ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 1, *January 2015*

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

Sanghamitra Panda[1], Satyanarayana Gandi[2], Amarendra Kothalanka[3]

Department of Computer Science & Engineering, Dadi Institute of Engineering & Technology, Anakapalle, A.P., India[1,2,3]

Abstract: 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.

Key words: Identity based Signature (IBS), shared key generation, User authentication, message encryption and decryption.

INTRODUCTION

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 *microsensors* that can be connected via a wireless network. These wireless microsensor 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 microsensor 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

DOI 10.17148/IJARCCE.2015.4106

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 1, *January 2015*

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 microsensor 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.

Existing Technique

In wireless sensor network providing security and efficient of data is the critical issue. The data transmission protocols for WSNs are vulnerable to a number of security attacks. Especially, attacks to CHs in CWSNs could result in serious damage to the network because data transmission and data aggregation depend on the CHs fundamentally. If an attacker manages to compromise or pretend to be a CH, it can provoke attacks such as sinkhole and selective forwarding attacks, hence disrupting the network .On the other hand, an attacker may intend to inject bogus sensing data into the WSN. To overcome those problems we can introduce proposed system.

Proposed Technique

In wireless sensor network efficient data transmission is one of the most important issues for WSNs. Here S has 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.

Users Authentication

This module is used for performing authentication of user can be done by trusted center. The trusted center retrieves the signature from the users and generate each user signature compare it. If both signatures are equal they are the authenticated user. If the signature are not equal they are not authenticate users. The authentication process as follows.

To sign a message b the signer *S* picks random padding X and calculates L*(b X)*

S then solves y*(y + a)* = L *(b X) % n*

If there is no solution *S* picks a new pad X and tries again.

If L is truly random the expected number of tries is 4.

The signature on b is the pair *(X, y)*

Given a message band a signature *(X, y)* send to the verifier.

The verifier *V* calculates y*(y + a)* and L*(b X)* and verifies that they are equal then retrieve the packet and both v and b are equal they are authenticated user.

Encryption

Initial1y plain text is split into blocks, having equal length after x-or operation with key which is send by the user. Then we take each distinct block and all the distinct blocks according to their sequence of appearance are kept in private key. The content after x-or operation is converted into binary form which is nothing but stream of bit which is decomposed into N number of blocks of equal length; say L bits where L is an integer. It may be happened that after decomposition of total source-stream of bit into some L-bit blocks, a blocks, less than L bits is left at last, say ML (means length of ML< L) which is kept unchanged during encryption. So here N should be less or equal to 2L ($N \leq 2L$). For the encryption we need to generate replaced code, named Identification Marks for each distinct block.

Send each split blocks with recently generated corresponding identification marks.

Let us consider the two consecutive identification marks and replace with identification marks which are generated on and onwards with the 2nd level regeneration process the replacement process will be continued upto D level .Now ML is appended at beginning with the output hence the encrypted text will be generated.

Decryption

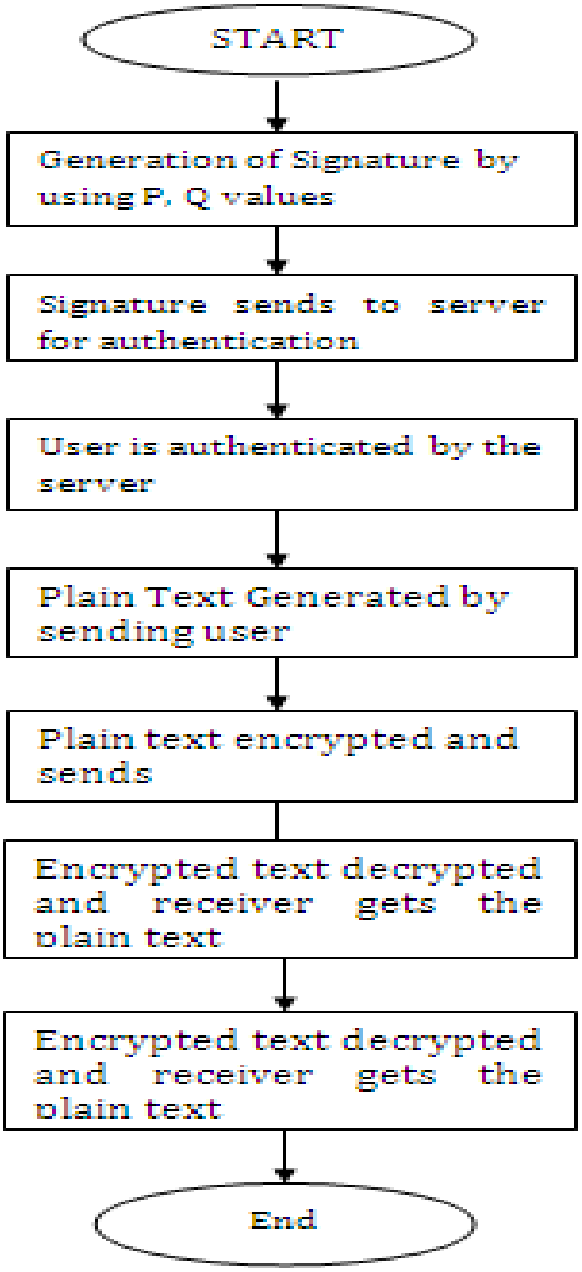
Collecting all distinct blocks, identification marks for each block is assigned. This identification mark is same as first level of identification mark. From the beginning of the encrypted text, unchanged block (ML) is collected, length of which is defined in to the key.

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.

DOI 10.17148/IJARCCE.2015.4106

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

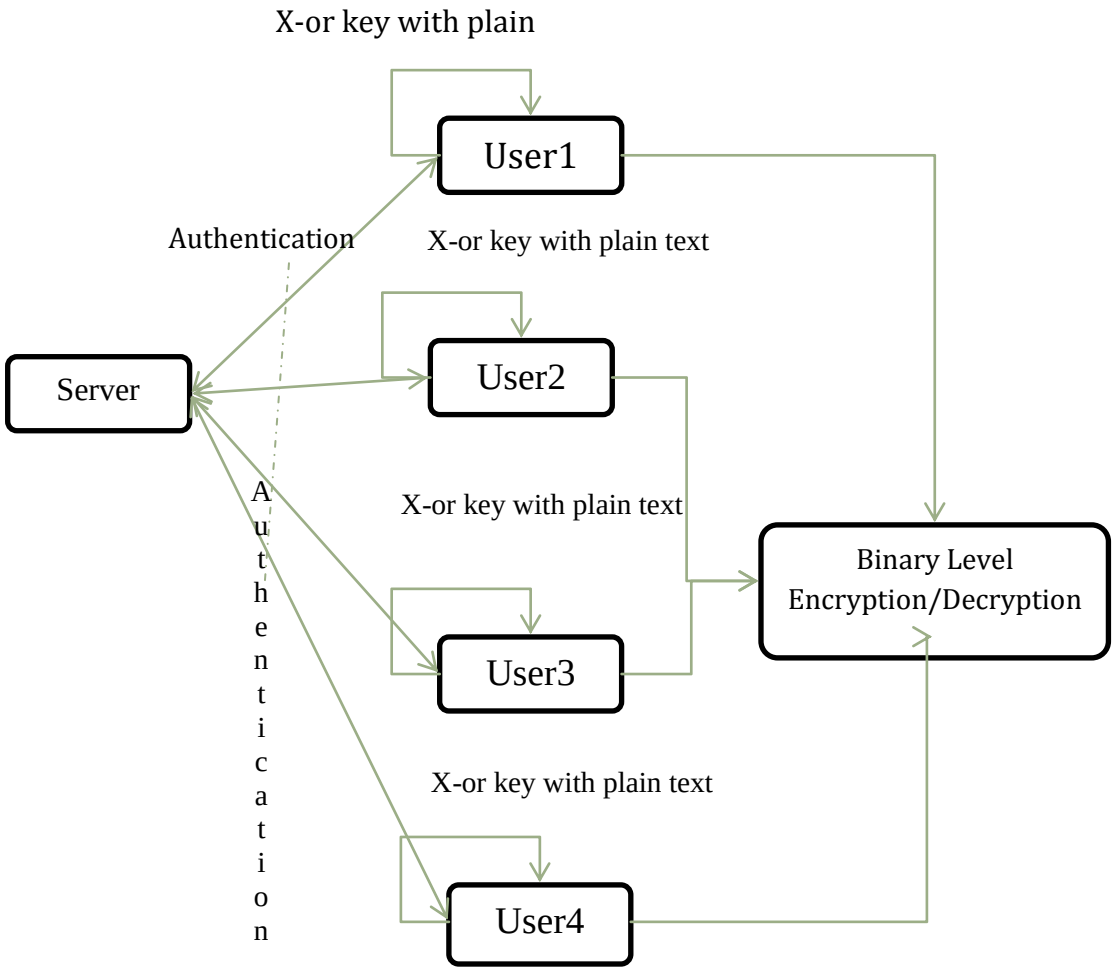
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 1, *January 2015*



DOI 10.17148/IJARCCE.2015.4106

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

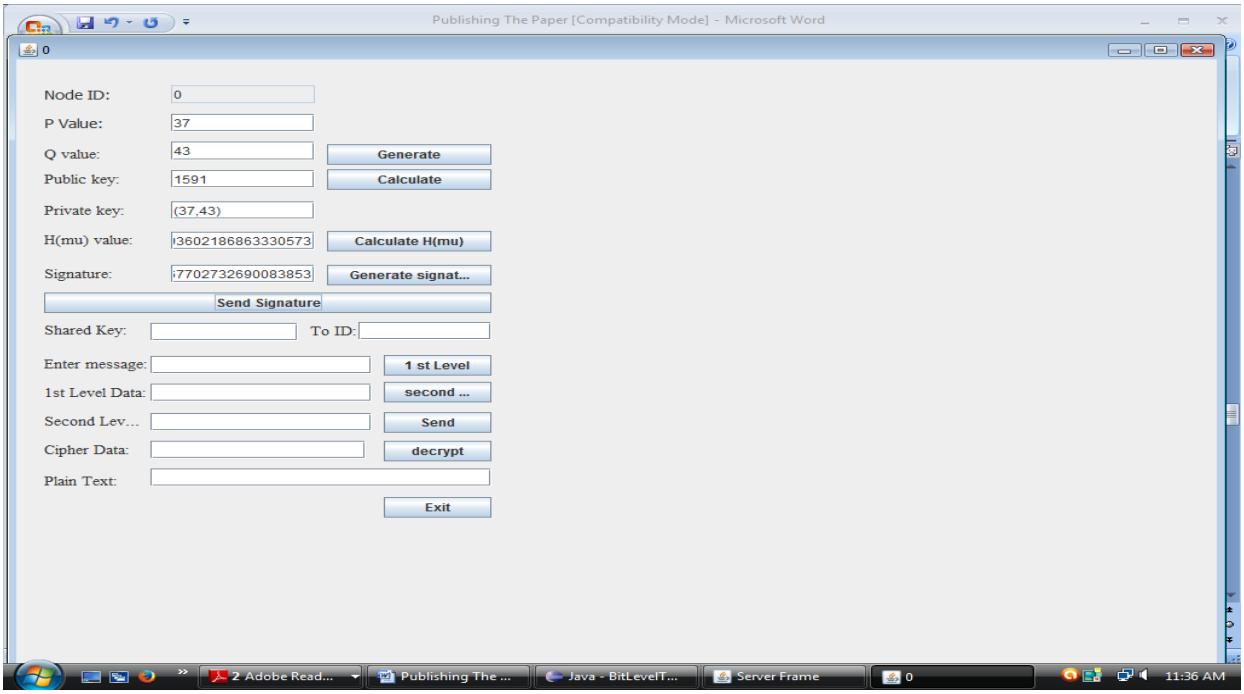
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 1, *January 2015*



EXPERIMENTAL RESULTS

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.



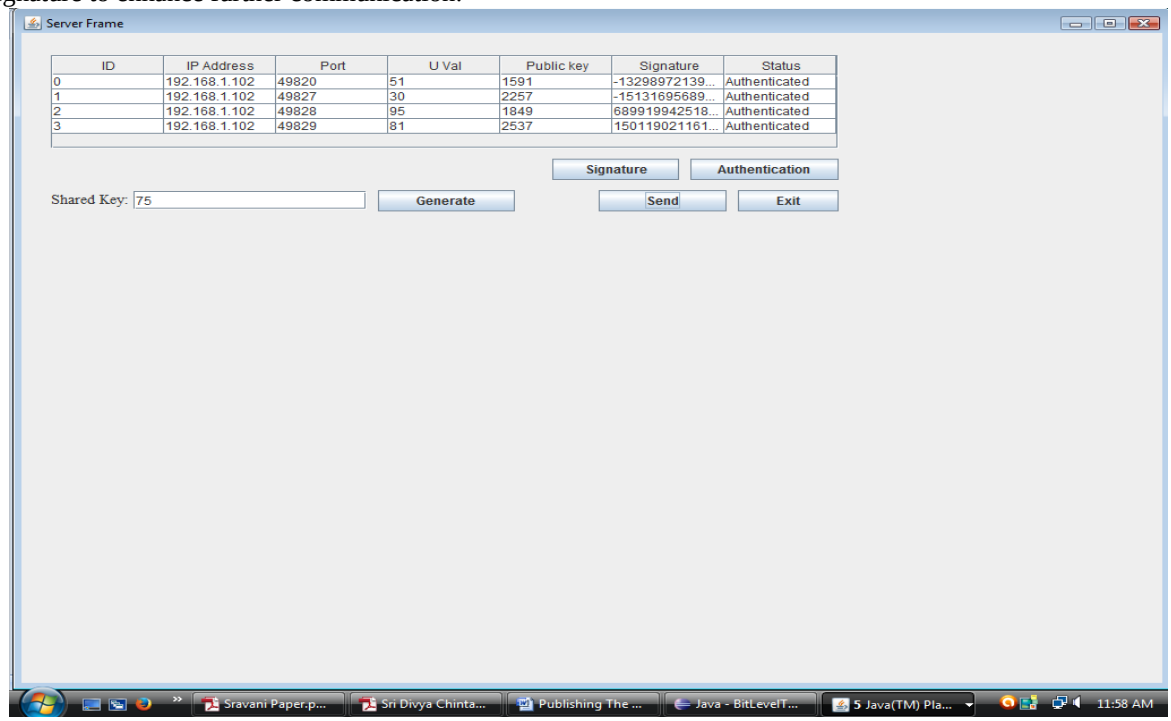
DOI 10.17148/IJARCCE.2015.4106

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 1, *January 2015*

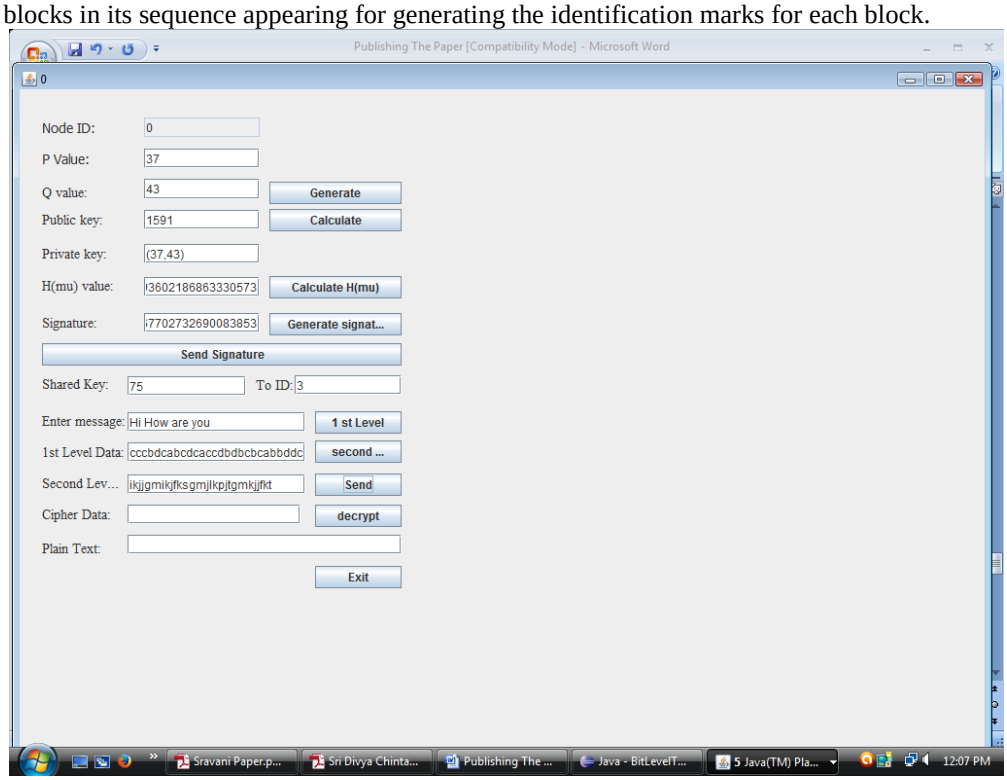
Server Authentication

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.



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 are using 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.



DOI 10.17148/IJARCCE.2015.4106

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

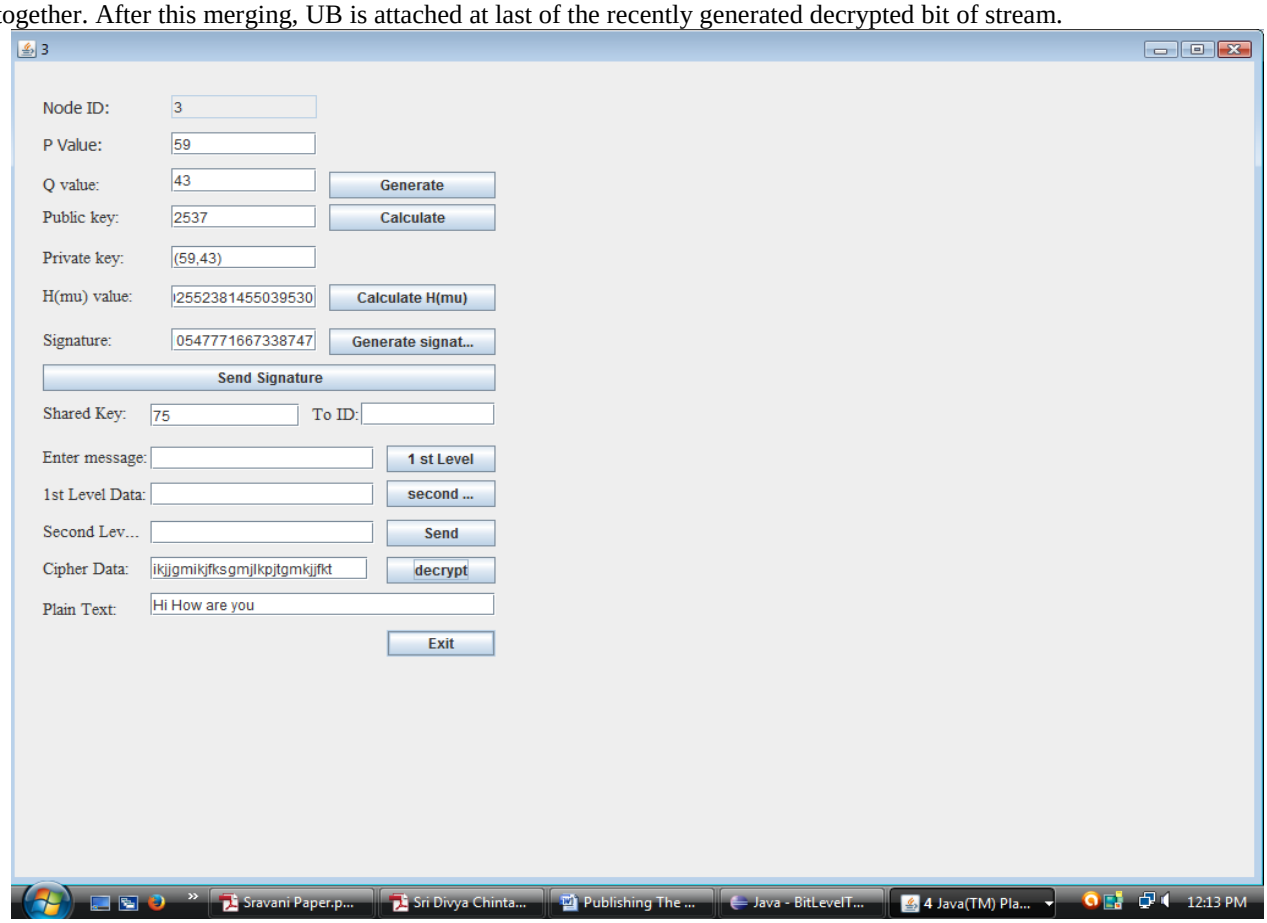
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 1, *January 2015*

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.



RESULT

As a result by providing those techniques we provide more security and efficiency for transferring data. We can overcome the demerits of earlier problems like hacking and other disturbances. The destination node gets the secure and correct data.

CONCLUSION

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 dat 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.

DOI 10.17148/IJARCCE.2015.4106

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 1, *January 2015*

REFERENCES

[1] T. Hara, V.I. Zadorozhny, and E. Buchmann, Wireless SensorNetwork Technologies for the Information Explosion Era, Studies inComputational Intelligence, vol. 278. Springer-Verlag, 2010.

[2] Y. Wang, G. Attebury, and B. Ramamurthy, "A Survey of SecurityIssues in Wireless Sensor Networks," IEEE Comm. Surveys &Tutorials, vol. 8, no. 2, pp. 2-23, Second Quarter 2006.

[3] A.A. Abbasi and M. Younis, "A Survey on Clustering Algorithmsfor Wireless Sensor Networks," Computer Comm., vol. 30, nos. 14/15, pp. 2826-2841, 2007.

[4] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "AnApplication-Specific Protocol Architecture for Wireless MicrosensorNetworks," IEEE Trans. Wireless Comm., vol. 1, no. 4, pp. 660-670, Oct. 2002.

[5] A. Manjeshwar, Q.-A.Zeng, and D.P. Agrawal, "An AnalyticalModel for Information Retrieval in Wireless Sensor NetworksUsing Enhanced APTEEN Protocol," IEEE Trans. Parallel &Distributed Systems, vol. 13, no. 12, pp. 1290-1302, Dec. 2002.

[6] S. Yi et al., "PEACH: Power-Efficient and Adaptive ClusteringHierarchy Protocol for Wireless Sensor Networks," ComputerComm., vol. 30, nos. 14/15, pp. 2842-2852, 2007.

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

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

[9] P. Banerjee, D. Jacobson, and S. Lahiri, "Security and Performance Analysis of a Secure Clustering Protocol for Sensor Networks,"Proc. IEEE Sixth Int'l Symp.Network Computing and Applications (NCA), pp. 145-152, 2007.

[10] K. Zhang, C. Wang, and C. Wang, "A Secure Routing Protocol 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