International Journal of Advanced Information Science and Technology (IJAIST) ISSN: 2319:2682
Vol.4, No.4, April 2015 DOI:10.15693/ijaist/2015.v4i2.374-379

Secure Data Transmission in Cluster Based Wireless Sensor Network Using IBS and IBOOS Protocols

A.Sivabalasubramanian
M.E Communication & Networking
National Engineering College, Kovilpatti

V. Jackins
Assistant Professor/Department of IT
National Engineering College, Kovilpatti

***Abstract*—Secure data transmission is a major issue in wireless sensor networks (WSNs). Clustering is an effectual and practical way to enhance the system performance of WSNs. In this paper, a secure data transmission approach for cluster-based WSNs (CWSNs), where the clusters are formed repeatedly. We propose two secure data transmission protocols for CWSNs, called IBS and IBOOS, by using the identity-based digital signature (IBS) scheme and the identity-based online/offline digital signature (IBOOS) scheme, respectively. In IBS protocol, avoid the orphan node problem and IBOOS protocol further reduces the computational overhead for protocol security. The results show that the proposed IBOOS protocols have better performance than the IBS protocols for CWSNs, in terms of computational overhead and energy consumption.**

Index terms -Cluster-based WSNs, ID-based digital signature, ID-based online/offline digital signature, secure data transmission protocol

I. INTRODUCTION

A wireless sensor network (WSN) is a wireless network consisting of spatially distributed autonomous devices using sensors to cooperatively monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants, at different locations. There are many potential applications for WSNs [9]. 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 [10].The existing CWSNs uses the Low-Energy Adaptive Clustering Hierarchy (LEACH) protocol. LEACH is an effective protocol 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. The main disadvantage of existing methodology is adding security to LEACH protocol is not possible because they dynamically, randomly, and periodically rearrange the network's clusters and data links. Only symmetric key management is applicable for security which suffers from an orphan node problem. Secure and efficient data transmission (SET) is, thus, especially necessary and is demanded in many such practical WSNs [1] [2].

In this paper, we focus on providing an efficient secure data communication for CWSNs. The contributions of this work are as follows:

- We propose two Secure and Efficient data Transmission protocols for CWSNs, called IBS and IBOOS, by using the IBS scheme and the IBOOS scheme, respectively. The key idea of both IBS and 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 [6]. Secure communication in 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 [8].
- 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 IBS and 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 attacks. Moreover, we compare the proposed IBOOS protocols have better performance than the IBS protocols for CWSNs, in terms of computational overhead and energy consumption.

II. IBS AND IBOOS FOR CWSNs

A. 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 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[7].

B. IBOOS Scheme for CWSNs

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 transmits 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.

III. PROPOSED IBS PROTOCOL

The proposed IBS has a protocol initialization prior to the network deployment and operates in rounds during communication, which consists of a setup phase and a steady-state phase in each round. We introduce the protocol initialization; describe the key management of the protocol by using the IBS scheme, and the protocol operations afterwards. Fig1. Shows the block diagram of the IBS protocol.

A. Protocol Initialization

In the protocol initialization, the BS performs the following operations of key predistribution to all the sensor nodes:

- Generate an encryption key k for the homomorphic encryption scheme to encrypt data messages
- Generate the pairing parameters
- Choose two cryptographic hash functions
- Generate master key msk & network public key
- Preload each sensor node with the system parameters

B. Key Management for security

The IBS scheme consists of following three operations: extraction, signing, and verification.

- ***Extraction***– Node extract private key
- ***Signature signing***– Compute digital signature master key

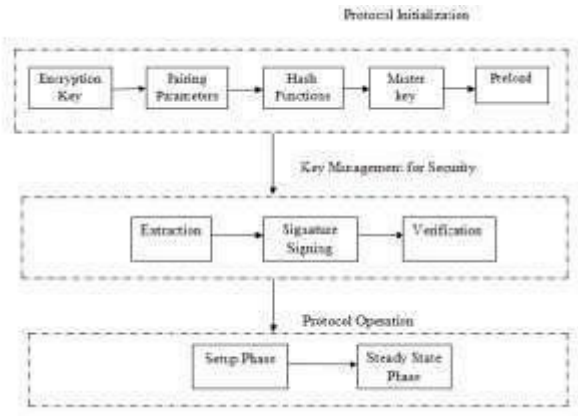


Fig.1. Block diagram of IBS protocol

- ***Verification***– When receiving the message, each sensor node verifies the authenticity. If the verification fails, the sensor node considers the message as either bogus or a replaced one, even a mistaken one, and ignores it.

C. Protocol Operation

After the protocol initialization, IBS operates in rounds during communication. Each round consists of a setuphase and a steady-state phase.

- ***Setup Phase***–The BS broadcasts its information to all nodes. The elected CHs broadcast their information. A leaf node joins a cluster of the CH *i.* A CH *i* broadcasts the schedule the message to its members.
- ***Steady-state Phase***–A leaf node j transmits the sensed data to its CH *i* .A CH *i* transmits the aggregated data to the BS.

IV. PROPOSED IBOOS PROTOCOL

The proposed IBOOS operates similarly to the previous IBS, which has a protocol initialization prior to the network deployment and operates in rounds during communication. We first introduce the protocol initialization, and then describe the key management of the protocol by using the IBOOS scheme, and the protocol operations afterwards. Fig2. Shows the block diagram of the IBOOS protocol.

A. Protocol Initialization

To reduce the computation and storage costs of signature signing processing in the IBS scheme, we improve IBS by introducing IBOOS for security in IBOOS. The operation of the protocol initialization in IBOOS is similar to that of IBS; however, the operations of key predistribution are revised for IBOOS. The BS does the following operations of key predistribution in the network:

- Generate an encryption key k for the homomorphic encryption scheme to encrypt data messages
- Generate the pairing parameters
- Choose two cryptographic hash functions

- Generate master key msk & network public key
- Preload each sensor node with the system parameters

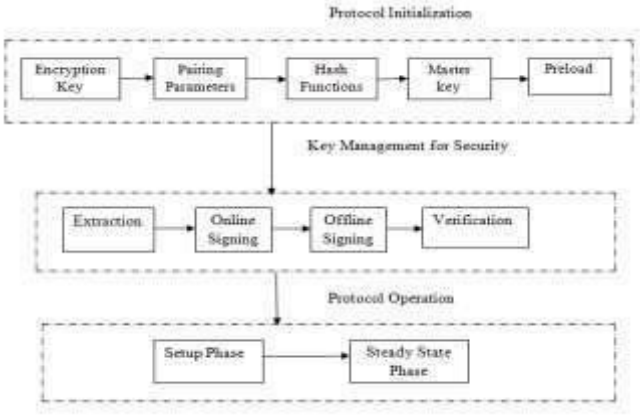


Fig 2. Block diagram of IBOOS protocol

B. Key Management for security

Assume that a leaf sensor node j transmits a message M to its CH i, and we denote the cipher text of the encrypted message as Cj, which is encrypted by the same encryption scheme in IBS. The corresponding private pairing parameters are preloaded in the sensor nodes during the protocol initialization. The IBOOS scheme in the proposed IBOOS consists of following four operations: extraction, offline signing, online signing, and verification.

- ***Extraction***– Node extract private key
- ***Offline signing***–offline phase can be executed on a sensor node
- ***Online signing***–Online phase is to be executed during communication
- ***Verification***– When receiving the message, each sensor node verifies the authenticity. If the verification fails, the sensor node considers the message as either bogus or a replaced one, even a mistaken one, and ignores it.

C. Protocol Operation

The proposed IBOOS operates similarly to that of IBS. IBOOS works in rounds during communication, and the self-elected CHs are decided based on their local decisions, thus it functions without data transmission in the CH rotations.

- ***Setup Phase***–The BS broadcasts its information to all nodes. The elected CHs broadcast their information. A leaf node joins a cluster of the CH *i.* A CH *i* broadcasts the schedule the message to its members.
- ***Steady-state Phase***–A leaf node j transmits the sensed data to its CH *i* .A CH *i* transmits the aggregated data to the BS.

V. SECURITY ANALYSIS

To evaluate the security of the proposed protocols, we have to investigate the attack models in WSNs that 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.

A. 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.
- ***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 [5], [10].
- ***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, for example, 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.

B. Solutions to Attacks and Adversaries

The proposed IBS and IBOOS provide different types of security services to the communication for CWSNs, in both setup phase and steady-state phase. Both in IBS and 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 IBS and IBOOS, the sensed data are encrypted by the homomorphic encryption scheme from [4], which deals with eavesdropping. Thus, the passive adversaries cannot decrypt the eavesdropped message without the decryption key. Furthermore, both IBS and IBOOS use the key management of concrete ID-based encryption [8].
- ***Solutions to active attacks on wireless channel***. Focusing on the resilience against certain attacks to CWSNs mentioned in attack models, IBS and IBOOS works 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, IBS and 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, IBS and 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 [3], 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.

VI. PERFORMANCE ANALYSIS

A. Performance Metrics

Several metrics can be defined to grade the performance of a technology against the elements of wireless networking. Some of these metrics have been carefully chosen to give an idea of behavior and the reliability of the networks. Before we go on to describe these metrics, it is reminded that the analysis focuses only on data transmission, and the metrics measure their features with respect to data packets, hence other routing overhead, are overlooked. A detailed explanation of these metrics follows: Packet loss, End to End Delay and Energy consumption.

- ***Packet loss***- Packet loss is typically caused by network congestion. When content arrives for a sustained period at a given router or network segment at a rate greater than it is possible to send through, then there is no other option than to drop packets. Packet loss can reduce throughput for a given sender, whether unintentionally due to network malfunction, or intentionally as a means to balance available bandwidth between multiple senders when a given router or network link reaches nears its maximum capacity. When reliable delivery is necessary, packet loss increases latency due to additional time needed for retransmission. Assuming no retransmission, packets experiencing the worst delays might be preferentially dropped (depending on the queuing discipline used) resulting in lower latency overall at the price of data loss. During typical network congestion, not all packets in a stream are dropped. This means that un dropped packets will arrive with low latency compared to retransmitted packets, which arrive with high latency. Not only do the retransmitted packets have to travel part of the way twice, but the sender will not realize the packet has been dropped until it either fails to receive acknowledgement of receipt in the expected order, or fails to receive acknowledgement for a long enough time that it assumes the packet has been dropped as opposed to merely delayed. Fig 3. Shows in x-axis, Number of nodes is assumed and in y-axis, packet loss is assumed. When compared with IBS nodes, the IBOOS node has less packet loss.

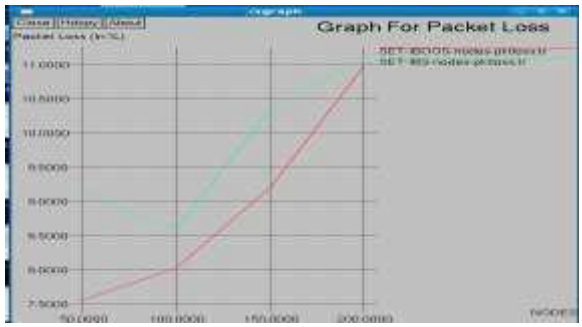


Fig.3 Comparison of packet loss in IBS and IBOOS protocol

- ***End to End***- The delay for a packet is the time taken for it to reach the destination. And the average delay is calculated by taking the average of delays for every data packet transmitted. The parameter comes into play only when the data transmission has been successful. It is defined as the average time taken for a packet to transmit across a network from the source to the destination. The lower value of end to end delay means the better performance of the protocol.

Average Delay = Sum of all Packet Delays / Total No. of Received Packets (1)

The delay is the time taken for a data packet to reach the destination node. The term, delay does not have much significance in this scenario. The simulations are performed with a star network topology, and the routing mechanism is disabled, because the standard doesn't support routing of data among peers. Therefore, the maximum number of hops for any data packet before reaching the destination node can be only1.

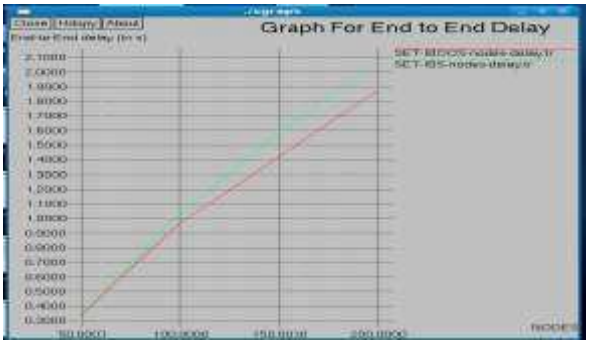


Fig.4 Comparison of delay in IBS and IBOOS protocol

Fig 4. Shows in x-axis, Number of nodes is assumed and in y-axis, End to End delay is assumed. When compared with IBS nodes delay, the IBOOS nodes delay has less .

- ***Energy Consumption***- The metric is measured as the percent of energy consumed by a node with respect to its initial energy. The initial energy and the final energy left in the node, at the end of the simulation run are measured. The percent energy consumed by a node is calculated as the energy consumed to the initial energy and finally the percent energy consumed by all the nodes in a scenario is calculated as the average of their individual energy consumption of the nodes. Fig 5. Shows in x-axis, Number of nodes is assumed and in y-axis, Energy consumption is assumed. When compared with IBS nodes energy consumption, the IBOOS nodes has less energy consumed .

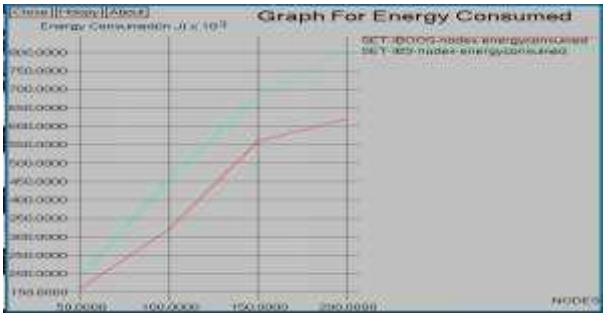
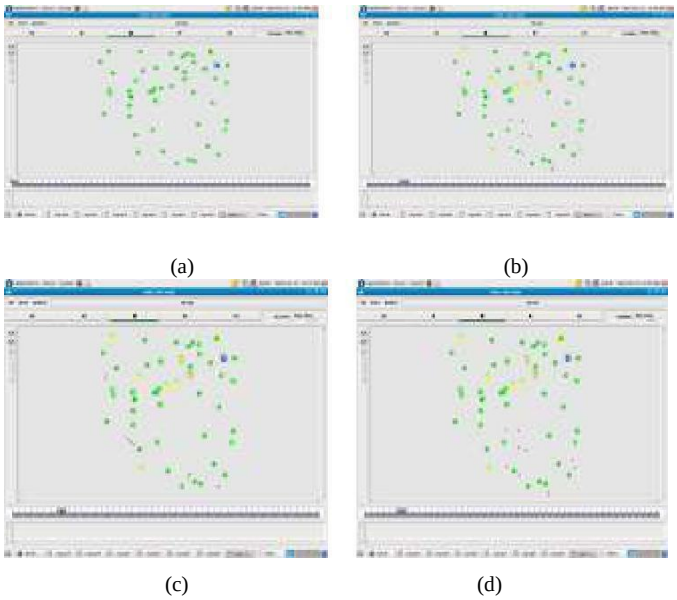


Fig 5. Comparison of Energy consumed in IBS and IBOOS protocol

VII. RESULTS AND DISCUSSION

In secure data transmission protocols for CWSNs, called IBS and IBOOS, by using the identity-based digital signature (IBS) scheme and the identity-based online/offline digital signature (IBOOS) scheme, respectively. In IBS protocol, avoid the orphan node problem and IBOOS protocol further reduces the computational overhead for protocol security. As a result, first creating the WSN with 50 nodes then set sink node it is nothing but centralized node and form cluster then elect cluster head on the basis of distance and packet transmission between leaf node and cluster head, as well as cluster head and base station and then implemented protocols, generated signature will be verified in two modes: valid and invalid. Each sensor node verifies the authenticity. If the verification fails, the sensor node considers the message as bogus, then drop the bogus packet.



(a) (b)

(c) (d)

Fig 6. Shows secure data transmission in CWSN using IBS and IBOOS

Fig.6(a) shows creating the WSN with 50 nodes and set sink node and fig.6(b) shows, elect cluster head on the basis of distance and fig.6(c) shows packet transmission between leaf node and cluster head, as well as cluster head and base station and fig.6(d) shows drop the bogus packet.

VIII. CONCLUSION

Thus two secure data transmission protocols IBS and IBOOS was proposed. These protocols could be effective for the key management in WSNs. The major advantages of these protocols are avoid orphan node problem, it is nothing but a node does not share a pairwise key with others in its preloaded key ring and also protect against active, passive and node compromising attack. Finally, simulation results show that the proposed IBOOS protocol have better performance than IBS protocol for CWSNs. With respect to computation, communication costs and energy consumption.

REFERENCES

[1]. 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.

[2]. Abdo Saif Mohammed.,"Secure Data Packet of Cluster Head and Base Station in Wireless Sensor Networks" *International Journal of Computer Science and Information Technologies*, Vol. 5 (4) , 2014.

[3]. B.Sun et al., "Intrusion Detection Techniques in Mobile Ad Hoc and Wireless Sensor Networks," *IEEE Wireless Comm. Magazine*, vol. 14, no. 5, pp. 56-63, Oct. 2007.

[4]. C. Castelluccia, E. Mykletun, and G. Tsudik, "Efficient Aggregation of Encrypted Data in Wireless Sensor Networks," *Proc. Second Ann. Int'l Conf. Mobile and Ubiquitous Systems: Networking and Services (MobiQuitous),* pp. 109-117, 2005.

[5]. C. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," *Ad Hoc Networks*, vol. 1, nos. 2/3, pp. 293-315, 2003.

[6]. D. Boneh and M. Franklin, "Identity-Based Encryption from the Weil Pairing," *Proc. 21st Ann. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO '01*), pp. 213-229, 2001.

[7]. 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.

[8]. Huang Lu.,"Secure and Efficient Data Transmission for Cluster-Based Wireless Sensor Networks" *IEEE Transactions on parallel and distributed systems*, vol. 25, No. 3, 2014.

[9]. I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. "A survey on sensor networks", *IEEE Communications Magazine*, 40(8):102–114, 2002.

[10]. 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.

Authors Profile

A.Sivabalasubramanian received the **B.E. degree** in Electronics and Communication Engineering from Unnamalai Institute of Technology, affiliated to Anna University, Chennai, India, in 2013 and currently doing **M.E. degree** in Communication and Networking Engineering from National Engineering College, affiliated to Anna University, Chennai, India.

V.Jackins received the **B.E. degree** in Electronics and Communication Engineering from Jayaraj annapackiam csi college of engineering, affiliated to Anna University, Chennai, India, in 2008 and his **M.E. degree** in Computer and Communication Engineering from National Engineering College, affiliated to Anna University, Tirunelveli, India in 2010 and currently doing his part time Ph.D. in Information and communication Engineering from Anna University, Chennai, India.