International Journal of Multidisciplinary Approach and Studies

ISSN NO:: 2348 – 537X

Cryptography and Efficient Data Transmission for Cluster-Based Wireless Sensor Networks

Sr. S. Jothi* & Sr. Avila Therese**

**Assistant Professor, Department of Computer Science, Jayaraj Annapackiam College for Women, Periyakulam*

***Assistant Professor, Department of Computer Science and Engineering, St. Anne's College of Engineering and Technology, Panruti*

ABSTRACT

Identifying effective data transmission is a critical issue for wireless sensor networks (WSNs). Clustering has been proved recently to be an effective and practical means of enhancing the system performance of WSNS. The present study focuses on securing the right kind data of transmission for cluster based WSNs (CWSNs), where the clusters are formed dynamically and periodically. There are two secure and efficient data transmission (SET) protocols for CWSNS. The schemes are called SET-IBS, Identity Based Digital Signature, and SET-IBOOs, Identity Based online / offline digital signature (IBOOS). In SET-IBS, security relies on the hardness of the Diffie-Hellman problem in the pairing domain. In SET-IBOOS further reduces the computational overhead for protocol security, which is crucial for WSNs, while its security relies on the hardness of the discrete logarithm problem. SET-IBS and SET-IBOOS protocols with respect to the security requirements and security analysis against various attacks are found feasible. The calculations and simulations are provided to illustrate the efficiency of the proposed protocols. The results show that, the proposed protocols have better performance than the existing secure protocols for CWSNs, in terms of security overhead and energy consumption. Keywords: Wireless Sensor Networks; Cluster-based WSNs; Identity-based digital signature; Identity-based online/offline digital signature.

I. INTRODUCTION

Data security and storage has become very important issue in Sensor networks for future information retrieval. Storage nodes serve as an intermediate tier between sensors and a sink for storing data and processing queries in wireless sensor networks. The importance of storage nodes also makes them attractive to attackers. Data Storage is happens via the Forwarding nodes and Storage nodes. Storage nodes are introduced in this paper to store collected date from the sensors in their proximities, it reduce the energy cost and communication cost induced by network query.

Aim of the research is to deploy the storage nodes and secure data transmission for cluster-based WSNs (CWSNs), where the clusters are formed dynamically and periodically. There are 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. A clustering routing protocol named Enhanced LEACH is proposed in this paper, which extend LEACH protocol by balancing the energy consumption in the network. The simulation results show that Enhanced LEACH outperforms LEACH in terms of network lifetime and power consumption minimization.

II. LITERATURE SURVEY

[1] 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; Clustering is a critical task in Wireless Sensor Networks for energy efficiency and network stability. In the existing method, a secure data transmission for cluster-based WSNs is presented in which the clusters are formed in a dynamic and periodic manner. A two secure and efficient data transmission protocols for CWSNs is presented which is 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. But the drawback in the existing method is there may lead to leakage of user's public key and secret key in the case of compromised users in the SET-IBS protocol and SET-IBOOS protocol is only efficient for the devices with high computational power. So, in order to overcome this problem an innovative technique is introduced which is called Enhanced Secure Data Transmission protocol which is used to improve the SE - IBS and SET - IBOOS protocol. In the improved SET-IBS protocol, to enhance the security a new secret key is created by using the master secret key for every identity. Also, to confuse the attackers, encapsulation algorithm is used. In this process, the two cipher texts are used: one is valid cipher text and another one is invalid cipher text. These cipher texts are encapsulated with the corresponding author's encapsulated key. In order to improve the efficiency in the SET-IBOOS protocol, the improved SET- BOOS protocol is proposed in which the online/offline attribute based encryption method is used. An experimental result shows that proposed method achieves high efficiency and high security.

[2] L.B. Oliveira et al., "SecLEACH-On the Security of Clustered Sensor Networks", Key management in wireless sensor network is a complex task due to its nature of environment. Wireless sensor network comprise of large number of sensor nodes with different hardware abilities and functions. Due to the limited memory resources and energy constraints, complex security algorithms cannot be used in sensor networks. Therefore, an energy efficient key management scheme is necessary to mitigate the security risks.

[3] W. Diffie and M. Hellman, "New Directions in Cryptography," Two kinds of contemporary developments in Cryptography are examined. Widening applications of teleprocessing have given rise to a need for new types of cryptographic systems, which minimize the need for secure key distribution channels and supply the equivalent of a written signature. This paper suggests ways to solve these currently open problems. It also discusses how the theories of communication and computation are beginning to provide the tools to solve cryptographic problems of long standing.

[4] D.W. Carman, "New Directions in Sensor Network Key Management," Secure data transmission network is a decisive issue for wireless technology networks (WTNs). Clustering is an effective and practical way to enhance the system performance & methods of WTNs.

III. WIRELESS SENSOR NETWORK

Wireless sensor network is ad-hoc network. It consists of small light weighted wireless nodes called sensor nodes, deployed in physical or environmental condition. All sensor nodes in the wireless sensor network are interacting with each other or by intermediate sensor nodes. A sensor nodes that generates data, based on its sensing mechanisms observation and transmit sensed data packet to the base station (sink). This process basically direct transmission since the base station may locate very far away from sensor nodes needs. More energy to transmit data over long distances so that a better technique is to have fewer nodes sends data to the base station. These nodes called aggregator nodes and processes called data aggregation in wireless sensor network.

a) Clustering in WSN

Group of sensor node can be combined or compress data together and transmit only compact data. This can reduce localized traffic in individual group and also reduce global data. This grouping process of sensor nodes in a densely deployed large scale sensor node is Target User Sensor node Sensor field Internet BS known as clustering.

b) Data Aggregation in WSN

The way of combing data and compress data belonging to a single cluster called data fusion (aggregation). The aim of data aggregation is that eliminates redundant data transmission and enhances the lifetime of energy in wireless sensor network.

i. Performance measure of data aggregation

The performance measures of data fusion algorithm are highly dependent on the desired application. In the data-aggregation scheme, every sensor nodes should have spent the same amount of energy in every data gathering round. Network lifetime, data accuracy, and latency are some of the significant performance measures of data-aggregation algorithms.

ii. Impact of data aggregation in wireless sensor network

In this paper we discuss the two main factors that affect the performance of data aggregation methods in wireless sensor network, such as energy saving and delay. Data aggregation is the process, in which aggregating the data packet coming from the different sources; the number of transmission is reduced. With the help of this process we can save the energy in the network. Delay is the latency connected with aggregation data from closer sources may have to held back at intermediate nodes in order to combine them with data from source that are farther away.

c) LEACH PROTOCOL

LEACH protocol is difficult to attack as compared to the more conventional multi hop protocols. In the conventional multi-hop protocols, the nodes around the base station are more attractive to compromise. Whereas in LEACH, the CHs are the only node that directly communicate with the base station. The location of these CHs can be anywhere in the network irrespective of the base station. And more over the CHs are periodically randomly changed. So spotting these CHs is very difficult for the adversary.

However, because it is a cluster-based protocol, relying fundamentally on the CHs for data aggregation and routing, attacks involving CHs are the most damaging. If any adversary nodes become a CH, then it can facilitate attacks like Sybil attack, HELLO good attack and selective forwarding. The intruder can broadcast a powerful advertisement to all the nodes in the network and hence, every node is likely to choose the adversary as the cluster-head. The adversary can then selectively forward information to the base-station or modify or dump it.

Key management is an effective method to improve network security. However, clusters in LEACH are formed dynamically (at random) and periodically, which changes interactions among the nodes and requires that any node needs to be ready to join any CH at any time.

d) SET-IBS and SET-IBOOS PROTOCOLS

In the proposed system, an innovative technique is introduced which is called Enhanced Secure Data Transmission protocol (ESDT) which is used to improve the SET-IBS and SET-IBOOS protocol. The goal of the proposed secure data transmission for CWSNs is to guarantee the secure and efficient data transmissions between leaf nodes and CHs, as well as transmission between CHs and the BS. Also, the computational complexity is an important concern.

i. Initialization of SET-IBS protocol.

Workflow of SET-IBS Protocol and its Operation Secure communication in SET-IBS relies on ID based cryptography in which user public keys are their ID information. Thus, users can obtain their corresponding private keys without auxiliary data transmission, which is efficient in communication and saves energy. Figure 6.1 illustrates the process of encryption and decryption using the keys generated. As shown in figure private key is generated from nodes ID and the mask (msk) function of Base station (BS). Similarly, public key is generated from msk function of CH. Using these keys security can be provided to the data.

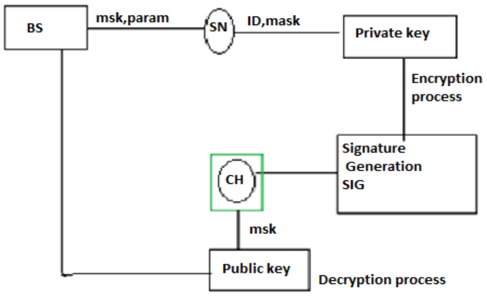


Figure 1: Workflow of SET-IBS protocol Workflow of SET-IBOOS and its Operation

Setup phase: In the protocol initialization the Base Station generates a master key *msk* and public parameter *param* for the generation of private key and sends them all to the sensor nodes.

Extraction process: Node j first obtains its private key from msk and where is its IDj, and is the time stamp of node j's time interval in the current round that is generated by its CH_i from the TDMA control.

Signature signing: The sensor node j picks a random number and computes. The sensor node further computes $\boldsymbol{c_j = h(C_j \mid t_j \mid \theta_j}$ **and** $\boldsymbol{\sigma_j = c_j\, sek_j + \alpha_j P}$**.** Where $<c_j, \sigma_j>$is the digital signature of node j on the encrypted message Cj. The broadcast message is now concatenated in the form of $<ID_j, t_j, C_j, \sigma_j, c_j>$.

Verification: Upon receiving the message, each sensor node verifies the authenticity in the following way. It checks the time stamp of current time interval and determines whether the received message is fresh. Then, if the time stamp is correct, the sensor node further computes $\boldsymbol{\theta_j = e\,(\,_,\, P)e(H(ID_j| \, t_j) \text{-} P_{pub)} c_j}$ using the time stamp of current time interval $\boldsymbol{t_{j.}}$ For authentication, which is equal to that in the received message, the sensor node considers the received message authentic, and propagates the message to the next hop or user. If the verification above fails, the sensor node considers the message as either bogus or a replaced one, even a mistaken one, and ignores it.

ii. Operation of SET-IBS protocol

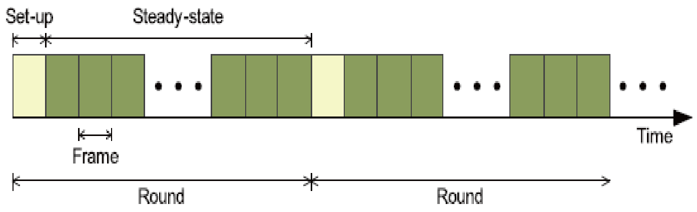


Figure 2 Operations of protocol

After the protocol initialization, SET-IBS operates in rounds during communication. 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 control. Sensor nodes transmit the sensed data to the CHs in each frame of the steady-state phase. For fair energy consumption, nodes are randomly elected 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 the setup phase, the time stamp T_s and node IDs are used for the signature generation. Whereas in the steady state phase, the time stamp t_j is used for the signature generation securing the inner cluster communications, and T_s is used for the signature generation securing the CHs to- BS data transmission.

iii. Initialization of SET-IBOOS protocol

SET-IBOOS is proposed in order to further reduce the computational overhead for security using the IBOOS scheme, in which security relies on the hardness of the discrete logarithmic problem. Private key is generated in similar way as that of IBS, Along with private key online signature is generated for encrypting the data. This online signature is obtained using offline signature. While decrypting the data online signature, sensor node ID and message M parameters.

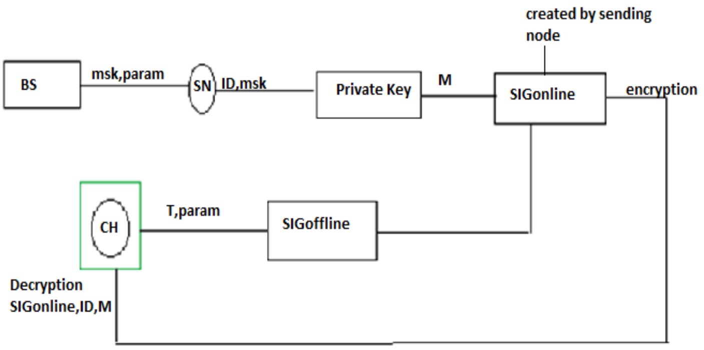


Figure 3 Workflow of IBOOS protocol

Setup phase: In the protocol initialization the Base Station generates a master key *msk* and public parameter *param* for the generation of private key and sends them all to the sensor nodes.

Extraction process: Before the signature process, node j first extracts the private key from the msk τ and its identity ID, as where

------(4)

$$R_j = g^{r_j}$$
$$s_j = r_j + H\left(R_j, ID_j\right)\tau mod\ q.$$

Offline signing: At the offline stage, node j generates the offline value $< \hat{\sigma}_j >$ with the time stamp of its time slot tj for transmission, and store the knowledge for signing online signature when it sends the message. Notice that, this offline signature can be done by the sensor node itself or by the trustful third party, for example, the CH sensor node. Let then

$$g^{s_j} = g^{r_j} g^{H\left(R_j,ID_j\right)\tau mod\ q} = R_j X^{H\left(R_j,ID_j\right) mod\ q}$$
$$\hat{\sigma}_j = g^{-t_j}$$

Online signing: At this stage, node j computes the online signature based on the encrypted data Cj and the offline signature $\hat{\sigma}_j$

$$h_j = H(C_j, ID_j)$$
$$z_j = \hat{\sigma}_j + h_j s_j mod\ q$$
$$\sigma_j = g^{\hat{\sigma}_j}$$

Then, node j sends the message to its destination with, and the online signature, in the form of $<ID_j, t_j, R, \sigma_j, z_j, c_j>$.

Verification process: Upon receiving the message, each sensor node verifies the authenticity in the following way. It checks the current time stamp tj or freshness. Then, if the time stamp is correct, the sensor node further computes the values of g^{z_j} and $\sigma_j R_j^{h_j} X^{h_j H(R_j, ID_j)} mod\ q,$ .If the values of and $\sigma_j R_j^{h_j} X^{h_j H(R_j, ID_j)} mod\ q,$, are equal from the received message, the node i considers the received message authentic, accepts it, and propagates the message to the next hop or user. If the verification above fails, the sensor node considers the message as either bogus or a replaced one, even a mistaken one, then rejects or ignores it.

iv. Operation of SET-IBS protocol

The proposed SET-IBOOS operates same as that of SET-IBS protocol. SET-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. However, the differences are that digital signature is changed from ID-based signature to the online signature of the IBOOS scheme. Once the setup phase is over, the system turns into the steady-state phase, in which

e) IMPROVED SET-IBS PROTOCOL

In the improved SET-IBS protocol, to enhance the security a new secret key is created by using the master secret key for every identity.

Setup phase: The setup algorithm takes as input a security parameter λ and produces the master public key mpk and the master secret key msk. The master public key defines an identity set ID, and an encapsulated-key set K. All other algorithms KeyGen, Encap, Decap, implicitly include mpk as an input.

Key generation: For any identity the KeyGen algorithm uses the master secret key msk to sample an identity secret key.

Valid Encapsulation: The valid encapsulation algorithm creates pairs (C, k) where C is a valid cipher text, and is the encapsulated-key.

Invalid Encapsulation: The alternative invalid encapsulation algorithm samples an invalid cipher text C for a given id.

Decapsulation: The decapsulation algorithm is deterministic, takes a cipher text C and an identity secret key and outputs the encapsulated key k.

f) IMPROVED SET-IBOOS PROTOCOL

To improve the efficiency in the SET-IBOOS protocol, the improved SET-IBOOS protocol is proposed which the online/offline attribute based encryption method is used.

Setup phase: The setup algorithm takes as input a security parameter λ and a universe description U, which defines the set of allowed attributes in the system. It outputs are the public parameters PK and the master secret key MK.

Extraction process: The extract algorithm takes as input the master secret key MK and an access structure (resp., set of attributes) $Ikey$ and outputs a private key SK associated with the attributes.

Offline. Encrypt (PK): The offline encryption algorithm takes as input the public parameters PK and outputs an intermediate cipher text IT.

Online. Encrypt (PK, IT,: The online encryption algorithm takes as input the public parameters PK, an intermediate cipher text IT and a set of attributes (resp., access structure) and outputs a session key and a cipher text CT.

Decrypt (SK; CT) → key. The decryption algorithm takes as input a private key SK for $Ikey$ and a cipher text CT associated with) $Ienc$ and decapsulates cipher text CT to recover a session key.

IV. CRYPTOGRAPHY

Cryptography is the most offered security service in WSN. Applying any encryption scheme requires transmission of extra bits, hence extra processing, memory and battery power are needed. For ensuring robust security for the network, the keys are to be managed, revoked, assigned to a new sensor network or renewed. In different cryptographic schemes and their encountered issues are discussed.

KEY-BASEDALGORITHMS

1. Symmetric And Asymmetric Key – Based Algorithm
2. Symmetric Key Encryption

Diffie-Hellman & Discrete Logarithm for Encryption and Decryption

1. Diffie–Hellman Key Exchange
2. The Discrete Logarithm Problem
3. Security of the Diffie-Hellman Key Exchange
4. The Elgamal Encryption Scheme

The Diffie–Hellman protocol is a widely used method for key exchange. It is based on cyclic groups. The discrete logarithm problem is one of the most important one-way functions in modern asymmetric cryptography. For the Diffie–Hellman protocol in Z*p*, the* prime p should be at least 1024 bits long. This provides a security roughly equivalent to an 80-bit symmetric cipher. For a better long-term security, a prime of length 2048 bits should be chosen. The Elgamal scheme is an extension of the DHKE where the derived session key is used as a multiplicative masked to encrypt a message. Elgamal is a probabilistic encryption scheme, i.e., encrypting two identical messages does not yield two identical cipher texts.

V. RESULT

Comprehending the extra energy consumption by the auxiliary security overhead and prolonging the network lifetime are essential in the proposed SET-IBS and SET-IBOOS. In order to evaluate the energy consumption of the computational overhead for security in communication, we consider three metrics for the performance evaluation of Network lifetime, system energy consumption and the number of alive nodes. For the performance evaluation, we compare the SET-IB and SET-IBOOS with LEACH protocol and SecLEACH protocol.

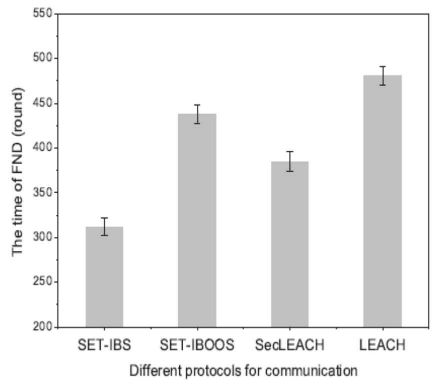


Figure 4 different protocols for communication

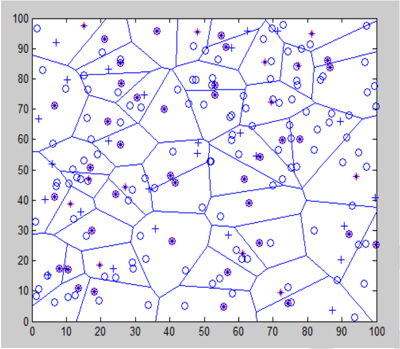
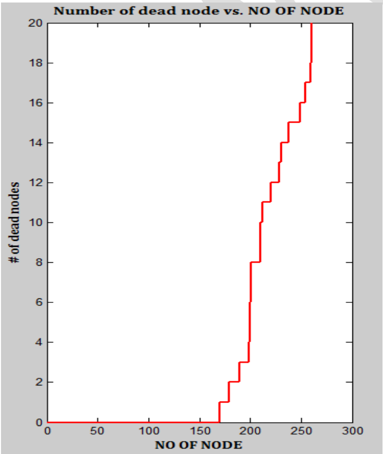


Figure 5. A snapshot of the random deployment of all the nodes is alive

We simulate a clustered wireless sensor network in a field with dimensions 100m X 100m. The total number of sensors n = 100. The nodes, both normal and advanced, are randomly (uniformly) distributed over the field. This means that the horizontal and vertical coordinates of each sensor are randomly selected between 0 and the maximum value of the dimension. The sink is in the center and so, the maximum distance of any node from the sink is approximately 70m (i.e. 2 √(A/2), where A is the length of the network area.

Network lifetime (the time of FND)

The below figure illustrates the time of FND using different protocols. We apply confidence intervals to the simulation results, and a certain percentage (confidence level) is set to 90%.We mainly consider the LEACH and SET for particularly LEACH to provided better performance for compare to all other protocols. The number of round increases to reduced number of dead node.



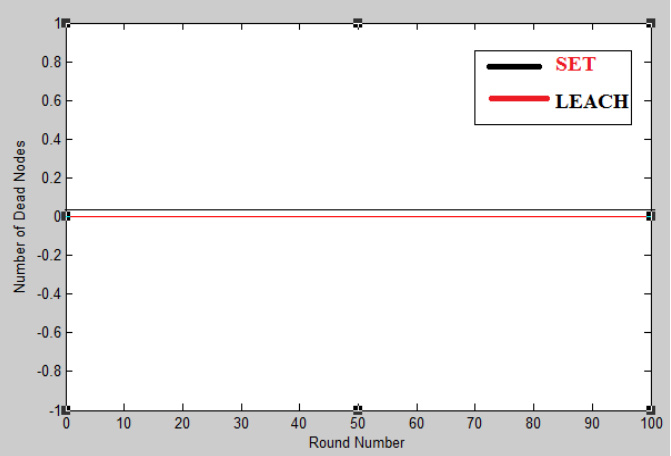


Figure 6 number of dead node vs. no of node

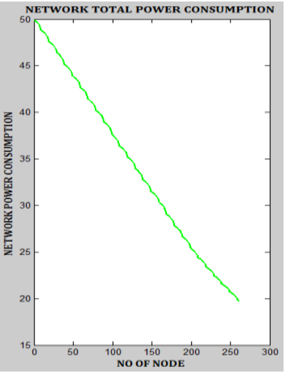
Figure 7 round numbers vs number of nodes

The number of alive nodes

The ability of sensing and collecting information in a WSN depends on the set of alive nodes (nodes that have not failed). Therefore, we evaluate the functionality of the WSN depending on counting the number of alive nodes in the network. Consider the below diagram to increase the number of rounds there is no dead node occur. So using LEACH and SET protocol there is no dead node present for increasing the number of rounds.

Total system energy consumption

It refers to the amount of energy consumed in a WSN. We evaluate the variation of energy consumption in secure data transmission protocols. The below figure shows to increase the number of nodes as well as increased number of rounds the overall network energy consumption low in LEACH protocol. In a cluster we used two types of node. One is normal node and another one is advanced node. The advanced node reduces the power consumption of the overall cluster.



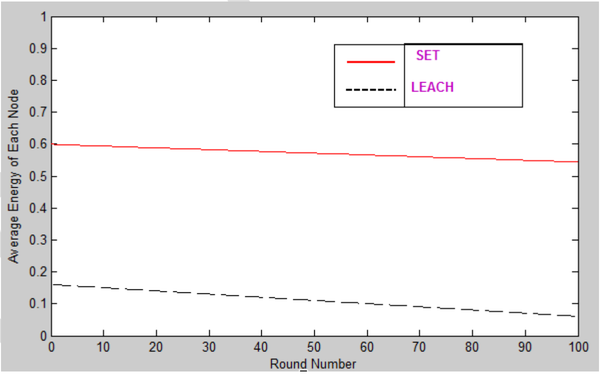


Figure 8 total power consumption

Figure 9 round number vs average energy of each nodes

Security and Throughput

SET protocol mainly used for secure and efficient data transmission in CWSN . We implement two types of algorithm in SET protocol . But compare to LEACH, SET provided low throughput. Only advantage is using security purpose but performance analysis is very low in SET. The above figure shows the comparison of the power consumption in two protocol LEACH only to provide low power compare to SET.

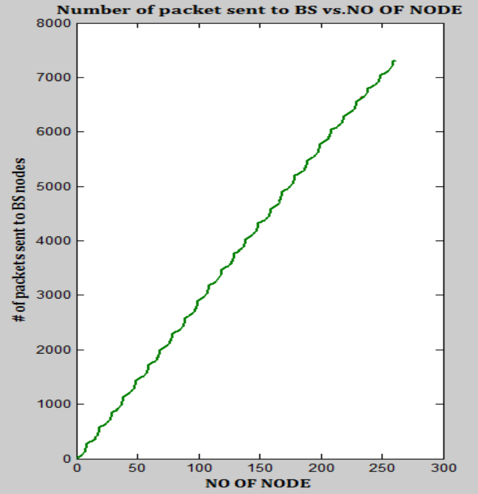


Figure 10 Number of packets sends to BS vs number of nodes

VI. CONCLUSION

In this paper, we 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. Finally, the comparison in the calculation and simulation results show that, the proposed protocols have better performance and security than existing secure protocols for CWSNs, with respect to both computation and communication costs.

VII. REFFERENCE

i. K. Dasgupta, K. Kalpakis, and P. Namjoshi, "An Efficient Clustering-based Heuristic for Data Gathering and Aggregation in Sensor Networks", IEEE 2003

ii. E. Fasolo, M. Rossi, J. Widmer, and M. Zorzi, "In-Network Aggregation Techniques for Wireless Sensor Networks: A Survey", IEEE Wireless communication 2007.

iii. Wendi Rabiner Heinzelman, Anantha Ch, and Hari Balakrishnan. Energy-efficient communication protocol for wireless microsensor networks.2000.

iv. H. Lu, J. Li, and G. Wang, "A Novel Energy Efficient Routing Algorithm for Hierarchically Clustered Wireless Sensor Networks," in *Proc. FCST*, 2009.

v. K. Pradeepa, W. R. Anne, and S. Duraisamy, "Design and Implementation Issues of Clustering in Wireless Sensor Networks," *Int. J. Comput. Applications*, vol. 47, no. 11, 2012.

vi. D. Boneh and M. Franklin, "Identity-Based Encryption from the Weil Pairing," in *Lect. Notes. Comput. Sc. - CRYPTO*, 2001.

vii. A. Shamir, “Identity-Based Cryptosystems and Signature Schemes,” in *Lect. Notes. Comput. Sc. - CRYPTO*, 1985.

viii. 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.

ix. S. Xu, Y. Mu, and W. Susilo, “Online/Offline Signatures and Multisignatures for AODV and DSR Routing Security,” Proc. 11th Australasian Conf. Information Security and Privacy, pp. 99-110, 2006.

x. 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.

xi. K. Dasgupta et al., “Maximum Lifetime Data Gathering and Aggregation in Wireless Sensor Networks”, In *Proc. of IEEE Networks’02 Conference*, 2002.

xii. Y. Wang, G. Attebury, and B. Ramamurthy, “A Survey of Security Issues in Wireless Sensor Networks,” *IEEE Commun. Surveys Tuts.*, vol. 8, no. 2, pp. 2–23, 2006.

xiii. 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.

xiv. W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, “An Application-Specific Protocol Architecture for Wireless Microsensor Networks,” *IEEE Trans. Wireless Commun.*, vol. 1, no. 4, pp. 660–670, 2002.

xv. A. Manjeshwar, Q.-A.Zeng, and D. P. Agrawal, “An Analytical Model for Information Retrieval in Wireless Sensor Networks Using Enhanced APTEEN Protocol,” *IEEE Trans. Parallel Distrib. Syst.*, vol. 13, pp. 1290–1302, 2002.