IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 19, Issue 4, Ver. IV. (Jul.-Aug. 2017), PP 61-67
www.iosrjournals.org

An Efficient Data Transmission in Cluster-Based Wireless Sensor Networks by using Advanced LEACH and SET Protocols

*Prasanthi Mula[1], Dr.Ch.V.Narayana[2]
[1]M.Tech.IV SEM (CSE) Lakireddy Balireddy College of Engineering, Mylavaram
[2]Professor, CSE Department, Lakireddy Balireddy College of Engineering, Mylavaram
*Corresponding Author: *Prasanthi Mula*

Abstract: *Wireless Sensor Networks (WSN) plays vital role in exploration field. Due to its immediately increasing utilization in monitoring various kinds of environment by appreciate physical phenomenon. Clustering is an adequate and compelling method to enhance conduct of the WSNs system. In this printed material, we think about a protected transportation of information for group based WSNs, where the batch are formed dynamically and anyway. We nominate two Secure and Efficient data Transmission protocols for CWSNs, called SET-IBS and SET-IBOOS, by using the Identity-Based digital Signature and the Identity-Based Online/Offline digital Signature respectively. The Leach protocol is treated and improved. In SET-IBS, security relies on the adherence of the Diffie-Hellman problem in the combine area. SET-IBOOS additionally decreases the computational operating cost for protocol security, which is critical for WSNs, while its defence depends on the cohesion of the problem of distinct logarithm We propose a novel approach for choosing group head utilizing the idea remaining vitality in Enhanced LEACH, Which extends LEACH contract by balancing the energy consumption in the network. The reproduction results show that Enhanced LEACH outperforms LEACH in terms of network system lifetime and reduce the energy expenditure.*

Keywords*: Wireless Sensor Network (WSN), Cluster Head (CH),Base Station (BS), Network life time. SET-IBS, SET-IBOOS, LEACH.*

Date of Submission: 12-07-2017 Date of acceptance: 05-08-2017

I. Introduction

Wireless sensor network (WSN) is a systems of network compose of spatially distributed apparatus using wireless sensor nodes to examine environmental or physical conditions, such as temperature, sound and evolution. The particular nodes are capable of sensing their environments; convert the information census in the vicinity, and mailing data to one or more collection points in a WSN. Efficient transportation of data is one of the most compelling issues for WSNs. Usually many WSNs are installed in covertly; harsh and often antagonistic physical environments for definite applications, such as armed forces sphere and appreciate tasks with deceptive surroundings. Efficient and protected transmission of data is thus very imperative and is appropriate in many such realistic WSNs. Cluster based conveyance of data in WSNs, has been inspected by researchers in order to achieve the network scrabbled and control, which augment node life span and reduces high frequency utilization by using local assistance between sensor nodes. In a cluster-based WSN (CWSN), each assemblage has a leader sensor node, known as cluster head (CH). A CH collects the data concentrated by the leaf nodes (non- CH sensor nodes) in its cluster, and sends the pooled data to the base station (BS).The expectation of the asymmetric key executive has been announce in WSNs in recent times, which compensates the defect from relating the symmetric key management for security. Digital trademark is one of the most significant security services conferred by cryptography in asymmetric key management systems, where the conclusive between the public key and the recognition of the signer is collected via a digital certificate. The Identity-Based digital Signature (IBS) scheme, based on the intricacy of factoring everything from Identity-Based Cryptography (IBC), is to establish an entity's public key from its character information, e.g., from its description number or its name. This states that security must beset every phase of the design of a wireless sensor network utilization that will require a high concentration of security. Probable utilization comprise monitoring detached or hostile locations, objective tracking in combat zone, catastrophe liberation networks, premature fire recognition, and environmental control. A primary topic that must be addressed when using cluster-based security protocols based on proportional session keys is the means used for determine the session keys in the primary place. A vital design burden for security protocols based on proportional keys is the degree of session key among the nodes in the organization. On the other hand, it has the clear security deficiency that the negotiation of a single node will disclose the global key. A wireless sensor network (WSN) generally subsists of a base station (or "gateway") that can communicate with a number of wireless sensors via a radio link. Data is confident at the wireless sensor node, constrict, and address to the gateway precisely or, if appropriate, uses other wireless sensor nodes to leading data to the gateway. The transmitted data is then conferred to the system by the gateway connection. The aspiration of this chapter is to arrange a brief technical introduction to wireless sensor networks and begun a few applications in which wireless sensor networks are permissive. A WSN usually subsist of tens to thousands of such nodes that disclose through wireless channels for intelligence sharing and cooperative convert. WSNs can be expand on a global scale for environmental observe and habitat study, over a battle field for combatant surveillance and reconnaissance, in appearing environments for search and delivery, in factories for condition based conservation, in buildings for framework health monitoring, in homes to realize agile homes, or even in bodies for patient monitoring. After the initial deployment (typically ad hoc), sensor nodes are important for self-organizing an applicable network framework, often with multi-hop Connection between sensor nodes. The onboard sensors then start assemble acoustic, seismic, infrared or seductive Information about the environment, using either continuous or action driven working modes as shown in Fig.1

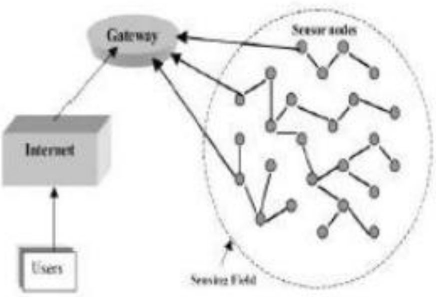


Fig.1. Architecture of WSN.

II. Research Elaborations

L.B. Jivanadhametal. proposed formation of a Secured Cluster-based architecture for a Dynamic Wireless Sensor Network that administer two topology authority procedures: node-move-in and node-move-out. The prepared security protocol assimilate one round Zero Knowledge Proof and AES algorithm to relate for bud authentication, wherever only authenticated bud will be acknowledged through node move-in operation. In addition they interpreted that, it needs O(h+q) rounds for a node to connect into a network securely, where h is the height of the aggressive cluster-based wireless sensor network and q is the number of adjoining nodes of a joining node. After the O(h+q) endeavour to join the network, the node is considered as afraid and is eventually deserted from accompany the network as in [2]. HichemSedjelmaciet.al expected an intrusion disclosure framework for a cluster-based WSN (CWSN) that design to merge the advantage of aberration and signature detection which are high detection rate and low false confident, correspondingly.

Wireless sensor networks (WSNs) have a excessive possible to be used in vital circumstances like armed forces and monetary function. On the other hand, these function are mostly frequently to be expand in hostile surroundings, where nodes and conversation are smart targets to intruders. This makes WSNs affected to a range of achievable attacks. Because of their attribute, reactionary security methods are not applicable. So here the authors have expected an intrusion detection groundwork for a cluster-based WSN (CWSN) that aims to merge the convenience of signature detection and aberration which are high disclosure rate and low false positive, correspondingly as in [2][3]. M.Younis Abdullah et al in approved the problem of guarantee addition to cluster based communication agreement for homogeneous wireless sensor networks consist of sensor nodes with very limited resources, and expected a security settlement where clusters are created annually and dynamically. Their comment depicts re-keying function agreement for wireless sensor networks security. They have estimate the local legislative functions as master function, ancestry function and rekeying function is engrave with sensor node. A security and achievement study proven that it is very competent in communication, storage, estimation and this approach is very successful in contend against a lot of convoluted attacks [4] Tingyao Jiang et.al presented a new dynamic imposition detection approach for cluster-based wireless sensor networks(CWSN). The nodes in a wireless sensor network are massed into clusters build upon the appropriate relationships with a cluster head (CH) in every cluster. The estimate scheme initially makes use of a clustering algorithm to compose a model of accepted traffic attitude, and then uses this model of accepted traffic to detect atypical traffic patterns. Along with the diverse network setting of clusters, this method might also dynamically set different exposure factors for different clusters to conclude a more proper exposure algorithm. The achievement study showed that the projected intrusion disclosure method can progress the detection efficiency and decrease the false conclusive rate, and is exceedingly efficient of the intensity conservation as in [5]. Nikolaos A. Pantaziset.al conferred a classification of energy adequate routing protocols and enlarges the classification originally done by Al-Kariki to better construe which issues/operations in each agreement illustrate/enhance the energy capability issues. The distributed demeanor and aggressive topology of Wireless Sensor Networks (WSNs)brings in many unusual compulsion in routing protocols that should be satisfied. The main important condition of a routing covenant, so as to be productive for WSNs, is the energy usage and the expansion of the network's life span. During the past few years, a lot of energy adequate routing agreement have been estimate for WSNs. The authors here conferred the four types of arrangement of energy adequate routing protocols: Network Structure, Communication Model, Topology Based and Reliable Routing. The routing protocols which belong to the first type can be additionally restricted as hierarchical or flat. The routing protocols acceptance to the second type can be additionally restricted as Query-based or Coherent and non-coherent based or Negotiation-based. The routing protocols acceptance to the third type can be also confidential as Location-based or Mobile Agent based. The routing protocols acceptance to the fourth type can be also classified as QoS-based or Multipath based. Lastly, a methodical review on energy adequate routing protocols for WSNs is arrange as in [5].planned for flat wireless sensor networks, which are not applicable for cluster-based wireless sensor networks (like LEACH). Here Kun Zhang et.al considered adding guarantee to cluster based routing protocols for wireless sensor networks which subsist of sensor nodes with very deficient resources, and have proposed a guarantee solution for LEACH which is a agreement in which the clusters are created repeatedly and dynamically. The solution expected by authors makes use of appreciate Random Pair-wise Keys (RPK) method, an advance security method that depends on balanced key methods and is a lightweight and preserve the heart of the original LEACH contract. Simulations determine that security of RLEACH has been appreciate, with contraction in energy discharge and very less performing cost as in [6][7]. In Wireless Sensor Networks (WSNs), a crucial security essential is verification to evade attacks against protected Communication, and to decline DoS attacks appropriate the limited assets of sensor nodes[3]. Resource constraint of sensor nodes are major adversity in implement strong public key cryptographic based mechanisms in WSNs. To deal with the complication of substantiate in WSNs, Yasmin, R et.al have expected secure and adequate framework for substantiate broadcast/multicast by sensor nodes and for outside user authentication, which uses existence based cryptography and online/offline signature design[1][8]. The most important aspiration of this framework are to allow all sensor nodes in the network, originally, to broadcast and/or multicast an substantiate message rapidly; secondly, to approve the broadcast/multicast message sender and the message capacity; and lastly, to confirm the accuracy of an outside user. The projected framework is also appraise by means of the most secure and adequate identity-based signature (IBS)schemes as in[1][7]. A secure routing for cluster-based sensor networks is where assemblage are formed repeatedly and dynamically. Together with the analysis of ID-based cryptography for security in WSNs, Huang Lu et.al expected anew secure routing protocol with ID-based stamp scheme for cluster-based WSNs within which the security is reliant on the firmness of the Diffie-Hellman problem in the arbitrary oracle model. Here the defect in the secure routing agreement with symmetric key combine is pointed out by authors. Because of the connection operating cost for security, authors provide simulation analysis results in details to determine how various criterion act among energy adaptability and security as in [1][9]. A process by which data is possessed and sent from sensor nodes to the base station is known as data gathering. It is completed via some sensor nodes called aggregators. A key role is played by security in data aggregation procedure to make sure confidence and privacy of aggregated data., In [9] Nguyen Xuan Quyet.al proposed a data gathering method for cluster-based WSN that advance the security against attackers. This method was based on increased homomorphism public key in creation which presents continued elimination of and supports hop-to-hop evidence. The logical investigation and union demonstrate that this access has both lower competition and better security achievement as compared to other approaches as in [9].

Leach protocol:

In this paper, we do not consider any prior ability about the data indeed in many operations; raw data may not be easily classify into different types. To conduct the collected data to a inaccessible location is also considered valuable because the total possessed data may be in a very large abundance. To simplify data query. The operation of LEACH is split into rounds. Each round begins with a setup aspect when the clusters are coordinated, followed by a Steady-state phase when data are conveyed from the nodes to the array head and on to the Base Station (BS). The LEACH organization has two phases: Set-up phase: The preferred CH informs about its choosing as CH among the group. Non cluster-head nodes determine their cluster for current round by choosing the CH that desire minimum connection energy, based on the accepted signal strength of the announcement from each CH. After the selection each non-CH informs the CH by address a join request informations (Join-REQ) back to the CH. Then the CH node sets up and performance a TDMA schedule to all member non-CH nodes. Steady State Phase: The Steady Sate Phase is injured into many frames, in which growth can send their data to the CH at most once per time slot. CH sends the accumulate data to BS in single hop manner. The LEACH administer better results related to earlier existing custom e.g. direct link protocol, minimum- transmission-energy protocol and static round up protocol in Wireless Sensor Network. The accessible redundant information is finally cancelled during aggregate process behave by CH. Then the CH will broadcast an announcement message to inform all others that it is the new cluster-head. The nodes send the join-request message accommodate their IDs by using CSMA (carrier sensing multiple access) to join a cluster. The node joins that cluster from which they received actives strength signal. After that, each CH knows its own cluster representative information. Based on the information, the CH creates TDMA chart table and broadcasts it to the cluster associate. So all the member nodes know their idle slots, and then the steady-state phase begins. The cluster established protocols (like LEACH) which are the data conveyance protocols for WSNs, are impressionable to many security attacks. In general, the aggression to Cluster Heads in CWSNs can produce deliberate harm to the network, since cover attacks. Data aggregation and data transportation rely on the CHs primarily. If an attacke manages to act as if it's a CH or agree the CH, it can incite intervention such as select forwarding attacks and sinkhole, thus annoying the network. by choice an attacker may mean to insert false appreciate data into the WSN, like cheating as a leaf node transferring false information to the CHs. However, LEACH like protocols are extra tough against insider charge rather than other types of protocols in WSNs as shown in Fig.2.

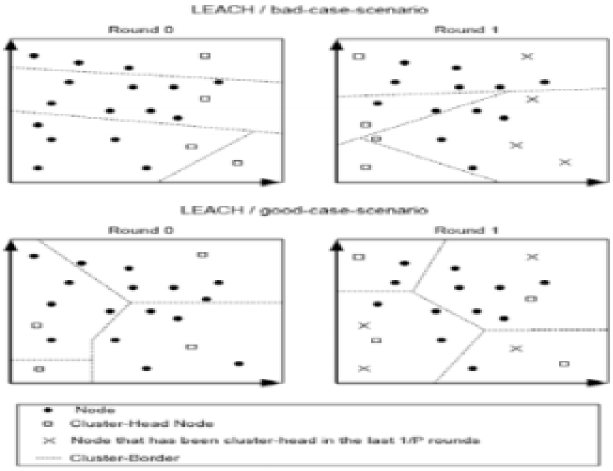

LEACH / bad-case-scenario
Round 0
Round 1
LEACH / good-case-scenario
Round 0
Round 1
Node
Cluster-Head Node
Node that has been cluster-head in the last 1/P rounds
Cluster-Border

Fig.2.Example of LEACH Network.

Since CHs are revolve from nodes to nodes in the network by rounds creating it harder for types of protocols in WSNs. The goal of the expected secure data communication for CWSNs is to guarantee a secure and energetic data transmission between leaf nodes and CHs, as well as communication between CHs and the BS. concurrently, most of existing secure conveyance protocols for CWSNs in the composition, however, apply the article key management for security, which endure from the orphan node complication that is imported, In this paper, we aim to solve this founding node problem by using the ID-based crypto-system that assurance security requirements, and introduce SET-IBS by using the IBS scheme. Furthermore, SET-IBOOS is scheduled to reduce the computational upwards 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 below figure3. We suppose that, all sensor nodes know the starting and ending time of each round, because of the time synchronization.

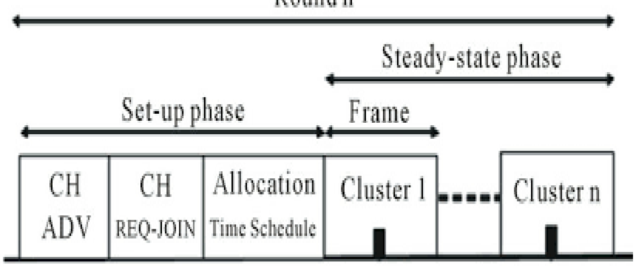


Fig3. Set protocol operation phases.

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 conduct data from sensor nodes to the BS. In each round, the schedule is divided into ensuing time slots by the TDMA (time Division multiple access) control. Sensor nodes transfer the sensed data to the CHs in each frame of the steady state phase. For fair energy expenditure, nodes are randomly selected as CHs in each round, and other non-CH sensor nodes join clusters using one-hop transmission, bank on the highest accepted signal strength of CHs. In order to elect CHs in a new round, each sensor node completes a random number and analyze it with a threshold. If the value is less than the entrance, the sensor node develops into 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 compromise, therefore, SET-IBS functions without data transmission with each other in the CH circle. 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 trademark bearing. Whereas, in the Steady state phase, the time-stamp Ti is used for the signature generation securing the inner array publicity, and Ts is used for the signature generation attaining the CHs-to-BS data transportational. The expected SET-IBOOS operates equivalently to that of SET-IBS. SET-IBOOS works in rounds all the while communication, and the self-elected CHs are determined based on their local opinion, thus it functions without data transmission in the CH rotations. For the IBOOS key administration in SET-IBOOS, the offline signatures are develop by the CHs, which are used for the online clue at the leaf nodes-build up leach is a T-LEACH stands for doorstep-based LEACH because it change cluster heads based on the threshold value of continuing energy on the sensor nodes. In traditional obligation relating to cluster development, the authors expected that the number of cluster heads be decreased to decrease energy expenditure or that energy capability based optimal cluster sizes be compose to extend the endurance time of the network. LEACH algorithm has a arrangement where cluster heads are preferred best probabilistic values and the compilation and transmission of directive occur during each round. therefore, the number of cluster heads and intimately compass periods come to be closely related to energy expenditure. In these algorithms, nodes play the roles of cluster heads annually, and these are not inspecting energy cost of that time. When conflicting sensor nodes become array heads through the performance of rounds, nodes selected as cluster heads must broadcast to representative nodes of the clusters to which they belong that they have become cluster heads. In direct to as the frequency of distribute and of cluster head recovery increases, energy consumption improvement due to message transportation for broadcasting. All the nodes start with initial power. It’s inaccessible that sensor nodes recharge energy and recover battery in everywhere sensor networks. Thus, it’s very imperative that sensor nodes expenditure energy comfortably. To calculate the whole intensity expenditure of the networks, we have to consider two parts. One is capacity of energy as appearance of sensor nodes. Another is a quantity of energy when role of sensor nodes is change. There is a important difference of energy utilization between cluster highest and member nodes. All member nodes are broadcast anticipated data to cluster head on appropriate time slot periodically. And then cluster head transmit data assemble in the cluster.

III. Cluster Network Model

In Cluster Network; subsist of large number of Sensor Nodes (SN) are arrange into different clusters. Each Cluster is confident of one Cluster Head (CH) sensor node which is voted in autonomously and cluster member nodes or leaf (non CH). Leaf (non CH), join a cluster build upon on the receiving signal strength. The Cluster Head (CH) gets the anticipate data from the leaf (non CH), aggregates the sensed instruction and then sends it to the base station. Clustred Architecture:

- Organizes the sensor nodes into clusters
- Each cluster is governed by a cluster- head
- Only heads send messages to a BS
- Suitable for data fusion
- Self-organizing

SET Protocol: -

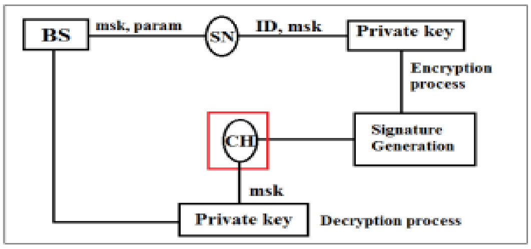
The goal of the expected secure data transmission for CWSNs is to assurance a secure and efficient data transmission between leaf nodes and CHs, as well as communication between CHs and the BS. for now, most of actual secure transmission protocols for CWSNs in the composition, however, apply the balanced key management for security, which suffers from the orphan node complication that is popularized, In this paper, we aim to solve this orphan node problem by using the ID-based crypto-arrangement that guarantees security concern , and propose SET-IBS by using the IBS scheme. Furthermore, SET-IBOOS is prospective to reduce the computational overhead in SET-IBS with the IBOOS design. 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 achieve in rounds during communication, which consists of a composition phase and a Steady-state phase in each round. We introduce the protocol initialization; characterize the key management of the protocol by using the IBS scheme, and the protocol activity afterwards.

IBS Scheme:

IBS is based on IBS scheme aspect. It has four aspect like setup at the BS, key extraction, signature signing and verification. 1. Setup at the BS: The BS generates master key (msk) and public guideline (param) and broadcast these to all sensor nodes in the network. 2. Key extraction: Sensor nodes develop private key by using ID of the node and master key (msk) transmitted by the base station. 3. Signing of signature: Signature (sign) is created by using a time-stamp (t), signing key (??) and message (M). 4. Verification of the data receiving nodes: Verification is done at the receiving nodes by using the digital signature (sign), ID of the node and message (M). the receiving node accepts the message (M) if sign is legal, otherwise rejects the message (M).

Workflow of SET-IBS Protocol:

SET-IBS depends on ID-based cryptography in which depiction of the hub (ID) is utilized as their open key and private key can be incite without assistant information transmission. It makes computerized signature and connect this centralized server mark to the detected uncorrupted information. This procedure is done at the mailing hub. At recipient, hub utilizes open key to unscramble the transmitted message. At that point hub test the adequacy of the computerized mark of acknowledged the message. On the off chance that the computerized mark is legitimate it acknowledges the message and transmit to base station (BS). On the off chance that the computerized mark is invalid, it demonstrates that the transmitted message is changed or adjusted. At that point it dismiss that message and advise sending hub to gathered that message once more.



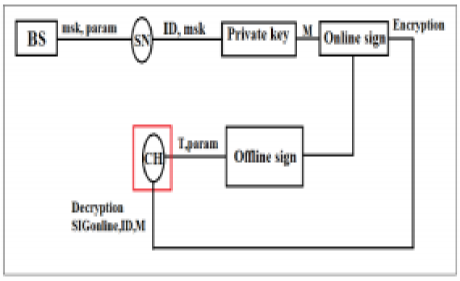
Workflow of SET-IBS protocol

IBOOS Scheme:

An IBOOS scheme has five phases. IBOOS scheme is similar to IBS scheme. In IBOOS scheme signature is generated in two phases. Those are online signature and offline signature. The IBOOS scheme has five phases those are: 1. Setup at the BS: The BS generates master key (msk) and public parameters (param) similar to IBS scheme. 2. Key extraction: Sensor nodes generates private key by using ID of the node and master key (msk) transmitted by the base station. 3. Offline signing: Offline signing (offline sign) is done at the receiver node by using given parameters and time stamp (t).The cluster head transmit offline sign to leaf node. 4. Online signing: Online signature (online sign) is generated at sending node by using private key, offline sign and message (M). 5. Verification: Verification is done at the receiving nodes by using the digital signature (sign), ID of the node and message (M). the receiving node accepts the message (M) if sign is legal, otherwise rejects the message (M).

Workflow of SET-IBOOS Protocol:

SET-IBOOS is proposed to limit the computational overhead and to enhance the execution of the system. Working of IBOOS is like IBS convention. In IBOOS convention to lessen computational overhead, signature marking is isolated into two stages. i.e. on the web and disconnected. Disconnected marking is done at the recipient before message has been known. Preferred standpoint disconnected sign is it can be performed effortlessly. By utilizing this disconnected sign online mark is produced at sender hub. Online sign is figured after message is known. This procedure is significantly quicker than the IBS convention.



Workflow of IBOOS protocol

IV. Conclusion

In this paper, the information transmission issues and the security issues in CWSNs. We at that point introduced two secure and proficient information transmission conventions separately for CWSNs, SET-IBS and SET-IBOOS. In the assessment segment, we gave practicality of the proposed SET-IBS and SET-IBOOS as for the security prerequisites and examination against directing assaults. SET-IBS and SETIBOOS are proficient in correspondence and applying the ID based crypto-framework, which accomplishes security prerequisites in CWSNs, and in addition tackled the vagrant hub issue in the safe transmission conventions with the symmetric key administration. Finally, the correlation in the estimation and reproduction comes about demonstrate that, the proposed SET-IBS and SET-IBOOS conventions have preferable execution over existing secure conventions for CWSNs. Regarding both calculation and correspondence costs, we brought up the benefits that utilizing SET-IBOOS with less helper security overhead is favoured for secure information transmission in CWSNs. In future, we are wanting to propose the comparative sort of answers for the decentralized remote sensor situations.

References

[1]. Huang Lu, Student Member, IEEE, Jie Li, Senior Member, IEEE, and Mohsen Guizani, Fellow, IEEE, “Secure and Efficient Data Transmission for Cluster-Based Wireless Sensor Networks”, IEEE Transactions on Parallel and Distributed Systems, Vol. 25, No. 3, March 2014.

[2]. 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.

[3]. 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.

[4]. A.A. Abbasi and M. Younis, “A Survey on Clustering Algorithms for Wireless Sensor Networks,” Computer Comm., vol. 30, nos. 14/ 15, pp. 2826-2841, 2007.

[5]. W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, “An Application-Specific Protocol Architecture for Wireless Micro-sensor Networks,” IEEE Trans. Wireless Comm., vol. 1, no. 4, pp. 660-670, Oct. 2002.

[6]. 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 & Distributed Systems, vol. 13, no. 12, pp. 1290-1302, Dec. 2002.

[7]. S. Yi 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.

[8]. K. Pradeepa, W.R. Anne, and S. Duraisamy, “Design and Implementation Issues of Clustering in Wireless Sensor Networks,” Int’l J. Computer Applications, vol. 47, no. 11, pp. 23-28, 2012.

[9]. L.B. Oliveira et al., “SecLEACH-On the Security of Clustered Sensor Networks,” Signal Processing, vol. 87, pp. 2882-2895, 2007.

IOSR Journal of Computer Engineering (IOSR-JCE) is UGC approved Journal with Sl. No. 5019, Journal no. 49102.

*Prasanthi Mula. "An Efficient Data Transmission in Cluster-Based Wireless Sensor Networks by using Advanced LEACH and SET Protocols." IOSR Journal of Computer Engineering (IOSR-JCE) 19.4 (2017): 61-67.