International Research Journal of Computer Science (IRJCS) ISSN: 2393-9842
Issue 05, Volume 4 (May 2017) SPECIAL ISSUE www.irjcs.com

A Survey on SET-IBS and SET-IBOOS Protocols for Cluster-Based WSN

Namana B.L[1], Megha Nayak[2], Vidya S[3], Nivedha N[4], Kantharaju H.C[5]
[1234]*UG Student,* [5]*Assistant Professor*
Department of CSE,
Vemana Institute of Technology,
,Visvesvaraya Technological University, Bengaluru, India,

Abstract ***—One of the main issue of the Wireless Sensor Networks (WSNs) is to furnish secure data transmission. In order to increase the performance of WSNs we use an efficient and constructive method called clustering. The survey is concerned with the secure data transmission for Cluster-based Wireless Sensor Networks (CWSN). To achieve energy competence we have introduced two new Secure and Efficient Data Transmission (SET) protocols. The proposed protocols are the SET-IBS and SET-IBOOS which is based on the Identity-Based Digital Signature (IBS) scheme and Identity-Based Online/Offline Digital Signature (IBOOS) scheme. The SET protocols have better performance compared to the existing protocols, in terms of security overhead and energy consumption for CWSNs.***

Keywords ***—Cluster-based WSNs, Secure Data Transmission, Identity-based Digital Signature, Identity-based Online/Offline Digital Signature***

I. INTRODUCTION

WSNs are used in many applications such as healthcare, military. These applications often examine the sensitive information such as opponent movement on the battleground or the place of staff in a building. Therefore security becomes most important in WSNs. Due to many constraints WSNs suffers, which includes partial energy resources, vulnerability to capture physically, computation capability is low, less memory[1].WSNs are set up in insensitive physical environments.

Efficient transmission of data is a significant issue for WSNs. Thus SET is very necessary and is vital in many such realistic WSNs. To decrease and balance the consumption of energy for CWSNs we make use of an efficient CWSN protocol called Low-Energy Adaptive Clustering Hierarchy (LEACH) [3]. To evade fast consumption of energy of cluster heads (CHs), they are randomly rotated in the network by the LEACH. The network's data links and clusters are reorganised periodically and dynamically by the LEACH protocol and adds the challenge to LEACH-like protocols such as RLEACH, Sec LEACH and GS-LEACH based on security. Therefore, providing constant long-term node-to-node dependence relationships and distribution of keys commonly are lacking for the above LEACH protocols. The security of symmetric key management relies on the orphan node problem which occurs in preloaded key ring where the pair wise key is not shared by a node with the rest of the nodes.

Digital signature scheme is a significant security service which is offered by asymmetric key management systems in cryptography. Digital certificate is obtained by binding the public key and the identification of the signer. To produce the public key of entity from its character information we use IBS. It tells that every phase of the design of a WSN application security must be encompassed for which a high intensity of security is required.

II. BACKGROUND

A. *Literature Survey*

In paper [2], Heinzelman et al., developed and assessed LEACH protocol's architecture for micro-sensor networks which integrates the concept of mutual clustering and media access with data aggregation that is application-specific to get exceptional working regarding to latency, application-perceived quality and system lifetime. LEACH adapts clusters by providing algorithms, a novel, cluster distribution configuration technique that provides self-organization for large number of nodes and CH rotating positions to allocate the load of energy between every nodes regularly and methods to save communication resources by providing distributed signal processing.

The outcome proves that regarding to magnitude as compared with general-purpose multi-hop methods the system lifetime can be enhanced using LEACH.The disadvantage of LEACH is that during their allocation of time division multiple accesses (TDMA) slot, the nodes broadcast their information to the CH continuously so its energy is not saved. While LEACH is being implemented, where every nodes are within the communication range of each other and the base station (BS), but the protocol scalability is limited.

Authors [3] introduced Power Efficient and Adaptive Clustering Hierarchy (PEACH) protocol for WSNs. This protocol has no much extra burden which makes the clusters and allows multi-level adaptive clustering and is also used for location-aware and location unaware WSNs. By the decrease in the consumption of energy of the nodes, there is an increase in network life span, which is better than the existing clustering protocols. Hence, the advantages of this protocol are that it gives extended network lifetime, lessens the consumption of energy, and improved scalability and also supports the adaptive multi-level hierarchical clustering. Here, the limitations that the security is not provided.

In paper [4], Leonardo B.Oet al., initially studied the difficulty in addition of security to CWSNs. So they proposed SecLEACH protocol for providing security in LEACH protocols. SecLEACH uses the key pre distribution that happens randomly. To provide security, hierarchical WSNs performs authenticated broadcast with active cluster configuration of rotating CHswhere µTESLA is used. The SecLEACH protocol also solves the orphan node problem by allowing the children which are already been adopted to bring back the orphan nodes into their clusters by adding up small protocols. The network performance is impacted by the amount of orphan nodes. As SecLEACH does not give pair wise communication so, the major issue in SecLEACH is the security which is possible to be its resiliency that is not in favour of node captures. Due to the constraints forced by sharing of key in SecLEACH, where all common nodes are not reachable by all CHs.

In paper [5], K. Zhang et al., studied that the addition of security to CWSNs which consisted of the sensor nodes with insensitively restricted resources. So, the authors proposed a solution of security for LEACH protocol that use advanced Random Pair-wise Keys (RPK) method which is based on probability of a definite number of node's shared key that are stored in each node's memory, which ensures network's connectivity by maintaining the probability of connection. This method relies on the symmetric key management which shows that RLEACH security has been improved, with decrease in energy utilization and least operating cost. The disadvantages of RLEACH are, well-built number of groups lead shorter lifetime as it establishes security mechanism using key management which increases the energy utilization and if less the amount of groups, the consumption of energy of establishing shared-key decreases and lessens the security.

A serious security need in authentication is to prevent attacks on the secure communication in WSNs and to reduce denial of service (DoS) attacks that use the limited resources of nodes. The main trouble is the sensor node's resource restraint while applying cryptographic based strong public key mechanisms of public key in WSNs.Due to the difficulty of authentication in WSNs, in paper [6] Rehana Yasmin et al., proposed an efficient and secure configuration for valid broadcast by sensor nodes and also for exterior user authentication, which makes use of identity-based online/offline signature (IBOOS) schemes. The main purpose of this proposed structure are to permit every node in the network, primarily, to transmit an authenticated message quickly; secondly, to verify the sender of the transmitted message and its contents; and lastly, to validate the authenticity of an external user. The proposed structure is also evaluated by the most SET-IBS schemes.

By studying the Identity-based cryptography in WSNs for security, in paper [7], H. Lu et al., advanced a new protocol for secure routing with IBS method for CWSNs where the security is reliant on the harshness of the Diffie-Hellman problem. So, as a effect of the communication operating cost for security, based on how a variety of parameters operate among saving energy and security, the authors provide the simulation work results. The limitation of this protocol is that the consumption of energy by the nodes is faster than LEACH protocol because communication burden and the pairing computation cost for IBS.

III. PROPOSED METHODOLOGY

A. *Network Architecture*

A CWSN consists of a base station (BS) which is fixed and a large number of wireless sensor nodes, which are standardized in their nature. Therefore, we assume that the BS is always dependable. The nodes are formed into clusters, every cluster has a CH and leaf (non-CH) nodes and the CH is selected based on the high energy level. Data combination is performed by the CHs and it transmits the data to the BS directly with relatively high energy. The energy of sensor nodes is consumed due to data sensing, processing and transmission which take place in CWSNs. The data processing cost is less compared to the cost of transmission of data. The aggregated data is sent by the CH node to the BS, this is preferred rather than sending data directly from the sensor nodes to the BS.

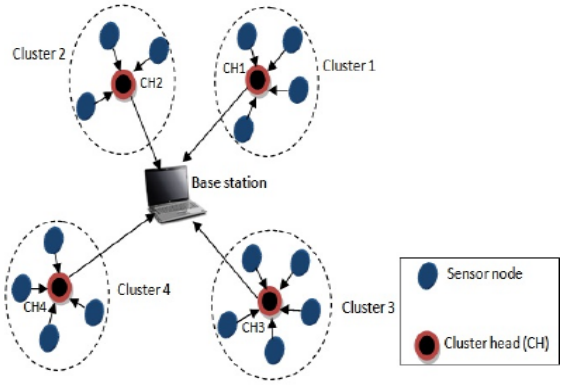

Fig 1: Architecture of CWSN

For saving energy the sensor node goes into the sleep node when there is no data transmission and the TDMA control is used for the transmission of data. Here in this paper, the proposed protocols are both designed for the same scenarios of CWSNs.

B. *SET-IBS*

The SET-IBS has a protocol initialisation for arrangement and operates in rounds during the communication; each round consists of a setup and a steady-state phase. The main idea of SET IBS is to validate the encrypted data which is efficient in key management and the key management is applied for its security.

1) ***Protocol Initialization*:** At initialisation stage, private pairing parameters are preloaded into the sensor nodes such that the node doesn't need to be generated by the private key at the initiation of each round necessary for the authentication of node with another. When node becomes orphan, its ID is distributed to all other nodes by the BS. This encryption scheme allows the conversion of the plain text to the cipher text. This result should match the decrypted result of the operations performed on plaintext. The BS preloads the key to all sensor nodes. It key is generated for encryption to encrypt the data messages.

- *It generates the pairing parameters.*
- *Chooses the cryptographic hash functions.*
- *It then picks an arbitrary integer as master key.*
- *It further preloads each sensor node with the public parameters*

2) ***Key Management for Security:*** We assume that the sensor leaf node n transfers the message to the CH, and the message is converted to cipher text with the key k using the homomorphic encryption scheme, where the cipher text is denoted by C. The SET-IBS scheme here consists of few operations they are abstraction, validation and verification.

3) ***Protocol operation:*** SET-IBS performs in rounds, each round contains a setup phase and a steady-state during communication.

SETUP PHASE:

i. The BS transmits its information to all the nodes
ii. The elected CH also broadcasts their information
iii. A leaf node joins a cluster of CH
iv. A CH broadcast the slotted message to its member

STEADY-STATE PHASE:

v. A non CH sensor node transmits the sensed information to its CH sensor node.
vi. A CH sensor node sends the aggregated information to the BS

C. SET-IBOOS

The SET-IBOOS is considered for higher energy competence, to reduce the computational operating cost for security in protocol which is essential for WSNs. SET-IBS is improved by introducing Online/Offline signature scheme for security in SET- IBOOS. The proposed protocol SET-IBOOS operates in the same way as the previous SET-IBS, which has a protocol initialization preceding to the network arrangement and it operates in sequences during communication.

1) ***Protocol Initialization:*** The protocol initialisation of this scheme is same like the SET- IBS. But the key predistribution operation is revised for this protocol. The BS does following operation for SET IBOOS:

- *It generates the encryption key with the help of homomorphic encryption scheme.*
- *The private key generation selects random generator g of group G and master key is chosen as the random number.*
- *Each node n selects the private key generation randomly and H as the hash function.*
- *Then it is preloaded with each sensor node of public parameters.*

2) ***Key Management for Security:*** The node n sends the message to the destination with time stamp and then the online signature in the form of identification of the node, offline signature, cipher text and time stamp. The IBOOS scheme in the SET-IBOOS protocol contains of four operations: extraction, offline signing, online signing, and verification.

3) ***Protocol operation:*** The operation of SET IBOOS is similar to SET IBS. It has set up phase and steady state phase.

Setup phase:

i. *The BS transmits its information to all the nodes*
ii. *The elected CH also broadcasts their information*
iii. *A leaf node joins a cluster of CH*
iv. *A CH broadcasts the allocation message*

STEADY-STATE PHASE:

v. The data is transmitted to the BS
vi. ID-based signature are changed to the online signature

IV. TABLE I
COMPARISON OF CHARACTERISTICS OF THE PROPOSED PROTOCOLS WITH EXISTING SECURE PROTOCOLS

Characteristics	Existing Protocols	Proposed protocols
Protocols	SecLEACH, LEACH, GS-LEACH, RLEACH	SET-IBS, SET-IBOOS
Key management	Symmetric	Asymmetric
Storage cost	High	Low
Network scalability	Low	High
Computational overhead	High	Low

V. OUTCOME

1) ***Packet delivery ratio***: The ratio between the received packets by the destination and the generated packets by the source. Therefore the existing protocols have less packet delivery ratio compared to the proposed protocols.

2) ***Delay:*** The difference between the time at which the sender generates the packet and the time at which the receiver receives the packet is known as delay. Hence delay in the SET protocols is less than the existing protocols.

*3)**Throughput:*** The number of valid packets received in a unit time and it is represented in bps. Therefore the SET protocols have more throughput than the exiting protocols.

4) ***Energy consumption:*** The energy consumption level of a node can be determined by finding the difference between the current energy value and initial energy value. Therefore the consumption of energy in the SET protocols is less compared to existing protocols.

5) ***Network lifetime:*** The time of first node dies (FND), which indicates that the duration of the sensor network is fully functional. Therefore maximising the life of FND in a WSN means to prolong the network lifetime. So we can say that the SET protocols have better network lifetime than the existing protocols.

VI. CONCLUSION

In the above literature survey, we have discussed about different protocols LEACH, PEACH, RLEACH, SecLEACH and Identity-Based Signatures LEACH. Here the drawback of the symmetric key management for secure data transmission has been reviewed followed by the study of two SET protocols for CWSNs. The SET-IBs and SET-IBOOS protocols are efficient in communication with the ID-based cryptography system and they achieve their security needs in CWSNs and also solve the orphan node problem in the secure data transmission protocols with ID information and digital signature for authentication. The SET-IBOOS has less secondary security overhead in term of computation, storage and communication costs for secure data transmission in CWSNs therefore, which results in less energy utilization and increase in the network life span. Hence these proposed protocols will give better performance as compared to existing protocols of CWSNs.

REFERENCES

[1]. T. Hara, V.I. Zadorozhny, and E. Buchmann, Wireless Sensor Network Technologies for the Information Explosion Era, Studies in Computational Intelligence, vol. 278. Springer-Verlag, 2010.
[2]. W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "An Application-Specific Protocol Architecture for Wireless Microsensor Networks," IEEE Trans. Wireless Comm., vol. 1, no. 4, pp. 660-670, Oct. 2002..
[3]. SanghoYi et al., "PEACH: Power-Efficient and adaptive Clustering Hierarchy Protocol for Wireless Sensor Networks," Computer Comm., vol. 30, nos. 14/15, pp. 2842-2852, 2007.
[4]. Leonardo B. Oliveira et al., "SecLEACH-On the Security of Clustered Sensor Networks," Signal Processing, vol. 87, pp. 2882-2895, 2007.
[5]. K. Zhang, C. Wang, and C. Wang, "A Secure Routing Protocol for Cluster-Based Wireless Sensor Networks Using Group Key Management," Proc. Fourth Int'l Conf. Wireless Comm., Networking and Mobile Computing (WiCOM), pp. 1-5, 2008.
[6]. Rehana Yasmin, E. Ritter, and G. Wang, "An Authentication Framework for Wireless Sensor Networks Using Identity-Based Signatures," Proc. IEEE Int"l Conf. Computer and Information Technology (CIT), pp. 882889, 2010.
[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.

