Secure and Efficient Data Transmission for Cluster Based Wireless Sensor Network Using Cryptography

Sangamsh J. kalyane, Dr.Nagaraj B. Patil

Assistant professor, Dept. of Computer Science and Engineering BKIT, Bhalki Karnataka, India
Associate &HOD CSE Dept Govt Engineering College, Raichur, 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

Secure and efficient data transmission is a critical issue for cluster-based wireless Sensor Networks (WSNs).

In Cluster–based WSNs authentication of users is a very Important issue .So, by authenticating the sent user and the destination user , we can achieve the security and efficiency of data over CWSNs. To provide security of data and authentication of user we proposed a technique where we are implementing two concepts for performing those operations. The first one is identity based signature (IBS) for verification of user generated by the verifier and second one is a key is xor operated with the data and get the cipher and then binary level technique for encryption and decryption of the original message.

The binary level technique converts the plain text into binary form and then splits the data into blocks and assign values to it based on identification mark (IM) technique which depends upon the length of the binary digits, then these are divided into two level, 1st level is 2 bit and 2nd level is 4 bit . Then at the receiver user the Cipher text will be decrypted by using the reverse technique and the destination user will get the original message. By providing those techniques we can improve efficiency, security overhead and energy consumption.

A wireless sensor network is a group of specialized transducers with a communication infrastructure that uses radio to monitor and record physical or environmental conditions and also used in the variety of application such as military sensing and tracking, environmental monitoring, disaster management etc.

The individual nodes are capable of sensing their environments, processing the information locally, and sending data to one or more collection points in a WSN. Secure data transmission is one of the most important issues for WSNs.

At the same time, many WSNs are deployed in rough, disregarded, and often adversarial physical environments for certain applications, such as military domains and sensing tasks with trustless surroundings. Secure data transmission is especially necessary and is demanded in many such practical WSNs.

Their own dynamic attributes for soldiers in their deployed regions or echelons, which could be frequently changed. To refer to this DTN architecture where multiple authorities issue and manage their own attribute keys independently as a decentralized DTN. Sensor technology, low-power electronics, and low-power radio frequency (RF) design have enabled the development of small, relatively inexpensive and low power sensors, called *micro sensors* that can be connected via a wireless network.

These wireless micro sensor networks represent a new paradigm for extracting data from the environment and enabling the reliable monitoring of a variety of environments for applications that include surveillance, machine failure diagnosis, and chemical/biological detection.

An important challenge in the design of these networks is that two key resources communication and width and energy—are significantly more limited than in a tethered network environment These constraints require innovative design techniques to use the available bandwidth and energy efficiently.

In order to design good protocols for wireless micro sensor networks, it is important to understand the parameters that are relevant to the sensor applications. While there are many ways in which the properties of a sensor network protocol can be evaluated, we use the following metrics.

A. Ease of Deployment

Sensor networks may contain hundreds or thousands of nodes, and they may need to be deployed in remote or dangerous environments, allowing users to extract information in ways that would not have been possible otherwise. This requires that nodes be able to communicate with each other even in the absence of an established network infrastructure and predefined node locations.

B. System Lifetime

These networks should function for as long as possible. It may be inconvenient or impossible to recharge node batteries. Therefore, all aspects of the node, from the hardware to the protocols, must be designed to be extremely energy efficient.

C. Latency

Data from sensor networks are typically time sensitive, so it is important to receive the data in a timely manner.

D. Quality

The notion of ―quality‖ in a micro sensor network is very different than in traditional wireless data networks. For sensor networks, the end user does not require all the data in the network because 1) the data from neighboring nodes are highly correlated; making the data redundant and 2) the end user cares about a higher-level description of events occurring in the environment being monitored.

The quality of the network is, therefore, based on the quality of the aggregate data set, so protocols should be designed to optimize for the unique, application- specific quality of a sensor network. This paper builds on the work described by giving a detailed description and analysis of low energy adaptive clustering hierarchy (leach), an application-specific protocol architecture for wireless micro sensor networks. Leach employs the following techniques to achieve the design goals stated: 1)randomized, adaptive, self-configuring cluster formation;

2) localized control for data transfers;

3) low energy media access control (MAC); and

4) application specific data processing , such as data aggregation or compression. Simulation results show that leach is able to achieve the desired properties of sensor networks.

II. RELATED WORK

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]. HichemSedjelmaci*et.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 arrange of possible attacks. Because of their characteristics, conservative security methods are not appropriate. So 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 low false positive, correspondingly as in [2MaanYounis 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]. Nikolaos A. Pantazis*et.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/enhancethe 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 inenergy 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 sensornodes 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 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 [10]. 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 to a 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: 1)set-up phase

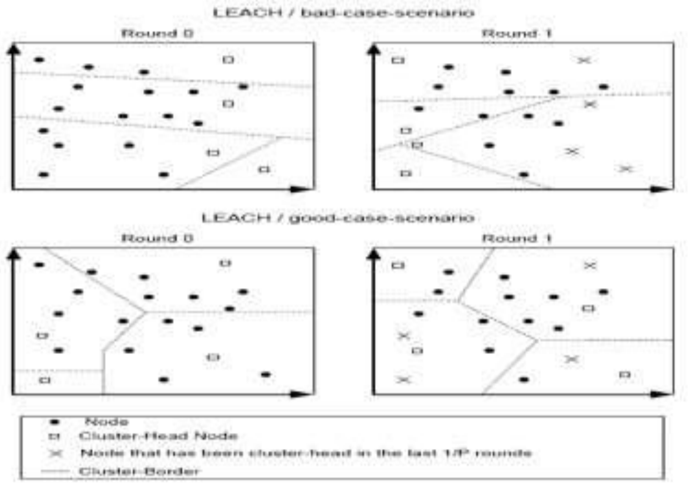
$$T(n) = \begin{cases} \frac{p}{1-p(r mode \frac{1}{p})} & n \in G \\ 0 & otherwise \end{cases}$$

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.

2) 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 to earlier existing protocols e.g. direct communication protocol, minimum- transmission-energy protocol and static Clustering protocol in Wireless Sensor 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. Since CHs are rotating from nodes to nodes in the network by rounds making it harder for types of protocols in WSNs.


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

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.

Meanwhile, 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. We suppose that, all sensor nodes know the starting and ending time of each round, because of the time synchronization.

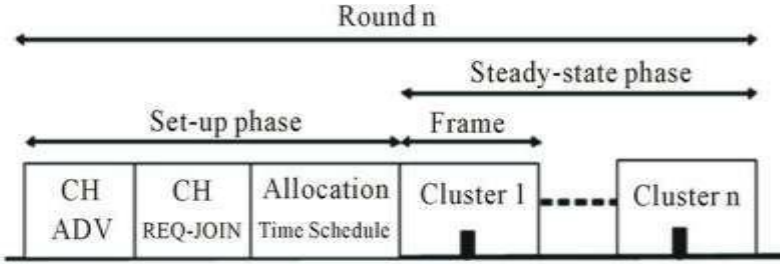
The operation of SET-IBS is divided by rounds as shown in Figure, which is similar to other LEACH-like protocols. Each round includes a setup phase for constructing clusters from CHs, and a steady-state phase for transmitting data from sensor nodes to the BS.

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 are randomly 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 securing 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 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.

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



LEACH Protocol operation

1) *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 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

2) *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.

3) *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 N 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. OBJECTIVE OF THE WORK

The wireless sensor network providing security and efficient of data is the critical problems. Secure and Efficient data transmission protocols for WSNs are vulnerable to a number of security active and passive attacks. Mostly, attacks to CHs in CWSNs could result in serious damage to the network because data transmission and data aggregation depend on the CHs(Cluster Head) node for Wireless Sensor Network.[2] The attacker manages to compromise or pretend to be a CH, it can provoke attacks such as sinkhole and selective forwarding attacks, hence disrupting the Sensor N/W.[3] The Existing System Sense the wireless sensor nodes to monitor physical or environmental conditions, and processing. The information data locally and sending to one or more collection points in a Wireless Sensor Network.

Limitations of Existing System:

- Adding security to LEACH-like protocols is challenging, because they dynamically, randomly and periodically rearrange the network's clusters and data links. Node-to-node trust relationships and common key distributions are inadequate for LEACH-like protocols.
- Apply the symmetric key management for security, which suffers from a□ so-called orphan node problem. This problem occurs when a node does not share a pair wise key with others in its preloaded key ring.
- In order to mitigate the storage cost of symmetric keys, the key ring in a node is not sufficient for it to share pair wise symmetric keys with all of the nodes in a network

There are two Secure and Efficient data Transmission (SET) protocols for CWSNs known as IBS and IBOOS.

The main idea using both IBS and IBOOS protocol is to authenticate the encrypted data which is sensed by sensor and apply the digital signatures to data which is encrypted which are efficient in communication and it signifies the security. Secret keys and pairing parameters are distributed in all sensor nodes by the base station which overcomes the key escrow problem Secure communication in IBS protocol is relies on the identity based cryptography is efficient in communication and saves energy. IBOOS protocol is proposed which is used to minimize the computational complexity for security. Both IBS and IBOOS protocol solve the orphan node problem with respect to symmetric key management in secure data transmission. In Proposed System Security and efficient transmission of data is necessary and demanded in many practical wireless sensor networks.

Advantages of Proposed System:

- Less computation and communication.
- High security.

IV. WORK CARRIED OUT SO FAR

Secure and efficient data transmission is a critical issue for cluster-based wireless Sensor Networks (WSNs).

In Cluster–based WSNs authentication of users is a very Important issue .So, by authenticating the sent user and the destination user , we can achieve the security and efficiency of data over CWSNs. To provide security of data and authentication of user we proposed a technique where we are implementing two concepts for performing those operations.

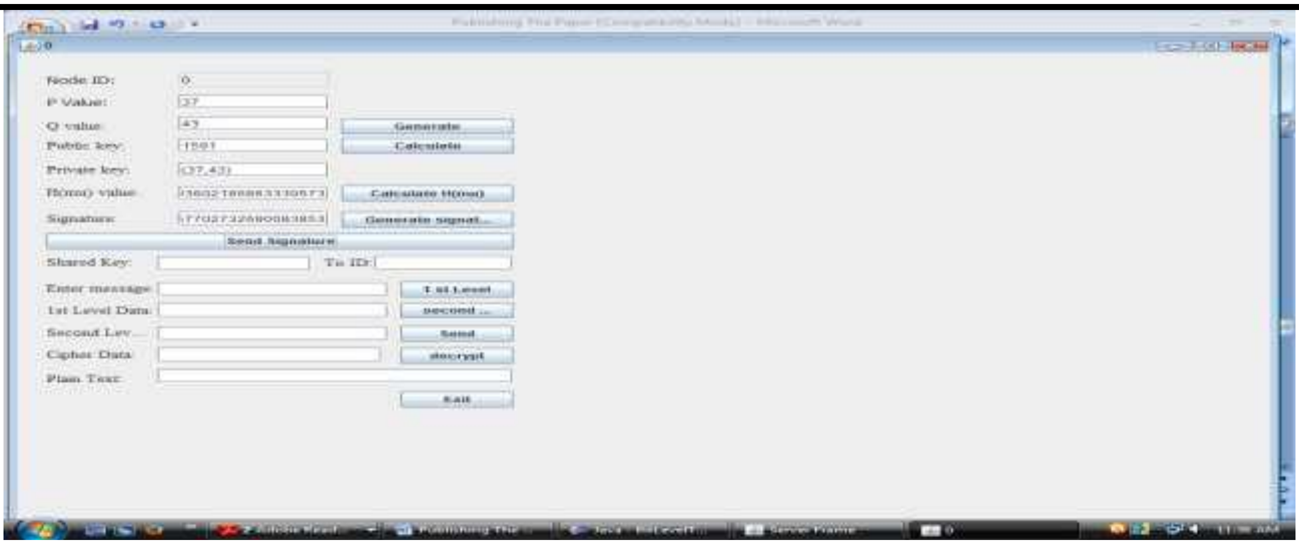
The first one is identity based signature (IBS) for verification of user generated by the verifier and second done is a key is xor operated with the data and get the cipher and then binary level technique for encryption and decryption of the original message. The binary level technique converts the plain text into binary form and then splits the data into blocks and assign values to it based on identification mark (IM) technique which depends upon the length of the binary digits, then these are divided into two level, 1st level is 2 bit and 2nd level is 4 bit .

Then at the receiver user the Cipher text will be decrypted by using the reverse technique and the destination user will get the original message. By providing those techniques we can improve efficiency, security overhead and energy consumption.

V. RESULTS AND DISCUSSIONS

Signature generated by Client

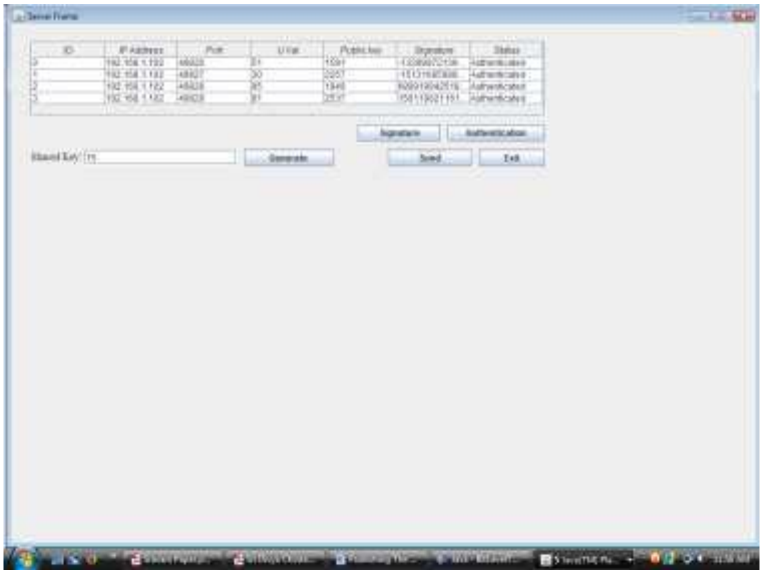
First sender is going to calculate a public key based on the P,Q values given by the user and those values are again used to generate the private key which is XOR with Hash function and generates the signature which will be send to the server for authentication..



Node ID: 0
P Value: 37
Q value: 43
Public key: 1591
Private key: (37,43)
H(mo) value: 15602188883330573
Signature: 17702732680083853
Shared Key:
To ID:
Enter message:
1st Level Data:
Second Lev...:
Cipher Data:
Plain Text:

Server Authentication

After receiving the signature the server authenticated the user and sends a shared key to all the clients who has send the signature to enhance further communication.



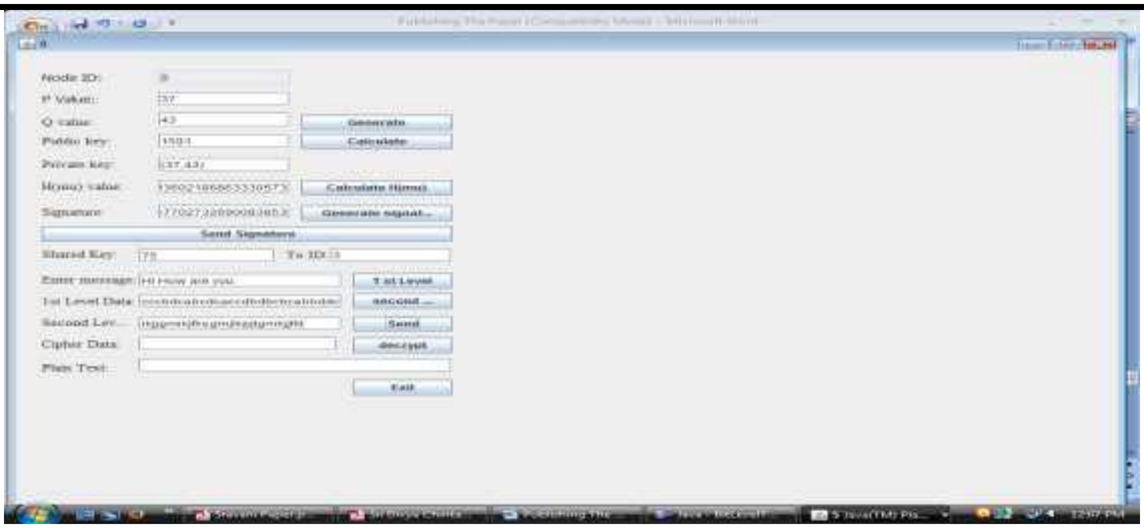
Server Frame

ID	IP Address	Port	U Val	Public key	Signature	Status
0	192.168.1.102	46925	31	1591	13086872136	Authenticated
1	192.168.1.102	46927	30	2257	1513168306	Authenticated
2	192.168.1.102	46928	35	1946	8099190425 16	Authenticated
3	192.168.1.102	46929	31	2537	15011902 1151	Authenticated

Shared Key: 11

Transferring the Massage

After receiving the shared key sent by the server, the user will enter the id of receiving user and then enters the message which will be encrypted using encryption techniques and message send to the particular user. Here we areusing 2 level of encryption techniques, Here we have 4 distinct blocks, according to the order they are 01, 00, 10, 11. So we put according to key generation technique 01=a, 00=b, 10=c, 11=d that is 1st level identification marks. For the generation of 2nd level identification marks, again the two bit representation of a ,b, c & d is aa, ab, ac, ad, bb, bc, bd,cc, cd, dd, ba, ca, da,cb, db, dc. Now we put aa=e, ab=f, ac=g, ad=h, bb=i, bc=j,bd=k, cc=l, cd=m, dd=n, ba=o, ca=p,da=q, cb=r, db=s,dc=t. As level of generation of identification marks for each block and length of decomposed block are chosen at run time as randomly, for it key is differed from each encryption to another. Not only that we are taken decomposed blocks in its sequence appearing for generating the identification marks for each block.

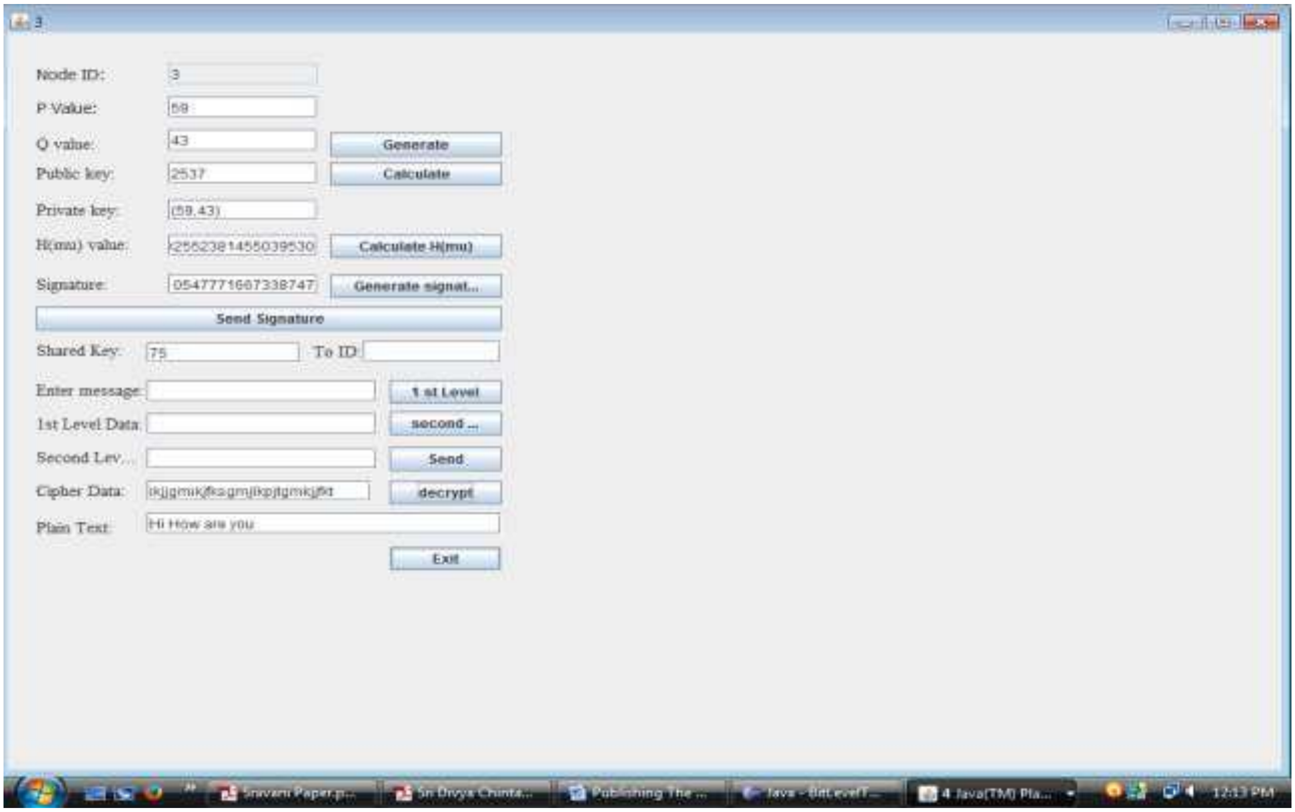


Node ID: 8
P Value: 37
Q value: 43
Public key: 1591
Private key: (37,43)
H(mu) value: 136021868653330573
Signature: 177027328900808653
Shared Key: 75
To ID: 3
Enter message: Hi How are you
1st Level Data: ccbdcabcdcaccdbdbcbcabbdc
Second Lev...: itjggmikjfksgmjlkpjtgmkjjfkt
Cipher Data:
Plain Text:

Receiving the message

The receiver will decrypt the message by decryption method and will get the actual message sent by the sender.Collecting all distinct blocks, identification marks for each block is assigned. This identification mark is same as First level of identification mark. From the beginning of the encrypted text, unchanged block (ML) is collected, length of which is defined in to the key.

Then every identification marks is replaced into identification marks. In that process we find two different Identification marks against each distinct block .Now we repeat finding identification marks up to D level in inverse Manner. Repeat the same procedure to identification marks up to Dang will get the data back .Replace the all Identification marks into its binary form with the help of key. Now we collected the entire bit-stream-blocks are merge together. After this merging, UB is attached at last of the recently generated decrypted bit of stream.



Node ID: 3
P Value: 59
Q value: 43
Public key: 2537
Private key: (59,43)
H(mu) value: 2552381455039530
Signature: 0547771667338747
Shared Key: 75
To ID:
Enter message:
1st Level Data:
Second Lev...:
Cipher Data: ikjjgmikjfksgmjlkpjtgmkjjfkt
Plain Text: Hi How are you

VI. CONCLUSIONS

In these the concepts of user authentication, Identity Based Signature, Encryption and Decryption, were proposed. By proposing those concepts more security and efficiency will be added to the given system.

Now a days the data transferring plays an important part in our daily life but the transfer of data must be secure. So to send the data in secure manner we has to follow some techniques. Such as authenticating the user with the verifier, and for the communication key generation algorithm is used. In this we are using another technique for the key is xor operated with the data and get the cipher and then binary level technique is used for encryption and decryption. By providing those technique we provide more security and efficiency for transferring data

REFERENCES

[1] S. Sharma and S. K. Jena, "A survey on secure hierarchical routing protocols in wireless sensor networks," in Proc. ICCCS, 2011.

[2] Heinzelman W. B., Chandrakasan A. P., Balakrishnan H., "An applicationspecific protocol architecture for wireless microsensor networks," IEEE Trans on Wireless Communications, Vol. 1, No. 4, 2002, pp. 660-670, doi: 10.1109/TWC.2002.804190.

[3] X. H. Wu, S. Wang, "Performance comparison of LEACH and LEACHC protocols by NS2," Proceedings of 9th International Symposium on Distributed Computing and Applications to Business, Engineering and Science. Hong Kong, China, pp. 254-258, 2010

[4] P.T.V.Bhuvaneswari and V.Vaidehi "Enhancement techniques incorporated in LEACH- a survey"Department of Electronics Engineering, Madras Institute Technology, Anna University Chennai, India, 2009

[5] Wu Xinhua and Huang Li "Research and Improvement of the LEACH Protocol to Reduce the Marginalization of Cluster Head"Journal of Wuhan University of Technology Vol. 35, No. 1, Feb. 2011, pp. 79-82, doi:10.3963/j.issn.1006-2823.2011.01.019 (in Chinese).