ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 6, June 2017

Secure and Efficient Data Transmission for Cluster Based Wireless Sensor Networks

Payal Kumbhalkar, Prof. Umesh Raut,

PG Student, Dept. of Computer Engineering, MIT, Pune, India

Associate Professor, Dept. of Computer Engineering, MIT, Pune, India

ABSTRACT: Wireless Sensor Networks (WSN) plays vital role in research field. Due to its rapidly increasing application in monitoring various kinds of environment by sensing physical phenomenon. Clustering is an efficient and effective method to enhance performance of the WSNs system. In this project work, we study a secure transmission of data for cluster-based WSNs (CWSNs), where the clusters are formed dynamically and randomly. 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. The cluster routing protocol LEACH (Low-Energy Adaptive Clustering Hierarchy) is considered and improved. In SET-IBS, security relies on the hardness of the Diffie-Hellman problem in the pairing area. SET-IBOOS additionally decreases the computational operating cost for protocol security, which is critical for WSNs, while its defense depends on the stability of the problem of discrete logarithm. We propose a clustering routing protocol named Enhanced LEACH, which extends LEACH protocol by balancing the energy consumption in the network.The simulation results show that Enhanced LEACH outperforms LEACH in terms of network system lifetime and reduce the energy consumption.

KEYWORDS: CWSN, LEACH, SET-IBS, SET-IBOOS.

I. INTRODUCTION

Wireless sensor network (WSN) is a system of network comprised of spatially distributed devices using wireless sensor nodes to examine environmental or physical conditions, such as temperature, sound and movement. The individual nodes are competent of sensing their environments, processing the information statistics in the vicinity, and sending data to one or more compilation points in a WSN. Efficient transmission of data is one of the most significant issues for WSNs. Usually many WSNs are installed in unobserved, harsh and often adversarial physical environments for specific applications, such as armed forces domains and sensing tasks with unreliable surroundings. Efficient and secure transmission of data is thus very essential and is required in many such realistic WSNs. Cluster-based transmissions of data in WSNs, has been examined by researchers in order to accomplish the network scalability and supervision, which maximizes node life span and reduces bandwidth utilization by using local cooperation between sensor nodes. In a cluster-based WSN (CWSN), each cluster has a leader sensor node, known as cluster-head (CH). A CH collects the data gathered by the leaf nodes (non- CH sensor nodes) in its cluster, and sends the pooled data to the base station (BS).The probability of the asymmetric key management has been revealed in WSNs in recent times, which compensates the deficiency from relating the symmetric key management for security. Digital signature is one of the most significant security services presented by cryptography in asymmetric key management systems, where the binding between the public key and the recognition of the signer is acquired via a digital certificate. The Identity-Based digital Signature (IBS) scheme, based on the complexity of factoring integers from Identity- Based Cryptography (IBC), is to develop an entity's public key from its character information, e.g., from its identification number or its name. This states that security must encompass every phase of the design of a wireless sensor network application that will require a high intensity of security. Probable applications comprise monitoring isolated or hostile locations, objective tracking in combat zone, catastrophe liberation networks, premature fire recognition, and environmental supervision. A primary topic

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 6, June 2017

that must be addressed when using cluster-based security protocols based on symmetric session keys is the means used for ascertaining the session keys in the primary place. A vital design concern for security protocols based on symmetric keys is the degree of session key among the nodes in the system. On the other hand, it has the clear security drawback that the negotiation of a single node will disclose the global key.

A wireless sensor network (WSN) generally consists of a base station (or "gateway") that can communicate with a number of wireless sensors via a radio link. Data is collected at the wireless sensor node, compressed, and transmitted to the gateway directly or, if required, uses other wireless sensor nodes to forward data to the gateway. The transmitted data is then presented to the system by the gateway connection. The purpose of this chapter is to provide a brief technical introduction to wireless sensor networks and present a few applications in which wireless sensor networks are enabling. A WSN usually consists of tens to thousands of such nodes that communicate through wireless channels for information sharing and cooperative processing. WSNs can be deployed on a global scale for environmental monitoring and habitat study, over a battle field for military surveillance and reconnaissance, in emergent environments for search and rescue, in factories for condition based maintenance, in buildings for infrastructure health monitoring, in homes to realize smart homes, or even in bodies for patient monitoring. After the initial deployment (typically ad hoc), sensor nodes are responsible for self-organizing an appropriate network infrastructure, often with multi-hop Connection between sensor nodes. The onboard sensors then start collecting acoustic, seismic, infrared or magnetic Information about the environment, using either continuous or event driven working modes as shown in Fig.1.

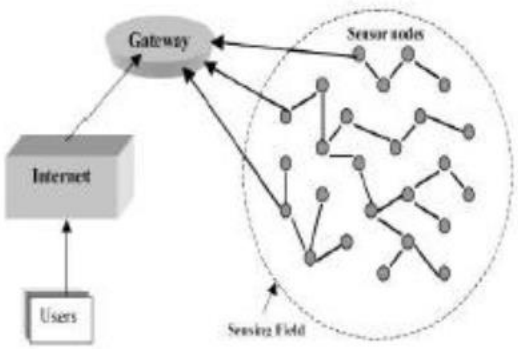

Fig.1. Architecture of WSN.

II. RESEARCH ELABORATIONS

L.B. Jivanadhamet al. proposed creation of a Secured Cluster-based architecture for a Dynamic Wireless Sensor Network that applies two topology management procedures: node-move-in and node-move-out. The planned security protocol incorporate one round Zero Knowledge Proof and AES algorithm to relate for node authentication, wherever only authenticated nodes will be acknowledged through node-move-in operation. In addition they explained that, it needs O(h+q) rounds for a node to connect into a network securely, where h is the height of the dynamic cluster-based wireless sensor network and q is the number of adjacent nodes of a joining node. After the O(h+q) attempts to join the network, the node is considered as insecure and is eventually discarded from joining the network as in [1]. HichemSedjelmaciet.al proposed an intrusion detection framework for a cluster-based WSN (CWSN) that intend to merge the advantage of anomaly
and signature detection which are high discovery rate and low false positive, correspondingly. Wireless sensor networks (WSNs) have a enormous potential to be used in vital circumstances like armed forces and commercial applications. On the other hand, these applications are mostly frequently to be deployed in hostile surroundings, where nodes and communication are smart targets to intruders. This makes WSNs susceptible to a range of possible attacks. Because of their characteristics, conservative security methods are not appropriate. So

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 6, June 2017

here the authors have proposed an intrusion detection framework for a cluster-based WSN (CWSN) that aims to merge the advantage of signature detection and anomaly which are high detection rate and MaanYounis Abdullah et al in inspected the problem of security addition to cluster based communication protocols
for homogeneous wireless sensor networks containing sensor nodes with very limited resources, and proposed a security resolution where clusters are created periodically and dynamically.

Their explanation depicts re-keying function protocol for wireless sensor networks security. They have projected the local administrative functions as master function, derivation function and rekeying function is imprinted with sensor node. A security and performance study proved that it is very proficient in communication, storage, computation and this technique is very successful in defending against a lot of complicated attacks [3] Tingyao Jiang et.al presented a new dynamic intrusion detection method for cluster-based wireless sensor networks(CWSN). The nodes in a wireless sensor network are assembled into clusters depending on the particular relationships with a cluster head (CH) in every cluster. The projected scheme initially makes use of a clustering algorithm to construct a model of standard traffic behavior, and then uses this model of standard traffic to detect anomalous traffic patterns. Along with the diverse network conditions of clusters, this method might also dynamically set different detection factors for different clusters to accomplish a more proper detection algorithm. The performance study showed that the projected intrusion detection method can progress the detection accuracy and decrease the false positive rate, and is extremely efficient of the energy preservation as in [4]. low false positive, correspondingly as in [2].

Nikolaos A. Pantaziset.al presented a classification of energy efficient routing protocols and expanded the classification initially done by Al-Kariki to better describe which issues/operations in each protocol illustrate/enhance the energy efficiency issues. The distributed behavior and dynamic topology of Wireless Sensor Networks (WSNs)brings in many unusual requirements in routing protocols that should be fulfilled. The main important aspect of a routing protocol, so as to be efficient for WSNs, is the energy usage and the extension of the network's life span. During the past few years, a lot of energy efficient routing protocols have been projected for WSNs. The authors here presented the four types of schemes of energy efficient routing protocols: Network Structure, Communication Model, Topology Based and Reliable Routing. The routing protocols which belong to the first type can be additionally classified as hierarchical or flat. The routing protocols belonging to the second type can be additionally classified as Query-based or Coherent and non-coherent based or Negotiation-based. The routing protocols belonging to the third type can be additionally classified as Location-based or Mobile Agent-based. The routing protocols belonging to the fourth type can be additionally classified as QoS-based or Multipath based. Lastly, a systematic review on energy efficient routing protocols for WSNs is provided as in [5].
Key management methods, except many of them were planned for flat wireless sensor networks, which are not suitable for cluster-based wireless sensor networks (like LEACH). Here Kun Zhang et.al investigated adding security to cluster based routing protocols for wireless sensor networks which consist of sensor nodes with very inadequate resources, and have proposed a security solution for LEACH which is a protocol in which the clusters are created periodically and dynamically. The solution proposed by authors makes use of enhanced Random Pair-wise Keys (RPK) method, an optimized security method that depends on symmetric key methods and is a lightweight and conserves the heart of the original LEACH protocol. Simulations demonstrate that security of RLEACH has been enhanced, with reduction in energy utilization and very less operating cost as in [6]. In Wireless Sensor Networks (WSNs), a crucial security necessity is authentication to evade attacks against secure Communication, and to diminish DoS attacks utilize the limited resources of sensor nodes. Resource restraint of sensor nodes are major difficulty in applying strong public key cryptographic based mechanisms in WSNs. To deal with the problem of authentication in WSNs, Yasmin, R et.al have proposed secure and efficient framework for authenticated broadcast/multicast by sensor nodes and for outside user authentication, which uses identity based cryptography and online/offline signature schemes.

The most important objectives of this framework are to allow all sensor nodes in the network, initially, to broadcast and/or multicast an authenticated message rapidly; secondly, to confirm the broadcast/multicast message

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 6, June 2017

sender and the message contents; and lastly, to confirm the authenticity of an outside user. The projected framework is also evaluated by means of the most secure and efficient identity-based signature (IBS)schemes as in [7]. A secure routing for cluster-based sensor networks is where clusters are formed periodically and dynamically. Together with the investigation of ID-based cryptography for security in WSNs, Huang Lu et.al proposed anew secure routing protocol with ID-based signature scheme for cluster-based WSNs within which the security is dependent on the hardness of the Diffie-Hellman problem in the random oracle model. Here the deficiency in the secure routing protocols with symmetric key pairing is pointed out by authors. Because of the communication operating cost for security, authors provide simulation investigation results in details to demonstrate how various parameters act among energy efficiency and security as in [8].

A process by which data is collected and sent from sensor nodes to the base station is known as data aggregation. It is completed via some sensor nodes called aggregators. A key role is played by security in data aggregation procedure to make sure confidentiality and privacy of aggregated data., In [9] Nguyen Xuan Quy et.al proposed a data aggregation method for cluster-based WSN that improves the security against attackers. This method was based on accelerated homomorphism public key encryption which presents continuous suppression of and supports hop-to-hop verification. The logical investigation and association demonstrate that this approach has both lower computational and better security performance as compared to other approaches as in [9]. In this paper, we do not assume any prior knowledge about the data indeed in many applications; raw data may not be easily categorized into different types.

To transmit the collected data toa remote location is also considered Expensive because the total collected data may be in a very large quantity. To facilitate data query. The operation of LEACH is divided into rounds. Each round begins with a setup phase when the clusters are organized, followed by a Steady-state phase when data are transferred from the nodes to the cluster head and on to the Base Station (BS).

The LEACH network has two phases:
Set-up phase: The selected CH informs about its selections as CH among the group. Non cluster-head nodes decide their cluster for current round by choosing the CH that requires minimum communication energy, based on the received signal strength of the advertisement from each CH. After the selection each non-CH informs the CH by transmitting a join request message (Join-REQ) back to the CH. Then the CH node sets up and broadcast a TDMA schedule to all member non-CH nodes. Steady State Phase: The Steady Sate Phase is broken into many frames, in which nodes can send their data to the CH at most once per time slot. CH sends the aggregated data to BS in single hop manner. The LEACH provides better results compared communication protocol, minimum-transmission-energy protocol and static Clustering protocol in Wireless Sensor to earlier existing protocols e.g. direct Network.

The available redundant information is subsequently cancelled during aggregation process performed by CH. Then the CH will broadcast an advertisement message to inform all others that it is the new cluster-head. The nodes send the join-request message containing their IDs by using CSMA (carrier sensing multiple access) to join a cluster. The node joins that cluster from which they received strongest strength signal. After that, each CH knows its own cluster members information. Based on the message, the CH creates TDMA schedule table and broadcasts it to the cluster members. So all the member nodes know their idle slots, and then the steady-state phase begins. The cluster based protocols (like LEACH) which are the data transmission protocols for WSNs, are susceptible to many security attacks. In general, the attacks to Cluster Heads in CWSNs can produce serious damage to the network, since security attacks. Data aggregation and data transmission rely on the CHs primarily. If an invader manages to act as if it's a CH or negotiate the CH, it can incite attacks such as selective forwarding attacks and sinkhole, thus upsetting the network. Alternatively an attacker may mean to insert false sensing data into the WSN, like pretending as a leaf node transferring false information to the CHs. However, LEACH like protocols are extra tough against insider attacks rather than other types of protocols in WSNs as shown in Fig.2. Since CHs are rotating from nodes to nodes in the network by rounds making it harder for types of protocols in WSNs.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 6, June 2017

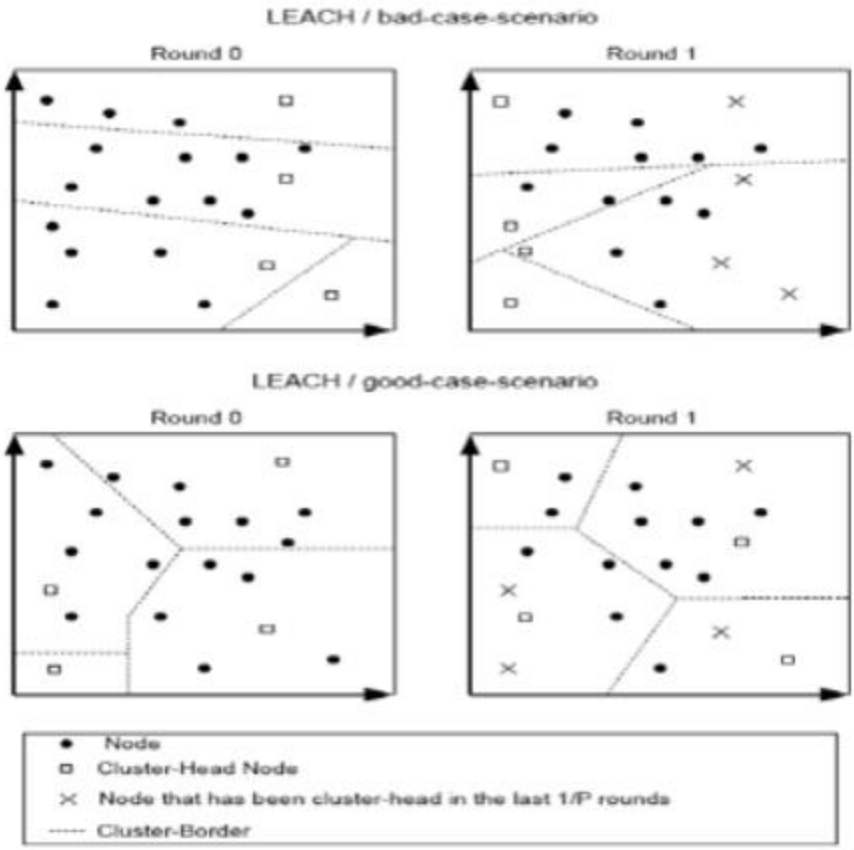

Fig.2.Example of LEACH Network.

The goal of the proposed secure data transmission for CWSNs is to guarantee a secure and efficient data transmission between leaf nodes and CHs, as well as transmission between CHs and the BS. eanwhile, most of existing secure transmission protocols for CWSNs in the literature, however, apply the symmetric key management for security, which suffers from the orphan node problem that is introduced, 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. The propose two novel Secure and Efficient data Transmission (SET) protocols for CWSNs, called SET-IBS and SET-IBOOS, by using the IBS scheme and the IBOOS scheme, respectively. We first present SET-IBS in this section. The proposed SET-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. After the protocol initialization, SET-IBS operates in rounds during communication. Each round consists of a setup phase and a steady-state phase as shown in Fig.3. We suppose that, all sensor nodes know the starting and ending time of each round, because of the time synchronization. The operation of SET-IBS is divided by rounds as shown in Figure, 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 consecutive time slots by the TDMA (time Division multiple access) control. Sensor nodes transmit the sensed data to the CHs in each frame of the steady state phase. For fair energy consumption, nodes

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 6, June 2017

arerandomly 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. The steady-state phase consists of the latter two Steps In the setup phase, the time-stamp Ts and node IDs are used for the signature generation. Whereas, in the Steady-state phase, the time-stamp ti is used for the signature generation ecuring the inner cluster communications, and Ts is used for the signature generation securing the CHs-to-BS data transmission. The proposed SET-IBOOS operates similarly to that of SETIBS. SET-IBOOS works in ounds during communication, and the self-elected CHs are decided based on their local decisions, thus it functions without data transmission in the CH rotations. For the IBOOS key management in SET-IBOOS, the offline signatures are generated by the CHs, which are used for the online signing at the leaf nodes.

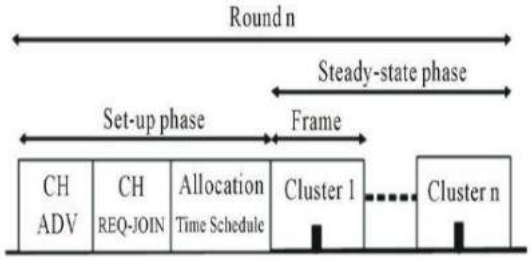

Fig.3. LEACH Protocol operation.

Setup phase

Step 1. $BS \Rightarrow G_z$: $\langle ID_{bz}, T_z, nonce \rangle$

Step 2. $CH_i \Rightarrow G_z$: $\langle ID_i, T_z, adv, \sigma_i, z_i \rangle$

Step 3. $L_j \rightarrow CH_i$: $\langle ID_i, ID_j, T_z, join, \sigma_j, z_j \rangle$

Step 4. $CH_i \Rightarrow G_z$: $\langle ID_i, T_z, alloc(\ldots, ID_j/t_j/\sigma_j, \ldots), \sigma_i, z_i \rangle$

Steady-state phase

Step 5. $L_j \rightarrow CH_i$: $\langle ID_i, ID_j, t_j, C, \sigma_j, z_j \rangle$

Step 6. $CH_i \rightarrow BS$: $\langle ID_{bz}, ID_i, T_z, F, \sigma_i, z_i \rangle$

/* The BS broadcasts its information to all nodes. */

/* The elected CHs broadcast their information. */

/* A leaf node joins a cluster of CH_i. */

/* A CH i broadcasts the allocation message. */

/* A leaf node j transmits the sensed data to its CH i. */

/* A CH i transmits the aggregated data to the BS. */

Enhanced leach is a T-LEACH stands for threshold-based LEACH because it replaces cluster heads based on the threshold value of residual energy on the sensor nodes. In traditional protocols relating to cluster optimization, the authors proposed that the number of cluster heads be reduced to decrease energy consumption or that energy efficiency-based optimal cluster sizes be constructed to extend the survival time of the network. LEACH algorithm has a structure where cluster heads are selected according to probabilistic values and the collection and transmission of messages occur during each round. Consequently, the number of cluster heads and rounding periods come to be closely related to energy consumption. In these algorithms,

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 6, June 2017

nodes play the roles of cluster heads periodically, and these are not considering energy cost of that time. When arbitrary sensor nodes become cluster heads through the performance of rounds, nodes selected as cluster heads must broadcast to member nodes of the clusters to which they belong that they have become cluster heads. Consequently, as the frequency of rounding and of cluster head replacement increases, energy consumption increases due to message transmission for broadcasting.

Algorithm 1 Steady phase

```
for each frame f in round r do
    for each cluster member cm_i do
        if cm_i.Timeslot = TRUE then
            Transmit data to aggregator node cm_aggregator
        else
            cm_i.SleepMode = TRUE;
        end if
    end for
    if cm_aggregator.Timeslot = TRUE then
        Transmit aggregated data to base station
    end if
end for
```

All the nodes start with initial power. It's impossible that sensor nodes recharge energy and replace battery in ubiquitous sensor networks. Thus, it's very important that sensor nodes expense energy efficiently. To calculate the whole energy consumption of the networks, we have to consider two parts. One is quantity of energy as roles of sensor nodes. Another is a volume of energy when role of sensor nodes is exchange. There is a significant disparity of energy consumption between cluster heads and member nodes. All member nodes are transmitting perceived data to cluster head on allocated time slot periodically. And then cluster head transmit data aggregated in the cluster.

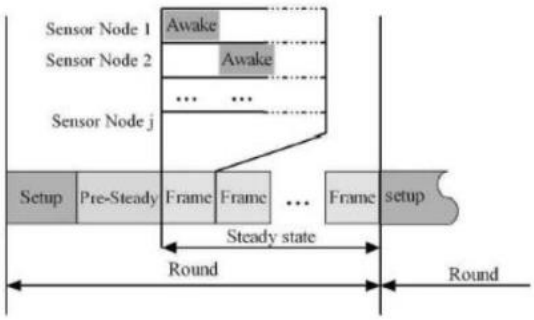

Fig.4. One round of Enhanced LEACH operation.

Enhanced LEACH which improves the energy distribution between sensor nodes in each round and prolong the network lifetime as shown in Fig.4. The implementation process of Enhanced LEACH is divided into rounds and each round is divided into three phases,1) Setup phase, 2)Pre-Steady phase and 3) Steady State phase; each sensor knows when each round starts using a synchronized clock. Setup –Phase: IN cluster each node creates a random number with the probability p, each node has the random probability (p) at the each round, and the next round it will creates another probability. Each node generates a random probability (p) at the beginning of a new round and computes the threshold value (T(n)) with the use of equation (1). If r=1 (i.e. the first round), let EMAX of all nodes be 1. In case of P < PT, the node is selected as a cluster head. A selected cluster head broadcasts an advertisement message over neighbor nodes. The neighbor nodes collect advertised message during a given time

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 6, June 2017

interval and then send a "join REQ" message to the nearest cluster head. The cluster head receives the "join-REQ" message and builds a cluster member list schedule. The member node receives and save the message for data transfer.

Pre-State phase: The main idea of this phase is to calculate the cluster Workload (which include aggregates the sensed data from cluster members and send the aggregated data to the base station) in one frame, then try to elect cluster member node that can handle the aggregation processes through all frames in the round. If not exist such a node, try to elect cluster member nodes that can handle the aggregation processes for each one frame in the round and the cluster head will handle the aggregation process for frames that there are no aggregator nodes for them. Steady State Phase: IN Steady State phase, the operation is divided into frames, in each frame; cluster member nodes send their data to the aggregation node Aggregator according to their time slots. The aggregation node must keep its receiver on to receive all the data from the nodes in the cluster. When all the data has been received, the aggregation node sends it to the base station after performs data aggregation. Cluster head maintains the received information of member nodes. The member nodes will have all the data in the form of TDMA table sent by sink node.

III. CONCLUSION

In this paper, the data transmission issues and the security issues in CWSNs. 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]T. Hara, V.I. Zadorozhny, and E. Buchmann, Wireless SensorNetwork Technologies for the Information Explosion Era, Studies inComputational Intelligence, vol. 278. Springer-Verlag, 2010.
[2]Y. Wang, G. Attebury, and B. Ramamurthy, "A Survey of SecurityIssues in Wireless Sensor Networks," IEEE Comm. Surveys &Tutorials, vol. 8, no. 2, pp. 2-23, Second Quarter 2006.
[3]A.A. Abbasi and M. Younis, "A Survey on Clustering Algorithmsfor Wireless Sensor Networks," Computer Comm., vol. 30, nos. 14/15, pp. 2826-2841, 2007.
[4]W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "AnApplication-Specific Protocol Architecture for Wireless MicrosensorNetworks," IEEE Trans. Wireless Comm., vol. 1, no. 4, pp. 660-670, Oct. 2002.
[5]A. Manjeshwar, Q.-A. Zeng, and D.P. Agrawal, "An AnalyticalModel for Information Retrieval in Wireless Sensor NetworksUsing Enhanced APTEEN Protocol," IEEE Trans. Parallel &Distributed Systems, vol. 13, no. 12, pp. 1290-1302, Dec. 2002.
[6]S. Yi et al., "PEACH: Power-Efficient and Adaptive Clustering Hierarchy Protocol for Wireless Sensor Networks," ComputerComm., vol. 30, nos. 14/15, pp. 2842-2852, 2007.
[7]K. Pradeepa, W.R. Anne, and S. Duraisamy, "Design andImplementation Issues of Clustering in Wireless Sensor Networks,"Int'l J. Computer Applications, vol. 47, no. 11, pp. 23-28,2012.
[8]L.B. Oliveira et al., "SecLEACH-On the Security of Clustered Sensor Networks," Signal Processing, 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,"Proc. IEEE Sixth Int'l Symp. Network Computing and Applications(NCA), pp. 145-152, 2007.
[10]K. Zhang, C. Wang, and C. Wang, "A Secure Routing Protocol forCluster-Based Wireless Sensor Networks Using Group KeyManagement," Proc. Fourth Int'l Conf. Wireless Comm., Networkingand Mobile Computing (WiCOM), pp. 1-5, 2008.
[11]S. Sharma and S.K. Jena, "A Survey on Secure HierarchicalRouting Protocols in Wireless Sensor Networks," Proc. Int'l Conf.Comm., Computing & Security (ICCCS), pp. 146-151, 2011.
[12]G. Gaubatz et al., "State of the Art in Ultra-Low Power Public KeyCryptography for Wireless Sensor Networks," Proc. IEEE ThirdInt'l Conf. Pervasive Computing and Comm. Workshops (PerCom),pp. 146-150, 2005.
[13]W. Diffie and M. Hellman, "New Directions in Cryptography,"IEEE Trans. Information Theory, vol. IT-22, no. 6, pp. 644-654, Nov.1976.
[14]14. A. Shamir, "Identity-Based Cryptosystems and Signature Schemes," Proc. Advances in Cryptology (CRYPTO), pp. 47-53,1985.
[15]D.W. Carman, "New Directions in Sensor Network Key Management,"Int'l J. Distributed Sensor Networks, vol. 1, pp. 3-15, 2005.
[16]R. 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. 882-889, 2010.