Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 8, August 2015, pg.132 – 142

RESEARCH ARTICLE

Secure and Efficient Data Transmission in Cluster based Wireless Sensor Network

Anup Pawar[1], Divya K V[2]

[1] M.Tech (Software Engineering), New Horizon College of Engineering, Bangalore, India

[2] Asst Professor, Department of Information Science & Engineering, New Horizon College of Engineering, Bangalore, India.

[1] anupbdr@gmail.com, [2] divya.k.vasudevan@gmail.com

Abstract: Wireless Sensor Network (WSN) is a collection of nodes which are deployed in an environment where the data is needed to be sensed to monitor any changes in surrounding. Each nodes are equipped with memory, battery, transceivers. The nodes are placed in such an environment where monitoring by human is difficult to schedule or managed efficiently by individual. Each node is responsible for manipulating the data it has sensed and transferring it to the Base Station (BS). These nodes are grouped into clusters so that the drainage of battery in wireless sensor network can be overcome and increase the scalability. In each cluster there is a Cluster Head (CH) which acts as a leader of the cluster and is responsible for gathering all the manipulated data from the each nodes in the cluster and transferring it to the Base Station. There is a need of secure and efficient transmission of data in cluster based WSN (CWSN) which will be discussed in this paper.

Keywords: CWSN, SET IBS, SET IBOOS, LEACH, IBS, IBOOS.

I INTRODUCTION

Cluster based Wireless Sensor Network is used to reduce the network consumption and also the increase in energy efficiency. Clustering in WSN is done to minimise the energy consumption and also to reduce the data transmission over the network required to transmit the message to the BS, as the CH becomes responsible for communication, which results into prolonged network lifetime.

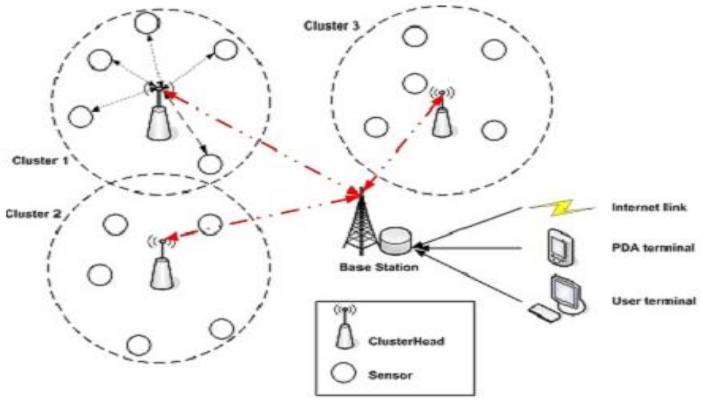

Fig 1: Cluster based WSN.

The set up phase is initiated as follows.

Advertisement phase: Initially each node makes decision whether to elect itself as CH for the current round or not. This decision is made on the suggested percentage of CH for the network and the number of times the node has been elected as CH till now. A node n chooses a random number between 0 and 1. If the random number is less than the threshold Tresh(n), the node becomes CH for the current round. The threshold is calculated using the formulae as shown below:

$$\text{Tresh(n)} = \begin{cases} \dfrac{p}{1-\left(r \bmod \frac{1}{p}\right)} & if\ n \in G \\ 0 & otherwise \end{cases}$$

Where p is the desired percentage of CH, r is the current round, G is the set of nodes that have not been CH for the last 1/p rounds. Each node that has elected itself as a CH for current round broadcasts a message as an advertisement to all the other non CH nodes using the same transmission energy. The non CH must keep their receiver open to hear the advertisement from the newly elected CH. The decision to join the CH is done on the advertisement heard with the largest signal strength is the cluster to whom minimum amount of transmission energy is required. If it ties than a random CH is selected.

Cluster Set up phase: As the node decides to which CH it wants to join they need to notify the CH that they want to join and this is done using CSMA MAC protocol.

Schedule Creation: Once the CH receives the notification from the nodes that they want to join it. The CH creates a TDMA schedule for each node in the cluster so that the nodes within its cluster must transmit the data in the allotted time.

Data Transmission: Once the nodes are allotted a time slot the nodes can transmit the data within the allotted time in the rest time the nodes goes to sleep mode so that energy consumption of the node is reduced.

The formation of cluster is established in two phases.

i) **Set up phase** where the clusters are formed and every round is initiated with this phase. The pseudo code for formation of set up phase is given below.

1. For Each (node A)
2. A generates random number r between 0 and 1
3. If (r < Threshold value)
4. A is elected as CH
5. A advertises its election as CH to all the nodes
6. Else
7. A becomes a regular node
8. A listens to message sent by all the CHs
9. A selects the CH with the loudest signal as its CH
10. A notifies the CH to which it has elected as Head and joins cluster
11. End If
12. For Each (cluster head CH)
13. For every node TDMA slot is created to transmit its data to CH
14. Allotted TDMA slots are distributed to each node which are part of cluster
15. End For

ii) The second phase is **Steady state phase** where the data is transmitted from leaf node to the BS. Steady state phase operations is longer than set-up phase operation. The pseudo code for the formation of Steady State phase, where data is collected from the nodes present in the cluster, is as below.

1. For Each (regular node A)
2. A aggregates data that is sensed by the node in the cluster
3. Data is transmitted by the N to CH in the allotted TDMA schedule.
4. End For
5. For Each (cluster head CH)
6. The data sensed by node is nodes present in the cluster is sent to the CH
7. The data is aggregated from all the nodes in the cluster at the CH
8. The aggregated data is sent to the Sink
9. End For

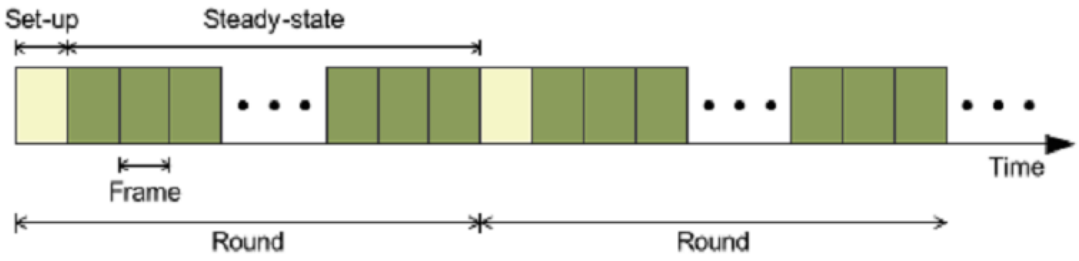

Fig 2. Steady and Set up phase operation

Earlier Low Energy Adaptive Clustering Hierarchy (LEACH) protocol was used, which is a type of hierarchical clustering, which is self-organising and self-adaptive. It uses each round as a unit, where the rounds are set-up phase and steady state phase as discussed earlier. In LEACH in order to consume equal energy of each node the CH's are rotated from one node to another in the cluster. But providing security to LEACH and similar kind of protocols is difficult as they rearrange the clusters network dynamically, periodically and randomly. So it is difficult to distribute common key and also difficult to provide long lasting node to node relationship. The main disadvantage of LEACH and similar protocols (SecLEACH, RLEACH, GSLEACH) are they use symmetric key management which suffers from an orphan node problem, occurs when node doesn't share its pairwise key with any other node so the node becomes orphan and does not belong to any cluster. In such case the node becomes independent CH without any nodes in its cluster, thus increasing the network energy consumption reducing the network lifetime efficiency. Even if the sensor nodes does not share its pairwise key with the nearest CH but does with the distant CH which requires more energy to transfer the data to the distant CH. To overcome this orphan node problem asymmetric key management is used.

II RELATED WORK

Symmetric key management was used in LEACH which lead to orphan node problem, occurring because of not sharing the pairwise key with another node in the network, leading to electing itself as a CH which leads to increase in consumption of networks energy. Earlier for secure transmission of data in CWSN asymmetric key management was employed instead of symmetric key, used in LEACH and similar protocols, which uses digital signature. In digital signatures the unique identifier associated with each node is used to create a public key. The main motive of this framework is to provide an authentication framework which solves the problem of energy consumption, storage overhead and the time to process. The Identity Based digital Signature (IBS) is used to compute nodes public key from its unique identity. The IBS scheme performs following four operations:

i) **Setup:** The BS, which acts as a trusted authority generates a master key, MSK, and the public parameters, param, for the private key generator, PKG, and distributes it to all leaf nodes.

ii) **Extraction:** With it's own unique ID the sensor nodes generate the private key with the help of MSK provided by the BS.

iii) **Signature Signing:** With the help of message M, time stamp t and signing key, the sending node generates a signature SIG.

iv) **Verification:** Given the message M, ID and the sender node generated signature SIG, the receiver node accepts the message M is the SIG is valid else it is rejected.

The Identity Based Online/Offline digital Signature (IBOOS) scheme was proposed to reduce the cost for storage of signature processing and reduce the computation. The offline phase can be executed on individual node or at the BS while during communication online phase was used. The offline scheme lacks reusability as it is precomputed by the third party. The operations performed by the IBOOS scheme are as follows:

i) **Setup:** The BS generates a master key MSK and the public key parameters, param, for the generation of private key at the sender node, and sends it to all the leaf nodes.

ii) **Extraction:** With the help of its unique ID the nodes create a private key with the help of MSK manipulated by the BS.

iii) **Offline Signing:** With the help of public parameters and the time stamp t, an offline signature SIGoff is generated by the CH and it is transmitted to all the leaf nodes in the cluster.

iv) **Online Signing:** With the help of private key, generated by the sensor node with the help of MSK, offline signature SIGoff and message M, a sending node generates an online signature SIGon.

v) **Verification:** Given ID, message M and online signature SIGon, the receiver node validates the message if the online signature is valid else rejected.

III PROPOSED SCHEME

For Secure and Efficient transmission of data over the network a new protocol called SET has been proposed which is used with the help of IBS and IBOOS scheme. In this scheme time stamp is being added for BS to node and leaf node to CH communication. The SET IBS has a protocol initialisation stage prior network deployment and operating in rounds. The main idea of SET IBS and SET IBOOS is to authenticate the encrypted data which are efficient in key management and applying key management for security. The operations in SET IBS are as follows.

a) **Protocol Initialisation:** In this stage let the time stamp for communication between BS to node is denoted by Tbn and let the time stamp for leaf node to CH be denoted by Tlc. The protocol initialisation works in round. In this paper we take IDpk as users public key under IBS scheme, propose a secure data transmission protocol by using IBS mainly for CWSN i.e.., SET IBS. At the initiation of protocol initialisation stage private pairing parameters are

preloaded into the sensor nodes so that the node does not have to generate the private key at the initiation of each round required for the authentication of node with another. Upon node becoming the orphan, its ID is distributed to all other nodes by the BS. In this scheme homomorphic encryption scheme is used which allows encryption of the cipher text, thus generating an encrypted result which when decrypted matches the result of the operations performed on plaintext. The BS performs the following operation of key pre distribution in all sensor nodes.

i) Generates the key for encryption required for the homomorphic encryption schemes to encrypt the data messages.

ii) Generate the pairing parameters.

iii) Choose the cryptographic hash functions.

iv) Pick a random integer as master key.

v) Preload each senor node with the public parameters.

b) Key Management for Security: Let's assume that the sensor leaf node n transmits the message M to the CH I, and encryption is done to the message with the key k done using homomorphic encryption scheme. The cipher text of the message is denoted by C. The SET IBS scheme consists of extraction, signing and verification operations.

$$C_n = h(C_n \mid |t_n \| \theta_n)$$

$$\sigma_n = C_n sek_n \| \alpha_n P$$

Where (σ_n, C_n) is the digital signature applied by node n on the encrypted message C_n. The message that is broadcasted is grouped as $(ID_n, T_n, C_n, \sigma_n)$

c) Protocol operation: The protocol operation is done as discussed before that is the setup phase and steady state phase.

The SET IBOOS is designed for higher energy efficiency. It operates similarly to SET IBS which includes protocol initialisation and operates in round during communication. The following operations take place in SET IBOOS

a) **Protocol Initialisation:** To minimise the computation and storage cost of signature signing IBOOS scheme is introduced. The protocol initialisation of this scheme is similar to SET IBS. The BS does following operation for SET IBOOS

i) Generates the encryption key with the help of homomorphic encryption scheme.

ii) The PKG selects random generator g of group G and chooses random number as master key.

iii) For each node n randomly select private key generation and H the hash function.

iv) Preload each sensor node with public parameters.

b) Key Management for Security: The node n transmits the message to the destination with time stamp and online signature in the form of ID of the node, time stamp t, offline signature σ and cipher text c.

c) Protocol Operation: The operation of SET IBOOS is similar to SET IBS. It has set up phase and steady state phase as discussed earlier.

Sl.No.	Characterstics	Secure data transmission Protocols	ID Based Schemes
1	Protocols	LEACH, SecLEACH, GSLEACH, RLEACH, SLEACH	SET IBS, SET IBOOS
2	Key assigned	Symmetric	Asymmetric
3	Storage Cost	High	Low
4	Network Scalability	Low	High
5	Computational Overhead	High	Low

Table 1: Comparison of ID based schemes and other secure transmission protocols

IV SNAPSHOTS

1. Base station which distributes the public parameters and master key to all nodes and selection of scheme is done.

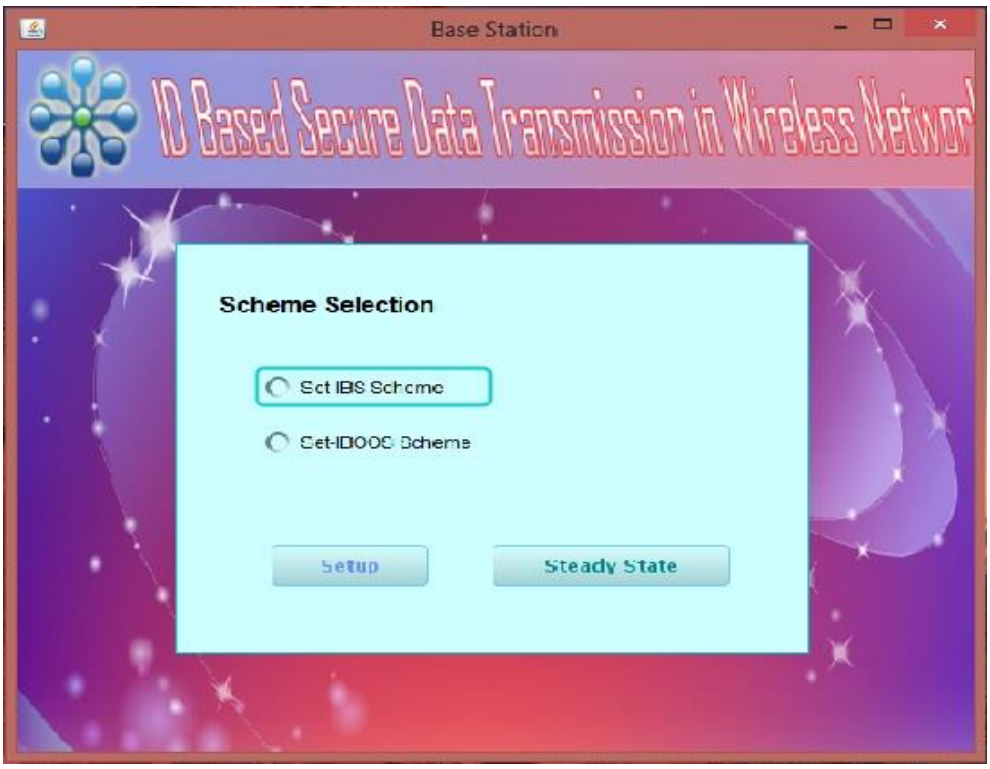

Fig 3: Base Station

2. Setup phase where the clusters are created.

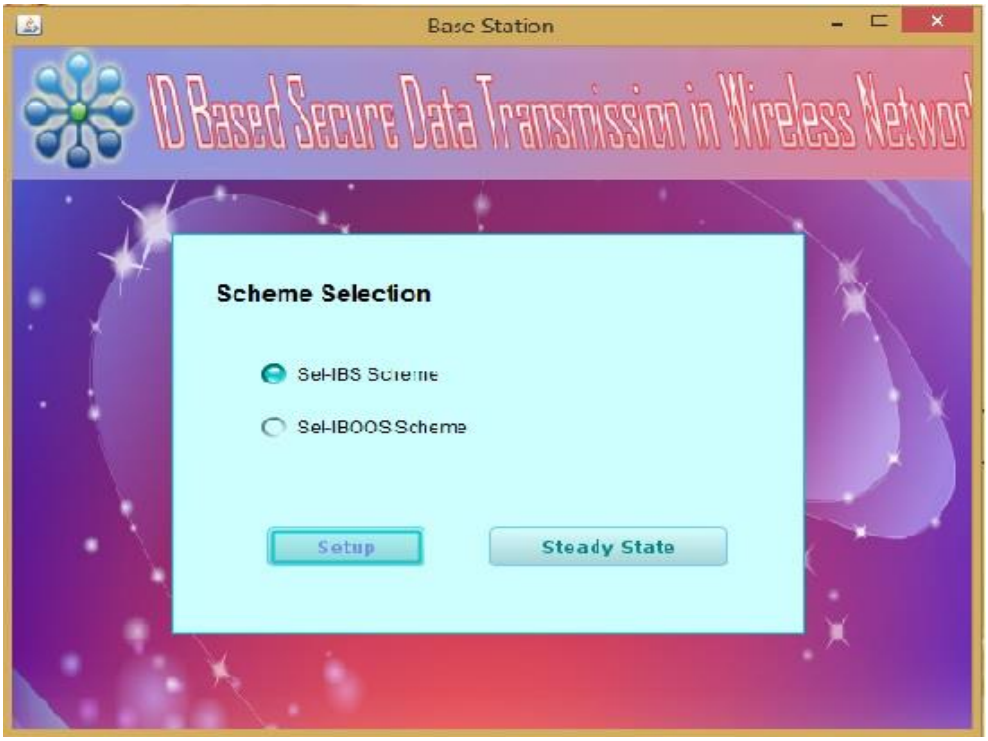

Fig 4: Set up phase

3. Steady state selection where leaf nodes transmit data to the CH.

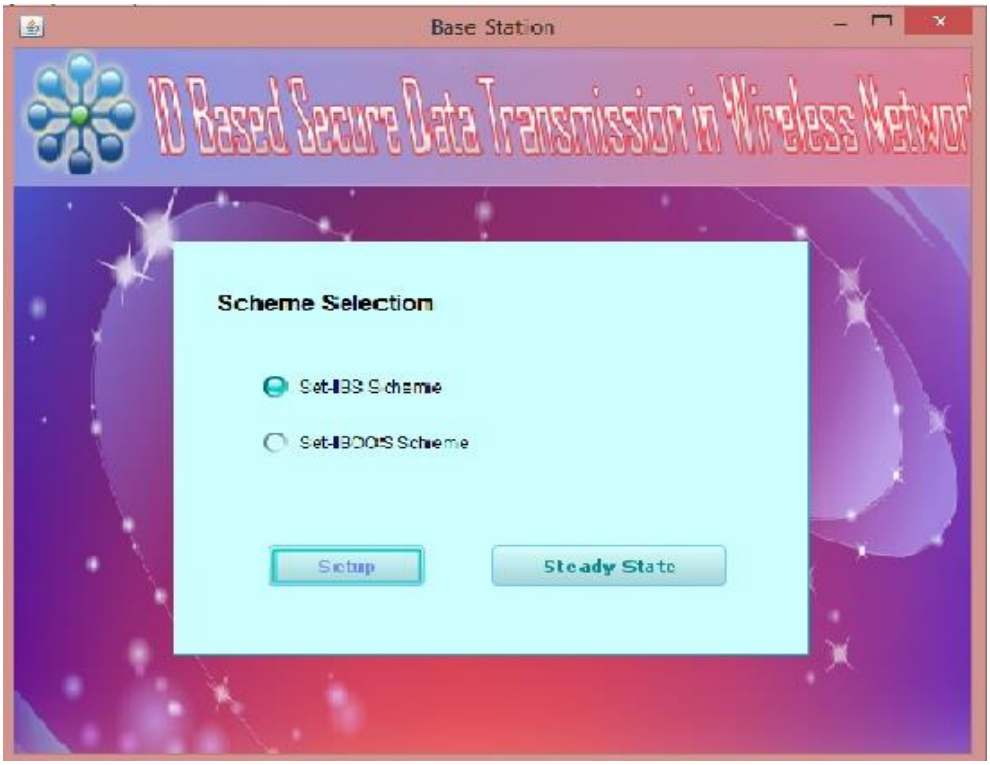

Fig 5: Steady state phase

4. Sender node which sends the data with the key.

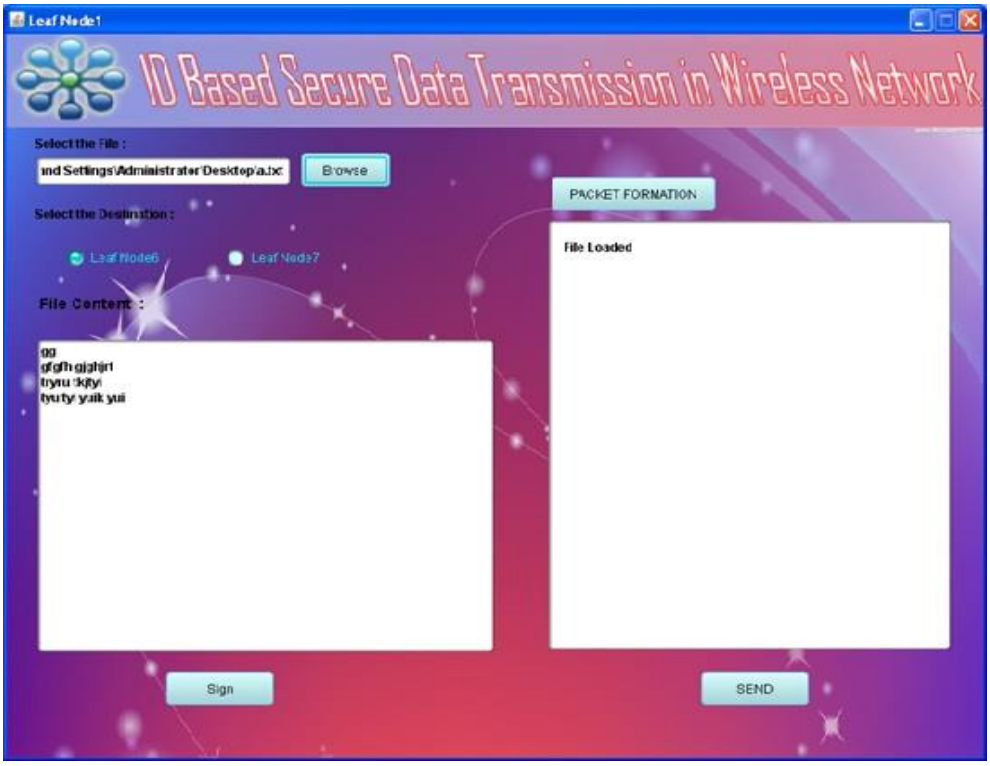

Fig 6: Sender Node

5. Receiver node which validates the received data that it accepts if the data is valid or else rejects.

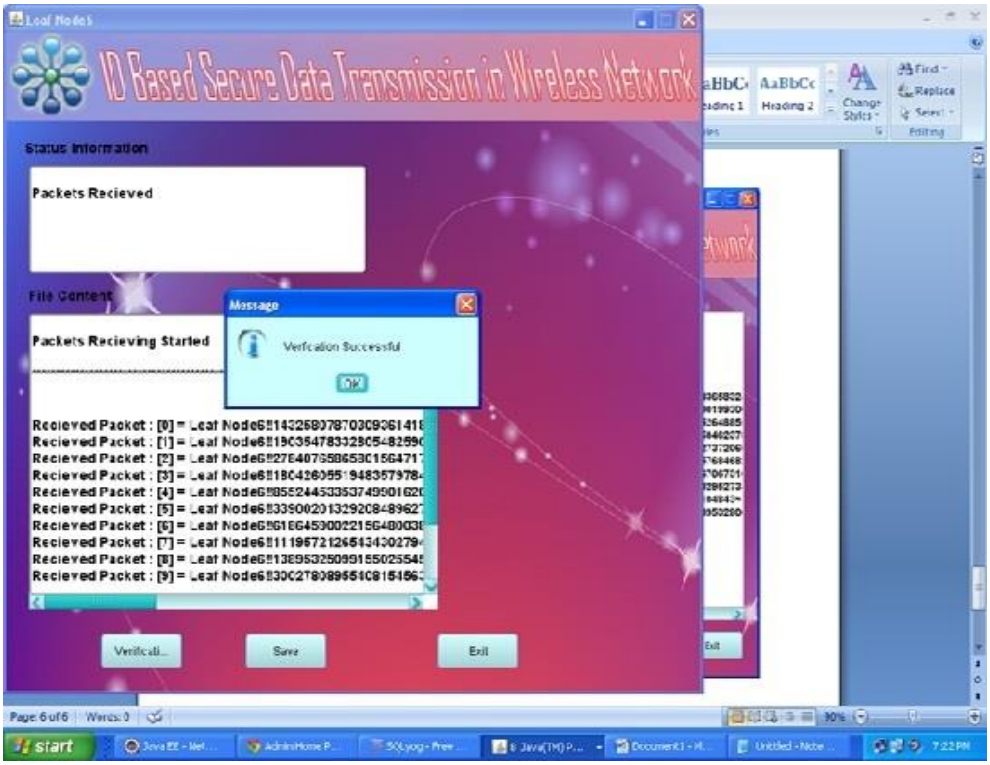

Fig 7: Receiver Node

V CONCLUSION

In this paper, initially it is identified that Clustering mechanism in WSN makes it possible for network scalability and hence decrease the energy consumption through aggregation of data. Clustering also enhances the system performance. We represented the existing protocols SET-IBS and SET-IBOOS and made an enhancement in terms of energy consumption and overhead data transmission. The paper also highlights the differentiation among various Cluster based protocols. In order to overcome security threats, Homomorphic encryption and Digital Signature are added to guarantee more security and reduction in computation cost. Added advantage, these two Enhanced protocols can now be used in real time application or sophisticated applications in some context like Military domains and Health sectors.

REFERENCES

[1]. Dilip Kumar, Trilok C. Aseri, & R.B. Patel "EEHC: Energy efficient heterogeneous clustered scheme for wireless sensor networks", Computer Communications, 2009.

[2] Rehana Yasmin, Eike Ritter, Guilin Wang *"*An authentication framework for Wireless Sensor Networks using identity-based signatures: Implementation and Evaluation", IEICE, 2012.

[3] Cheng-Kang Chu, Joseph K. Liu, Jianying Zhou, "Practical ID-based Encryption for Wireless Sensor Network", ASIACSS, 2010.

[4] Mohammad AL-Rousan , A. Rjoub and Ahmad Baset, "A Low-Energy Security Algorithm for Exchanging Information in Wireless Sensor Networks" Journal of Information Assurance and Security, 48-59, 2009.

[5] S. Muthusamy, Dr. C. Poongodi, Dr. D. Deepa "Identity Based Digital Signature Scheme in Cluster Based Wireless Sensor Networks for Secure and Efficient data Transmission – A Survey" IJAICT Volume 1, Issue 6, October 2014.

[6] Suchismita Chinara, Santanu Kumar Rath, "A Survey on One-Hop Clustering Algorithms in MobileAd Hoc Networks", Journal of Systems and Networks Management, 2009.[7] Suraj Sharma and Sanjay Kumar Jena " A Survey on Secure Hierarchical Routing Protocols in Wireless Sensor Network", ICCCS, 2011.

[7] R.Anbarasi, S.Gunasekaran "The Feasibility of SET-IBS and SET-IBOOS Protocols in Cluster-Based Wireless Sensor Network" IJIRCCE, 2014.

[8] M.C. Swathi & A. Dhasaradhi "Providing Efficient and Secure Data Transmission in CWSNs*",* IJARCSMC, 2014.

[9] Azzedine Boukerche, " Algorithms and protocols for Wireless Sensor Network".

[10] Sansar Choinyambuu, "Homomorphic Tallying with Paillier Cryptosystem", 2009.

[11] Naveed Islam, William Puech and Robert Brouzet, "How to Secretly Share the Treasure Map of the Captain?" LIRMM, 1999.

[12] Barry Boehm, edited by Wilfred J. Hansen, "Spiral Development: Experience, Principles and Refinements", 2000.

[13] Sepideh Zareei, Elham Babaee, Rosli Salleh, Saeed Moghadam," Employing Orphan Nodes to Avoid Energy Holes in Wireless Sensor Networks", www.scirp.org, 2013. [14] Wendi Rabiner Heinzelman, Anantha Chandrakasan, and Hari Balakrishnan, "EnergyEfficient Communication Protocol for Wireless Microsensor Networks", Published in the Proceedings of the Hawaii International Conference on System Sciences, January 4-7, 2000.

[15] Basilis Mamalis, Damianos Gavalas, Charalampos Konstantopoulos, and Grammati Pantziou," Clustering in Wireless Sensor Networks"

[16] Srie Vidhya Janani. E, Ganeshkumar.P, Vasantha Suganthi.G, Sultan.M, Kaleeswaran.D, "A Survey on Algorithms for Cluster Head Selection in WSN", IJARCET, 2013.

