However, the difference in step 2 and step 3 is change from the IBS to the online signature$(\sigma_i, z_i)$of the IBOOS scheme.

In step4,the offline signatures for the leaf nodes in its cluster is generated by a CH i. Then broadcasts an allocated message_(*alloc*(. . . , *IDj*/*tj*/σ *j*, . . .)) to its cluster for the secure communication during the steady-state phase, yet to concatenated with the online signatures. The TDMA control composes the allocation message consist of time schedule, which also allocates the time-stamp with an offline signature (*IDj*/*tj*/σ *j)*for node j.

W hen the setup phase is over ,the network system changes into the steady-state phase, in which data is transmitted to the BS. The steady-state operates similarly to that in steps 5 and 6 of table1

where the IBS is changed into the online signature of the IBOOS scheme.

VIII. PROTOCOL FEATURES

The protocol characteristics and hierarchical clustering solutions are this section .

• *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.

IX. 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. We focus on the energy consumption spent on message propagation and computation. We use the network simulator OMNeT++ 3.0 to simulate the proposed SET-IBS and SET-IBOOS, and the simulation source code can be found in [15].

X. IBSand **IBOOS** for **CWSN**s

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 CWSNs. We adapt the conventional
IBS scheme for CWSNs by distributing functions to different kinds of sensor nodes, based on [11] 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 CWSNs, based on [14].
In a multiplicative finite cyclic group G of prime order *q*, there exists an element *g* as the generator and elements

$g^x \in$ G, such that, G = (g) ={gx | $x \in Z_q^{*}$}, where, Z_q^{*}(Z_q^{*} = {0, 1, . . . , q−1}) is a multiplicative group consisting of q−1 integers, in which the multiplication operation in the group ends in the remainder on the division by q (mod q) [24]. The Discrete Logarithm Problem (DLP) [15] in the cyclic group G is to compute x, in which the computational complexity is believed to be hard in this work.

XI. 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. 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 CWSNs.

REFERENCES

[1] 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.

[2] 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.

[3] 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.

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] S. Sharma and S. K. Jena, "A Survey on Secure Hierarchical Routing
Protocols in Wireless Sensor Networks," in *Proc. ICCCS*, 2011, pp. 146–151.

[11] 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.

[12] W. Diffie and M. Hellman, "New Directions in Cryptography," *IEEE Trans. Inf. Theory*, vol. 22, no. 6, pp. 644–654, 1976.

[13] A. Shamir, "Identity-Based Cryptosystems and Signature Schemes," in *Lect. Notes. Comput. Sc. - CRYPTO*, 1985, vol. 196, pp. 47–53.

[14] D. W. Carman, "New Directions in Sensor Network Key Management,"
Int. J. Distrib. Sens. Netw., vol. 1, pp. 3–15, 2005.

[15] R. Yasmin, E. Ritter, and G. Wang, "An Authentication Framework for Wireless Sensor Networks using Identity-Based Signatures," in *Proc.*
IEEE CIT, 2010, pp. 882–889.

[16] H. Lu, J. Li, and H. Kameda, "A Secure Routing Protocol for Cluster-
Based Wireless Sensor Networks Using ID-Based Digital Signature," in *Proc. IEEE GLOBECOM*, 2010, pp. 1–5.

