International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)
Web Site: www.ijettcs.org Email: editor@ijettcs.org
Volume 5, Issue 2, March-April 2016 **ISSN 2278-6856**

Cluster Based Wireless Sensor Network: Security Using SHA1 and Authentication using Election Algorithm

Scholar. Jubber Salim Nadaf [1], Prof.Dr.Shuhas Patil [2]

[1] Dept. Computer Engineering Bharati Vidyapeeth Deemed University College of Engineering Pune-41Maharshtra

[2]Dept. Computer Engineering Bharati Vidyapeeth Deemed University College of Engineering Pune-41Maharshtra

Abstract

The proposed system is on Wireless sensor network and clustering technique has been applied for better communication with a cluster leader election among nodes. The cluster head helps is better communication this is been done with election algorithm .even though security has been main problem for this SHA1 algorithm, an industry standard algorithm is been implemented. SHA1 helps is sending Encrypted message and files over network providing security mechanism. SHA1 is 128 bit Encryption algorithm and used along with MD5 and Digest for providing security to web application. Proposed system is been built on standalone system with varying Ip and Port Number's ,a set of 10 nodes with a base station has been built for research work .The Average delay achieved with SHA1 is 4.5.

Keywords: Wireless Sensor Network (WSN), Network Clustering, SET, CWSN

1. INTRODUCTION

Mobile Adhoc network help in establishing network in any remote areas like military ware field disaster situation or any other situations where lack of network setup with wired connectivity lacks. In future scope to them sensor network sense data and transmit them dynamically .Issues that MANET face is nodes have to transmit data over time either broadcasting or routing technique which has large energy requirement and have no grantee of data been transmitted to other destination place node. Also data is been shared between nodes and give rise to security . To have better network we come up with WSN and active work is to make them applicable in all form of system with better performance and better security mechanism.

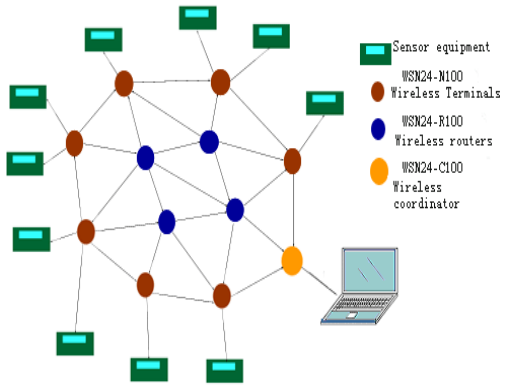

Fig1: Wireless Sensor Network

To have better network we come up with WSN and active work is to make them applicable in all form of system with better performance and better security mechanism.

Applications OF WSN:

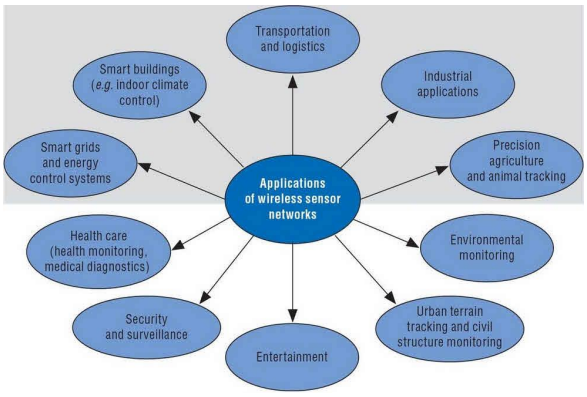

Fig2: WSN Application Area

[1.] Smart buildings.
[2.] Smart Grids.
[3.] Health care.
[4.] Security and surveillenace.
[5.] Entertainment.
[6.] Tracking in terrain.
[7.] Environment monitoring.
[8.] Agriculture and animal tracking.
[9.] Transportation and logistics.

[10.]Industrial applications.

2. BACKGROUND KNOWLEDGE

2.1WSN [1]

WSN many times termed wireless sensor and actuator network (WSAN) are geo-distributed deemed sensors to *observer* corporeal or ecological circumstances that as temperature humidity sound etc. and to helpfully permit their information over the system to target location. The additional contemporary systems are two-directional also allowing *switch* of device action. The growth of sensor networks was interested by military requests that as battleground shadowing nowadays such systems are secondhand in numerous manufacturing and customer requests that as manufacturing procedure checking and control with health monitoring and many more.

TWSN is constructed of nodes from a scarce to numerous 100or 1000 in which each knob is linked to other many time to many other knob sensors. All such sensor network knob has characteristically numerous parts a radio device with interior antenna or joining to outside antenna with microcontroller an electric track for joining sensors with a energy stack that as battery or any other energy source harvesting it. Sensor node would differ in size from a box size to small grain size depending on its application area though major size depends on microcontroller size and is also a active research to make sensor networks better. cost of sensor nodes is likewise mutable reaching from 10 to 100 of dollars dependent on difficulty of individual sensor node. Size and cost restraints on device knobs consequence in consistent restraints on capitals that as energy memory computation speed and infrastructures bandwidth. Topology of WSN could vary from meek star to an progressive hop mesh network. The spread method amongst hops of system could be routing or flooding.

2.2 WSN Features [1]

Features of a WSN include:

- Power ingestion restraints for nodes i.e **[energy harvesting]**
- Capability to manage with node letdowns [**resilience**]
- Certain flexibility of nodes [MWSN]
- Heterogeneity of nodes.
- Scalability in huge deployment area.
- Capability to withstand exacting ecological circumstances
- Easy to deploy
- Cross-level architecture.

2.3 WSN Platforms

- Hardware
- Software
- OS
- Online cooperative sensor data organization stages.

2.4 WSN Related Technologies

- Distributed sensor network
- Data integration and sensor web
- network processing
- Open-WSN

3. TABULATED LITERATURE SURVEY

Sr.no	Author	Abstract	Technique	Limitations	Scope
1	Heinzelman	work focus on energy effective cluster focused LEACH (low energy adaptive clustering hierarchy), achieving better life.	[1.] Adaptive cluster.	Intra cluster communication	Constraint based .
2	Oliveira	Proposed work implements random key pre-distribution for achieving security. SeLEACH gives authenticity with integrity, confidentiality based system.	[1.] includes µTESLA, [2.] Random key predistribution	Overhead of seLEACH is much than LEACH.	distance estimates
3	Abbasi	This work presents procedures in WSN's for clustering and comparative examination on	[1.] Varaiable convergence time	No comparativ	WNS's .better design

		their complexity scalability, cluster overlapping with support for node stability.	algorithms. [2.] Linked cluster Algorithms(LCA) [3.] Adaptive clustering [4.] .Random competition based clustering [5.] Hierarchical clustering. [6.] Energy-Efficient Hierarchical_Clustering (EEHC) [7.] Algorithm for Cluster Establishment. [8.] Hybrid Energy-Efficient Distributed Clustering (HEED):	e analysis between algorithms	
4	Zhang	WSN's.article presents procedure to add additional security to LEACH for clustering process with random pair wise key(RPK). Development shows RLEACH to be light and energy saving.	[1.] Pre-distribution Phase\ [2.] Shared-key discovery phase. [3.] Cluster set-up phase [4.] Schedule creation phase [5.] Data transmission phase	Overhead is more t	3 tier design
5	Pradeepa	Article focuses on design and issues related to WSN development.	. 1. Node mobility. 2. Traffic load 3. Load balancing. 4. Dynamic cluster control. 5. Inter cluster co-ordination. 6. Data Aggregation. 7. Fault Tolerance. 8. Scalability. 9. Node heterogeneity. 10. Self reconfiguration. .	Research work is been tested in simulation which at times fail with false values.	Algorithms developed are mostly for Flat network and fail for dynamic one. Development of algo and system design we show consider clustering issues.
7	Rebecca	Leader selection procedure in dynamic network is ben presented. TORA bring scalable and stable system.	[1.] selection of leader node. [2.]	no proof ,as no values	Election Algorithm .
8	Wendi	LEACHES a protocol architecture for energy effective and better clustering algorithm for application specific domain.	1 Cluster Head Selection Algorithms. 2.Cluster-Formation Algorithm. 3 Steady-State Phase	Algorithm is constraint based.	Intra Cluster Management

9	Rajeshwari	Re–election is implemented reducing data loss and load balancing access problem	1. Cluster Formation for WSN 2. Cluster Head Selection 3. Routing Tree Construction 4. Re-Electing Cluster Head. 5. Data Transfer.	needs to be tested in real as values may vary in real time.	additional security algorithm with industry standards.
10	Huang	secure and cluster based WSN is presented. SET-IBS and SET-IBOS are presented with online and offline digital signature. Computational overhead is reduced with better security and energy consumption.	**1.** IBS Setup WSN Extraction. Signature signing Verification **2.** IBOS Setup WSN Extraction. Offline signing Signature signing verification	tested 100 nodes w	can be extended to attribute based system ABS ones.
11	Shuhas Patil	Sensor nodes' positions achieve a vital part in numerous sensor network. This adds added security measure to network and eliminate re-authentication and tracing. A amount of methods have been planned newly to resolve positions issues of sensors but insufficient to provision antagonistic and dynamic environments as designs are lone for static environments. Work propose efficient node authentication and key talk protocol that slim furs overhead in node re-authentication and also eases difficulty of localization nodes..	A new Protocol for re-authentication is been proposed which is new fresh idea.	Need to be tested for large and heterogeneous networks.	proposed protocol will be the efficient solution to increase the lifetime of sensor network
12	Shuhas patil	projected system forms a Hierarchical Cluster Topology & by test assessed to validate its efficiency in noticing and stopping professionally Black Hole attacks.	**1.**Hierarchical Cluster Topology **2.**Single and Cooperative Black Hole Attack **3.** Black Hole Attack Detection and Prevention Using Proposed Trust Model.	Tested in simulation	Large scale test bed needs to be taken .
13	Shuhas patil	Mobile sensor knobs are key precondition for many environmental and non-joined requests of WSN. key impartial of this effort is to spread security of roving nodes to achieve secure direction-finding in WSN.	1. Phase 1: Determination and discovery of main nodes. 2. Phase 2: Main nodes communication set-up. 3. Phase 3: Main nodes distribution of authentication	Tested for distance based metric could be tested for no No.of nodes	Clustering can bring more better results

			Keys. 4. Phase 4: Primary authentication of slave nodes. 5. Phase 5: Secondary authentication of slave nodes		

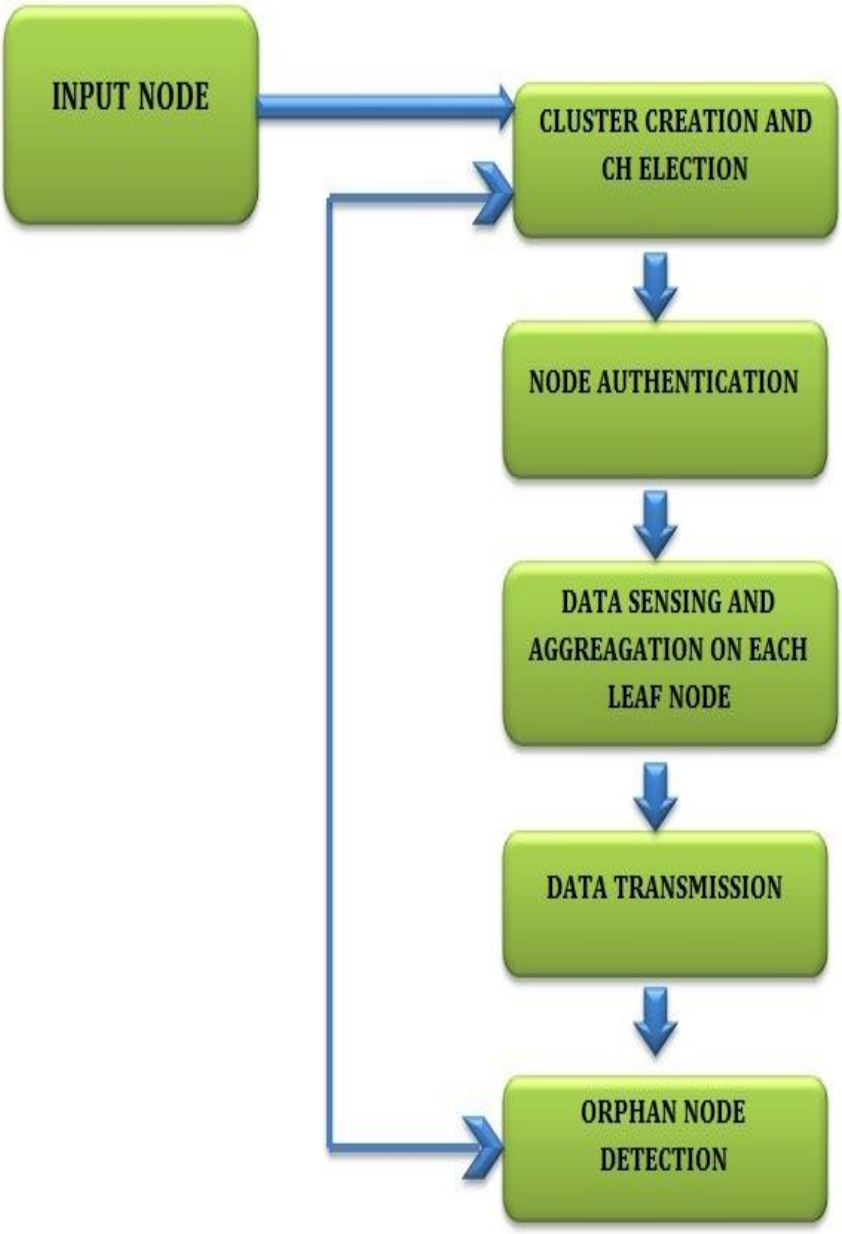

Fig 3: Proposed System Architecture

4. PROPOSED SYSTEM

❖ Work 1

Proposed Algorithm

Input: Generate Nodes network **{N1, N2, N3, N4……..}.**

addNode.setModel(new javax.swing.DefaultComboBoxModel(new String[] { "N1","N2", "N3", "N4", "N5", "N6", "N7", "N8", "N9", "N10","N11"}));

Set_baseStation ();

Process: **Clustering of nodes ()** // group//
Cluster head ()// election algorithm//
1. Node –power
2. C1:n2, n3 {5, 3, 2}→5
Authentication ()
Logger.getLogger(N1.class.getName()).log(Level.SEVERE, null, ex);
3. Sha1 Process

```
Public void processTheBlock (byte[] work, int H[], int K[]) {

        int[] W = new int[80];
        for (int outer = 0; outer < 16; outer++) {
           int temp = 0;
           for (int inner = 0; inner < 4; inner++) {
              temp = (work[outer * 4 + inner] & 0x000000FF) <<
(24 - inner * 8);
              W[outer] = W[outer] | temp;
           }
        }
        for (int j = 16; j < 80; j++) {
           W[j] = rotateLeft(W[j - 3] ^ W[j - 8] ^ W[j - 14] ^ W[j -
16], 1);
        }
        A = H[0];
        B = H[1];
        C = H[2];
        D = H[3];
        E = H[4];
        for (int j = 0; j < 20; j++) {
           F = (B & C) | ((~B) & D);
           //    K = 0x5A827999;
           temp = rotateLeft(A, 5) + F + E + K[0] + W[j];
           System.out.println(Integer.toHexString(K[0]));
           E = D;
           D = C;
           C = rotateLeft(B, 30);
           B = A;
           A = temp;
        }
 for (int j = 20; j < 40; j++) {
           F = B ^ C ^ D;
           //   K = 0x6ED9EBA1;
           temp = rotateLeft(A, 5) + F + E + K[1] + W[j];
           System.out.println(Integer.toHexString(K[1]));
           E = D;
           D = C;
           C = rotateLeft(B, 30);
           B = A;
           A = temp;
         }
        for (int j = 20; j < 40; j++) {
           F = B ^ C ^ D;
           //   K = 0x6ED9EBA1;
           temp = rotateLeft(A, 5) + F + E + K[1] + W[j];
           System.out.println(Integer.toHexString(K[1]));
           E = D;
           D = C;
           C = rotateLeft(B, 30);
           B = A;
           A = temp;
        }
```

5.Hash key ---hash value

```
try {
            Digest digester = new Digest();
            String z = string;
            System.out.println("Message: " + z);
            jTextBrowse.setText("");
catch (NoSuchAlgorithmException e)
  {
     e.printStackTrace();
  }
            byte[] dataBuffer = (z).getBytes();
            thedigest = digester.digestIt(dataBuffer);
            jTextOutput.setText(thedigest);
            String hashvalue = thedigest;
            System.out.println("Output: " + thedigest);
         //   DBUtils.addHashValue(thedigest,z);
catch (Exception ex) {
        }
```

6. Hash value to node →hash value .

7. Compare (h1, h2);

8. Delay Abs ();

6. Research Evaluation of Work

Proposed Work has been evaluated for Security and Cluster generation Time Complexity

Table 1: Research Results

Parameter	**Algorithm1[SHA1]**
Authentication overhead[n4,n3,n2n1]	4.56
Authentication overhead[n5,n7,n2,n8]	4.32
	4.5(Avg)

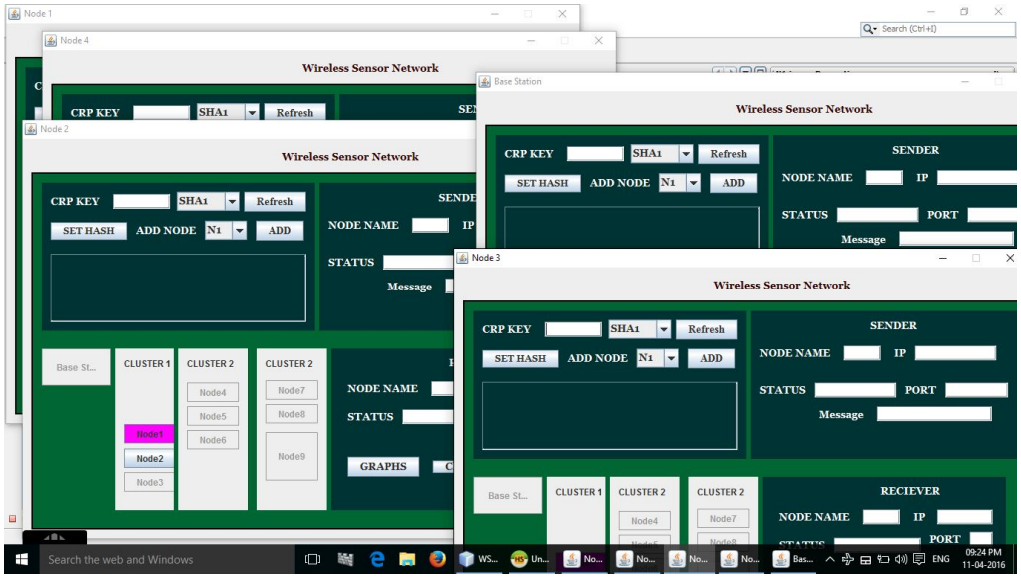

Fig1: Research work Snapshot 1

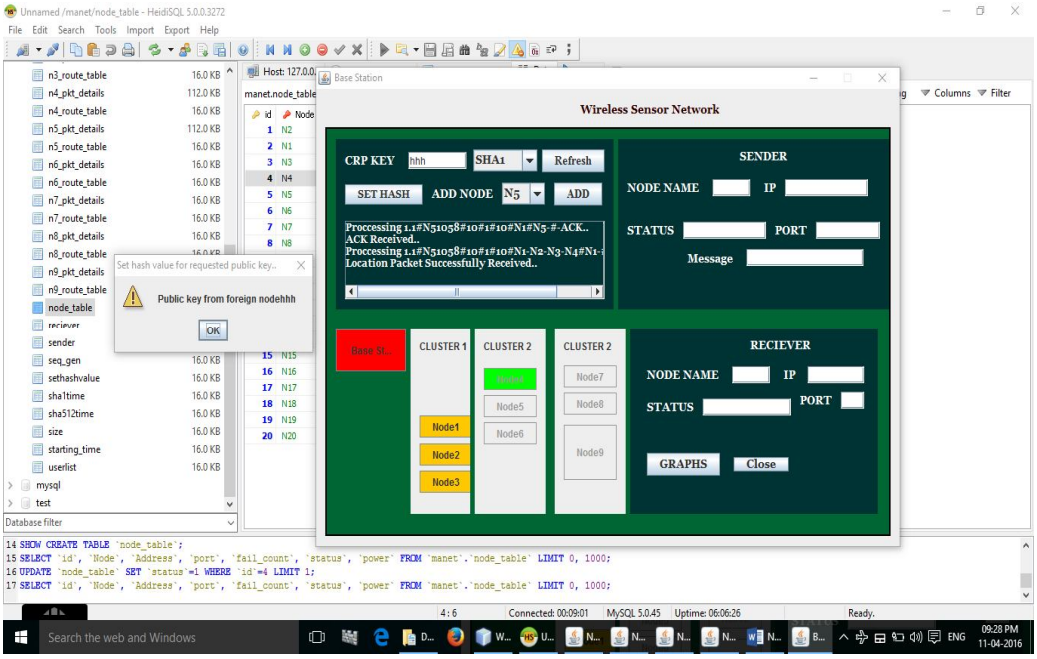

Fig2: Research work Snapshot 2

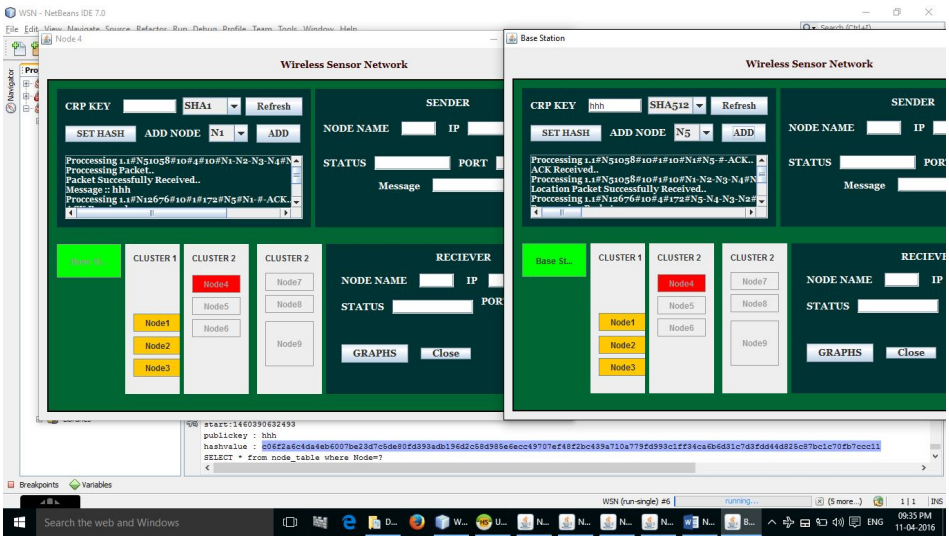

Fig3: Research work Snapshot 3

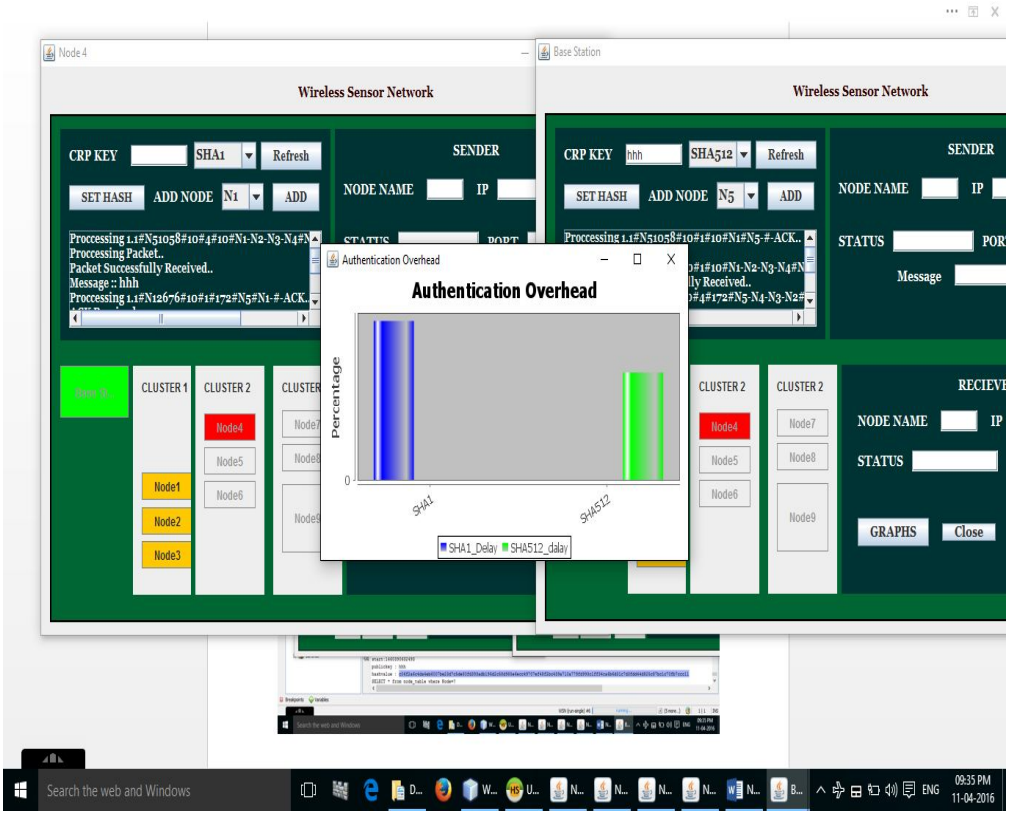

Fig4: Research work Snapshot 4

6. CONCLUSION

System has been developed for small WSN with test of 10 nodes the delay found here is 4.5 which can be reduced with more faster and better security mechanism like SHA512 algorithm. Also Network needs to be tested for heterogeneous network.

Acknowledgement

I acknowledge Prof. Dr. Shuhas Patil for his valuable guidance on every work of M.Tech Project. I Thanks Prof. Anand Bhalerao our principle & HOD Prof. Dr. Devendra Singh Takhore for paper publication, without his efforts this work would have not been possible

References

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

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

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

[4] 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.

[5] 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.

[6] http://wsnl.stanford.edu/tutorial.html.

[7] Rebecca Ingram, Tsvetomira Radeva, PatrickShields, Saira ViqarJennifer E. Walter,Jennifer L. Welch, "A Leader Election Algorithm for Dynamic Networks with Causal Clocks" distributed computing manuscript[online] http://groups.csail.mit.edu/tds/papers/Radeva/Radeva-etal.pdf.

[8] Wendi B. Heinzelman, Member, IEEE, Anantha P. Chandrakasan, Senior Member, IEEE, and Hari Balakrishnan, Member, IEEE , "An Application-Specific Protocol Architecture for Wireless Microsensor Networks" , IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 1, NO. 4, OCTOBER 2002.

[9] Huang lu, student member, ieee, jie li, senior member, ieee, and mohsen guizani, fellow, ieee, secure and efficient data transmission for cluster-based wireless sensor networks" , ieee transactions on parallel and distributed systems, vol. 25, no. 3, march 2014.

[10] P. Rajeshwari, B. Shanthini and Mini Prince, "Hierarchical Energy Efficient Clustering Algorithm for WSN" , Middle-East Journal of Scientific Research 23 (Sensing, Signal Processing and Security): 108-117, 2015, ISSN 1990-9233© IDOSI Publications, 2015 DOI: 10.5829/idosi.mejsr.2015.23.ssps.30.

[11] G. M. Edake G. R. Pathak ; S. H. Patil, "A Hybrid Novel Perspective of Secure Routing in Wireless Sensor Networks", Indian Journal of Science and Technology, Vol 9(10), DOI: 10.17485/ijst/2016/v9i10/88908, March 2016

AUTHORS

Scholar. Jubber Salim Nadaf is currently pursuing M.Tech (Computer) from Department of Computer Engineering, Bharati Vidyapeeth Deemed University College of engineering Pune, India. He received his B.E (Computer) Degree from Shivaji University LNBC Institute Of Engg & Technology Satara, Maharashtra, India. His area of interest include Network security & Wireless Sensor Network

Prof. Dr.Shuhas H Patil is working as a Professor in Computer Engineering Department at Bharati Vidyapeeth University College of engineering, Pune, Maharashtra, India. He received his Ph.D (Computer) degree from Bharati Vidyapeeth University College of Engineering, Pune. His research interests include Computer Network, Network Security, WLAN Security. He attended more than 100 plus national and international conferences and published papers in IEEE ACM and renowned Journals.