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**

SET for CWSN Using Election Algorithm for Authentication and Security Using SHA512

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

Transmitting data on Wireless sensor network has been challenging task. Wireless sensor Networks (WSN's) can be optimized and made better to perform with cluster formation. This research is extension to previous research of clustering WSN's for secured transmission of data. The Proposed system is ABS (attribute based System) and ABOOS (attribute based Offline Online System) as core base of system. The System is designed and implemented with Election algorithm for Authentication and SHA-1 and SHA512 for security purpose. Results analysis presents a better system with better cluster generation process and advanced industry standard security with SHA Algorithm .Previous survey analysis suggests that sha1 and MD5 are crack able and hack prone. Research work has been evaluated on Time Delay and comparative analysis of SHA-1 and SH512, presenting better efficiency of SH512 over SHA1. The Experimental results show time delay on 4.5 avg for SHA and 1.5 for SHA512 providing best security mechanism..

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

1. INTRODUCTION

WSN is system of geographically distributed nodes to monitor temperature, sound and various events [2]. Nodes in network sense and communicate data across network facilitate communication and data transfer. Though this technology comes with certain limitations like efficiency and security. Security is today primary important and necessary factor followed by Effective Communication of data across nodes.[2,3,6,].

Transmission of Data is been done in network via cluster generation to achieve scalable network, maximizing node lifetime work time, reduction to bandwidth by mutual communication among nodes [3]. Cluster Head (CH) are generated in cluster for communicating and sending data in network via base station. This mechanism has been opted in numerous research works and been activate area of research in Wireless sensor networks

A cluster Head aggregates data to transfer and sends to base station [5,7] presented low energy protocol with effective and influential CWSN termed as LEACH. This protocol increases life of network. Various other protocols have been presented like APTEEN, PEACH [4,5] on similar lines to LEACH. Summarized examination on CWNS and protocols used in their development present that CWSN's Architecture is complicated.[3]

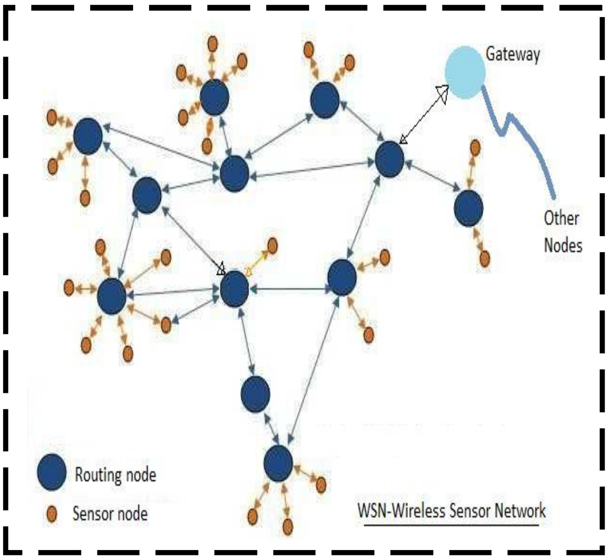


Fig1: Wireless Sensor Network

Merging of many contributing technologies Evolved in WSN-:

A. **Circuits:** Development in circuits technology has contributed to WSN Low power

- **[1.]** On chip sensors/MEMS.
- **[2.]** Miniature Size.
- **[3.]** Lowe-cost Imaging.
- **[4.]** Energy Scavenging.

B. **Networking:** Networking domain has been flatform and major research domain under WSN. The research has been boosted with following technologies.

- **[1.]** Self-configuring network.
- **[2.]** Scalability.
- **[3.]** Ad-hoc Network.
- **[4.]** Hybrid Network.
- **[5.]** Distributed Routing and Scheduling.

C.Wireless:

[1.] Multi-Hop Routing.
[2.] Energy Efficiency.
[3.] Very Low duty Cycle Efficient MAC.
[4.] Cooperative Communication.

D. Computation:

[1.] Processing power.
[2.] Embedded Software.
[3.] Collaborative Processing methods.
[4.] On board Processing.

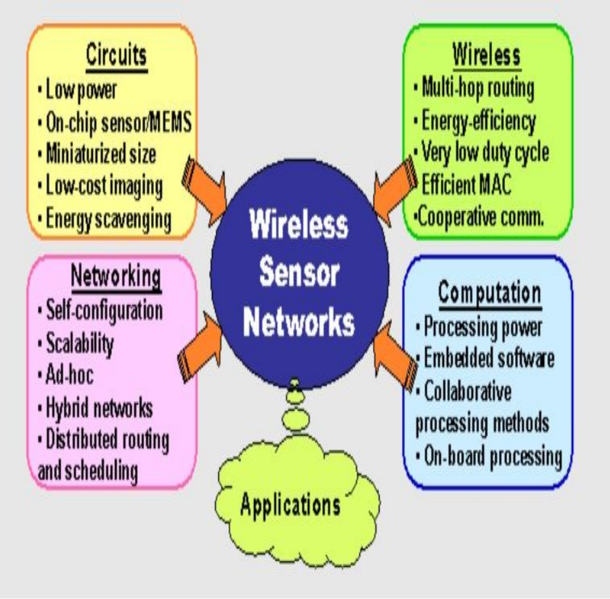


Fig2: WSN Research and technologies Evolved [10]

2. BACKGROUND KNOWLEDGE

1.1 WSN perspective and Characteristics [6]

- ❖ deployed for precise sensing application just not merely for communication drives
- ❖ Energy feasting chief issue to persist networks lifetime: hard environments deployment, huge number of nodes.
- ❖ Co-operative work of node for common task.
- ❖ Transmission of data on lower bandwidth.
- ❖ Redundancy if denser deployment.
- ❖ At times Node fail, change in topology.
- ❖ Memory resources and computing with limit value of power.
- ❖ Optimization on energy use than BW or Throughput constraints.

1.2 WSN Additional Characteristics [6]

- ❖ Self-Configuration: In large deployments.
- ❖ Scalability: coverage variance.
- ❖ Redundancy handling: failure of node is handled.
- ❖ Localized procedures: data sharing from node to node then direct long distance.
- ❖ Functional Cluster: sensing-processing-communication task.
- ❖ Prone to inaccurateness: devices and hard environments bring inaccurateness.
- ❖ Compared to other wireless network Primacies and metrics are precisely dissimilar.
- ❖ Tune up of Traditional WN techniques to special one is not possible.
- ❖ Require Design approach shift.

1.3 WSN Design Approach [6]

- ❖Design approach not for pure communication scheme.
- ❖Design view not pure algorithm.
- ❖No Technique to reconcile.

1.4 WSN Note

- ❖Local Exchange of data.
- ❖Distributed processing.
- ❖Communication of Information

3. TABULATED LITERATURE SURVEY

Sr.no	Author	Abstract	Technique	Limitations	Scope
1	Heinzelman	**Abs:** Networking with sensor node helps monitor environment by aggregated data from nodes. Protocols require to be latent and energy effective. This work focus on energy effective cluster focused LEACH (low energy adaptive clustering hierarchy), achieving better life.	**Algo:**LEACH has Self Organizing method for nodes. Adaptive cluster are generated. **Process:** Even Energy distribution.	LEACH Constraint based protocol this is has been major limitation.	Intra-cluster communication effective bandwidth usage.
2	Oliveira	Abs: Decrease in system delay with increase throughput and energy in data aggregation is	**Algo:**SeLEACH algorithm has been developed based on	Overhead of seLEACH	Work on distance estimates is scope

		shown by CSN(cluster sensor Network). Dynamic Nature of System makes security measures inadequate in LEACH protocol implementation. Proposed work implements random key predistribution for achieving security. SeLEACH gives authenticity with integrity, confidentiality based system.	LEACH. **Process**: includes µTESLA, Random key predistribution (main Technique).	is much than LEACH. It has diverse tradeoffs for memory energy use	
3	Abbasi	**Abs:** WSN's have been widely used in many applications like disaster management, surveillance, border protection.to achieve scalability nodes are cluster in non duplicate manner This work presents procedures in WSN's for clustering and comparative examination on their complexity scalability, cluster overlapping with support for node stability.	**Algo:**Algorithms presented are **1**.Varaiable convergence time 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):	Survey has been in best tabulated format but not comparative analysis between algorithms	Clustering brings scalability to WNS's.proper design and development of WSN would make system scalable.
4	Zhang	Security is been neglected by Routing protocols in WSN. Key management is been widely used in WSN but fails for dynamic 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.	**Algo:** LEACH is presented, it is self-organizing dynamic cluster generation algorithm. RLEACH is been developed **Process:** **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 than LEACH .could be minimized.	2 tier System is found to be best ,this deign can be extended to 3 tier and made better.
5	Pradeepa	Sensor networks have wide applications in military, surveillance and are deployed in hard areas with requiring human intervention. Cluster generation method increases capability of network. Article focuses on design and issues	Algo: article presents issues to design and algo. 11. Node mobility. 12. Traffic load 13. Load balancing. 14. Dynamic	Research work is been tested in simulation which at times fail with false	Algorithms developed are mostly for Flat network and fail for dynamic one. Development of algo and system design we show

		related to WSN development.	cluster control. 15. Inter cluster co-ordination. 16. Data Aggregation. 17. Fault Tolerance. 18. Scalability. 19. No.Cluster,Cluster G time, 20. Node heterogeneity. 21. Self and reconfiguration. All Above are major issues related to design and algo of WSN and need better design and clustering to handle them.	values.	consider clustering issues.
7	Rebecca	Leader selection procedure in dynamic network is ben presented. Algorithm ensures that even though change in topology and network dynamics for selecting a leader in network with TORA as base selection process. Algorithm brings stability to network.	Algo: presents and focuses on distributed algorithms and issues related to them are discussed in selection of leader node.	Research work with no proof ,as no values are been providesd.Pure Theoretical work	Election Algorithm is procedure that grantees selection of leader in dynamic network and its implements has scope for betterment.
8	Wendi	WSN allow user to aggregate information and intelligently develop communication systems. This article LEACH a protocol architecture for energy effective and better clustering algorithm for application specific domain.	Algo: LEACH is presented. Process: 1. Cluster Head Selection Algorithms. 2.Cluster-Formation Algorithm. 3.Steady-State Phase 4. LEACH-C: BS Cluster Formation	Algorithm is constraint based.	Intra Cluster Management is needed.
9	Rajeshwari	WSN is group of large low micro sensors in where users send receive msg .Energy is vital constraint in WSN. Paper focuses on HEEC(Hierarchical Energy Efficient Clustering Algorithm).better life and reducing of energy is achieved in WSN with HEEC. New Clustering algo node grouping election of cluster head. Re –election is implemented	Algo: The proposed algorithm for HEEC is used to maximize life of network is as following. Process: 7. Cluster Formation for WSN 8. Cluster Head Selection 9. Routing Tree Construction 10. Re-Electing	The work is simulation work hence needs to be tested in real as values may vary in real time.	Security mechanism can be enhance with additional security algorithm with industry standards.

		reducing data loss and load balancing access problem	Cluster Head. 11. Data Transfer.		
10	Huang	Security is major issue in WSN's. clustering is practical method to uplift performance.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.	Algorithm IBS and IBOS Process: **3.** IBS Setup WSN Extraction. Signature signing Verification **4.** IBOS Setup WSN Extraction. Offline signing Signature signing verification	tested for 100 nodes with large number of assumption been made.	Digital signature based ,can be extended to attribute based system ABS ones.
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 Keys. 4. Phase 4: Primary authentication of slave nodes. 5. Phase 5: Secondary authentication of slave nodes	Tested for distance based metric could be tested for no No.of nodes	Clustering can bring more better results

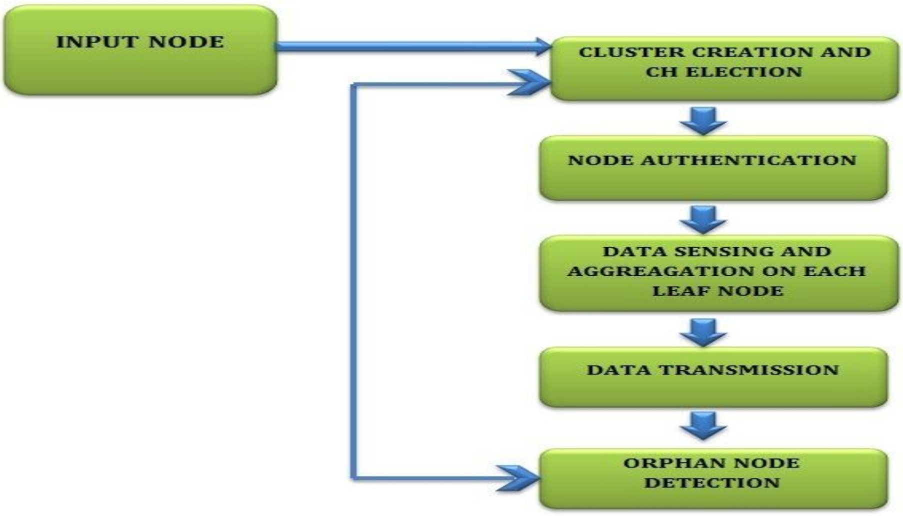

INPUT NODE
CLUSTER CREATION AND CH ELECTION
NODE AUTHENTICATION
DATA SENSING AND AGGREAGATION ON EACH LEAF NODE
DATA TRANSMISSION
ORPHAN NODE DETECTION

Fig 3: Proposed System Architecture

3.2 Problem Definition

Design and Develop A Cluster Wireless Sensor Network and Implement SET (Secure Effective Transmission) in Network. Provide Object Oriented Design Approach.

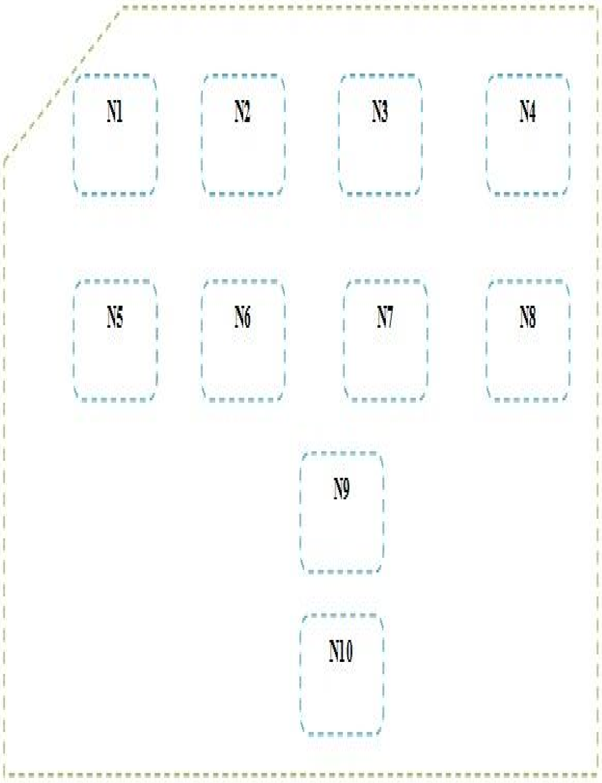
3.2.1 Issues To Handle

1. Security : develop better Security algorithm with lower complexity
2. Clustering: A Better Cluster Generation algorithm implementation with lesser rise to issues to cluster generation achieving scalable and mobile system.

4. PROPOSED SYSTEM

4.1System Design: For Experimental purposes system is been developed with set of 10 nodes and virtualization is been done in JAVA Environment

Assumptions: A Base station node is been set N2 we assume Heterogeneous network at this time which will be extended future.



4.2 Algorithmic procedure

This work compares SHA1 and SHA512 algorithm working and Demonstrates that 512 is better Approach to security than SAH1 as of demonstrated in our previous work.

Work 2

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;
            }
        }

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 = 40; j < 60; j++) {
            F = (B & C) | (B & D) | (C & D);
            //   K = 0x8F1BBCDC;
            temp = rotateLeft(A, 5) + F + E + K[2] + W[j];
            E = D;
            D = C;
            C = rotateLeft(B, 30);
            B = A;
            A
 for (int j = 60; j < 80; j++) {
            F = B ^ C ^ D;
            //  K = 0xCA62C1D6;
            temp = rotateLeft(A, 5) + F + E + K[3] + W[j];
            E = D;
            D = C;
            C = rotateLeft(B, 30);
            B = A;
            A = temp;
          }

          H[0] += A;
          H[1] += B;
          H[2] += C;
          H[3] += D;
          H[4] += E;


          int n;
          for (n = 0; n < 16; n++) {
            System.out.println("W[" + n + "] = " +
toHexString(W[n]));
          }
          System.out.println("H0:" + Integer.toHexString(H[0]));
          System.out.println("H0:" + Integer.toHexString(H[1]));
          System.out.println("H0:" + Integer.toHexString(H[2]));
          System.out.println("H0:" + Integer.toHexString(H[3]));
          System.out.println("H0:" + Integer.toHexString(H[4]));
       }
```

4. sha521 process

```
Try {
      System.out.println("In SHA512..######"+salt);
      MessageDigest md = MessageDigest.getInstance("SHA-
512");
      md.update(salt.getBytes("UTF-8"));
      byte[] bytes = md.digest(passwordToHash.getBytes("UTF-
8"));
      StringBuilder sb = new StringBuilder();
      for(int i=0; i< bytes.length ;i++)
      {
        sb.append(Integer.toString((bytes[i] & 0xff) + 0x100,
16).substring(1));
      }
      generatedPassword = sb.toString();
   }



        } catch (Exception ex) {
        }
```

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 ();

5.Evaluation of Work

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

Table 1: Research Results

Parameter	**Algorithm1[SHA1]**	**Algorithm2[SHA512]**
Authentication overhead[n4,n3,n2n1]	4.56	1.45
Authentication overhead[n5,n7,n2,n8]	4.32	2.45
	4.4(Avg)	**1.6(avg)**

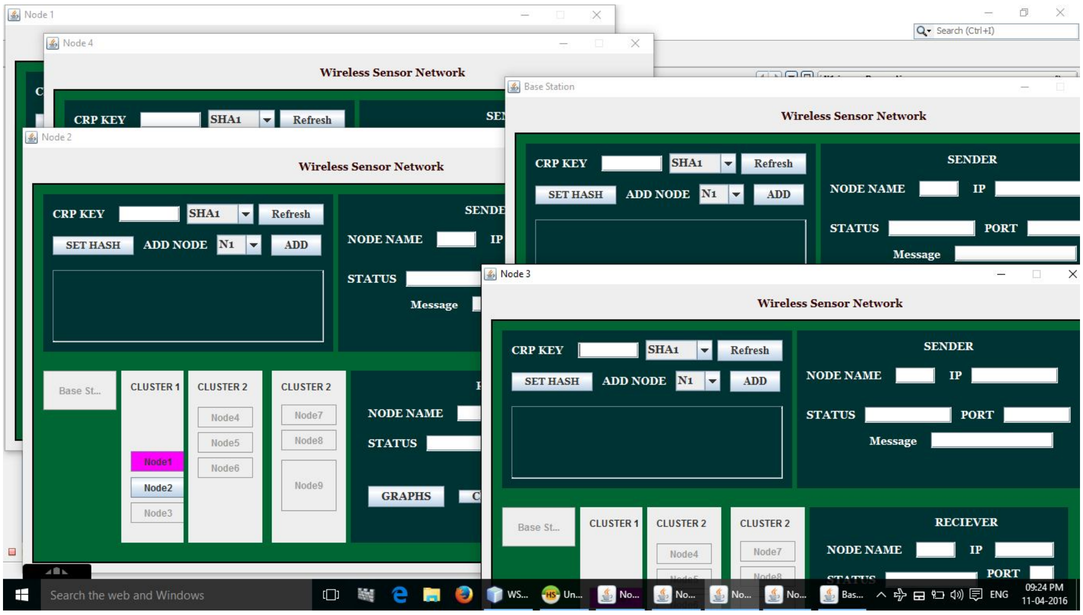
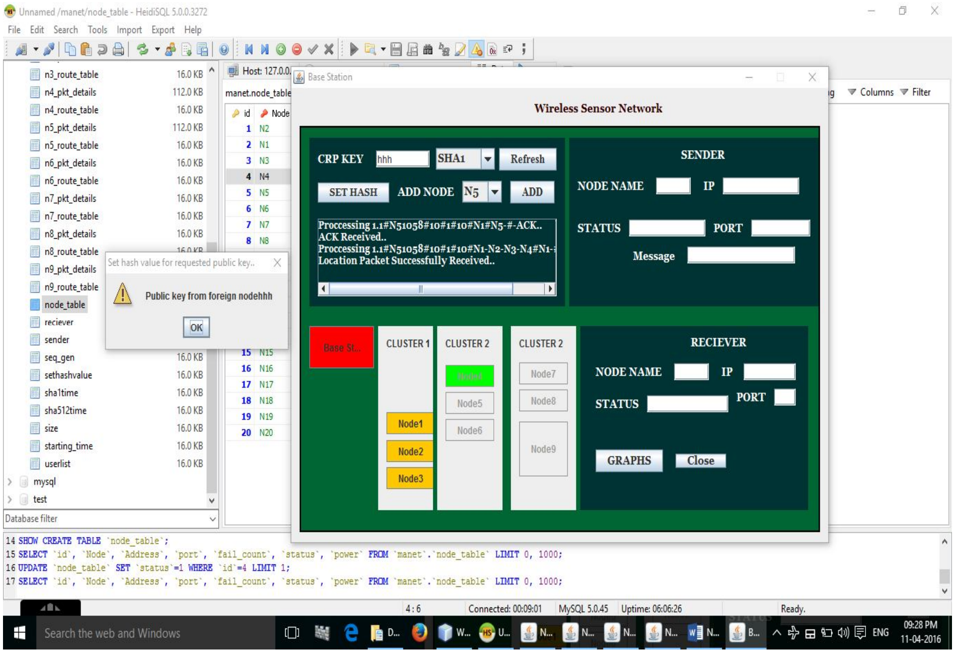


Fig1: Research work Snapshot 1



CRP KEY: hhh

```
Proccessing 1.1#N51058#10#1#10#N1#N5-#-ACK..
ACK Received..
Proccessing 1.1#N51058#10#1#10#N1-N2-N3-N4#N1-i
Location Packet Successfully Received..
```

Set hash value for requested public key..

Public key from foreign nodehhh

OK

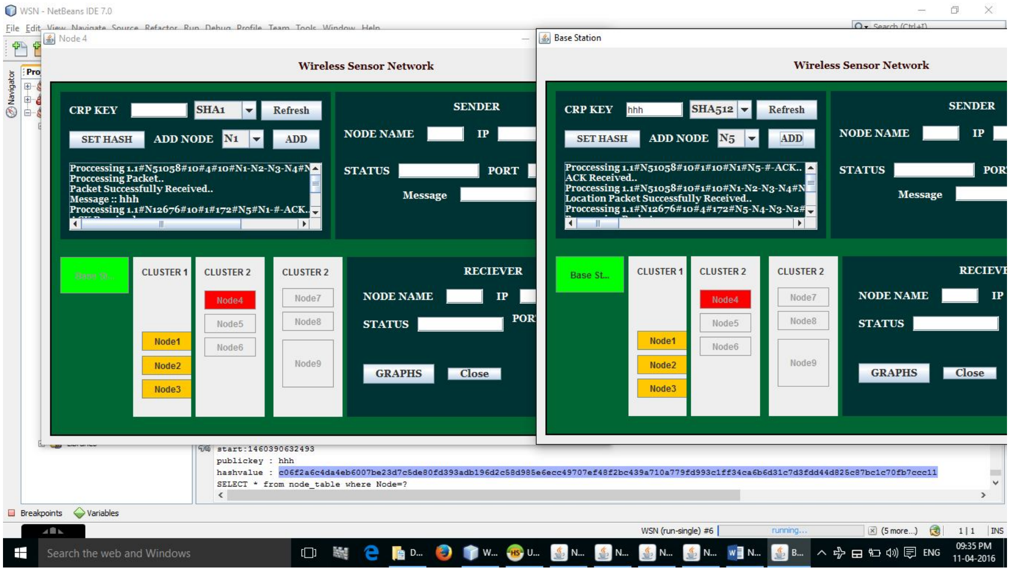
n3_route_table	16.0 KB
n4_pkt_details	112.0 KB
n4_route_table	16.0 KB
n5_pkt_details	112.0 KB
n5_route_table	16.0 KB
n6_pkt_details	16.0 KB
n6_route_table	16.0 KB
n7_pkt_details	16.0 KB
n7_route_table	16.0 KB
n8_pkt_details	16.0 KB
n8_route_table	16.0 KB
n9_pkt_details	
n9_route_table	
node_table	
reciever	
sender	
seq_gen	16.0 KB
sethashvalue	16.0 KB
sha1time	16.0 KB
sha512time	16.0 KB
size	16.0 KB
starting_time	16.0 KB
userlist	16.0 KB
mysql	
test	

id	Node
1	N2
2	N1
3	N3
4	N4
5	N5
6	N6
7	N7
8	N8
15	N15
16	N16
17	N17
18	N18
19	N19
20	N20

```
14 SHOW CREATE TABLE `node_table`;
15 SELECT `id`, `Node`, `Address`, `port`, `fail_count`, `status`, `power` FROM `manet`.`node_table` LIMIT 0, 1000;
16 UPDATE `node_table` SET `status`=1 WHERE `id`=4 LIMIT 1;
17 SELECT `id`, `Node`, `Address`, `port`, `fail_count`, `status`, `power` FROM `manet`.`node_table` LIMIT 0, 1000;
```

4 : 6 Connected: 00:09:01 MySQL 5.0.45 Uptime: 06:06:26 Ready.

Fig2: Research work Snapshot 2



WSN - NetBeans IDE 7.0

Node 4 — Wireless Sensor Network

CRP KEY: SHA1; ADD NODE: N1

```
Proccessing 1.1#N51058#10#4#10#N1-N2-N3-N4#N
Proccessing Packet..
Packet Successfully Received..
Message :: hhh
Proccessing 1.1#N12676#10#1#172#N5#N1-#-ACK..
```

Base Station — Wireless Sensor Network

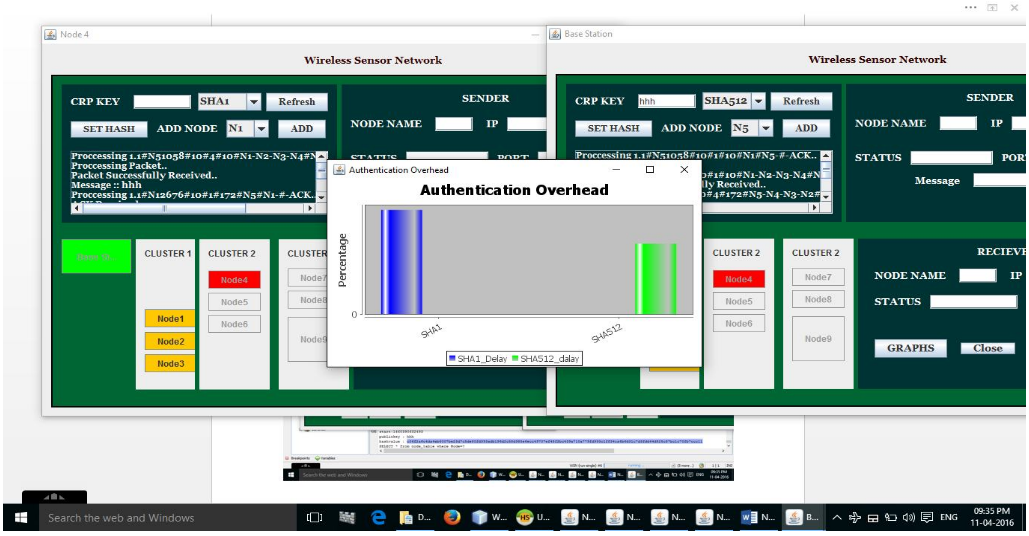
CRP KEY: hhh; SHA512; ADD NODE: N5

```
Proccessing 1.1#N51058#10#1#10#N1#N5-#-ACK..
ACK Received..
Proccessing 1.1#N51058#10#1#10#N1-N2-N3-N4#N
Location Packet Successfully Received..
Proccessing 1.1#N12676#10#4#172#N5-N4-N3-N2#
```

```
start:1460390632493
publickey : hhh
hashvalue : c06f2a6c4da4eb6007be23d7c5de80fd393adb196d2c58d985e6ecc49707ef48f2bc439a710a779fd993c1ff34ca6b6d31c7d3fdd44d825c87bc1c70fb7ccc11
SELECT * from node_table where Node=?
```

WSN (run-single) #6 running... (5 more...) 1 | 1 INS

Fig3: Research work Snapshot 3



Node 4 — Wireless Sensor Network

CRP KEY: SHA1; ADD NODE: N1

```
Proccessing 1.1#N51058#10#4#10#N1-N2-N3-N4#N
Proccessing Packet..
Packet Successfully Received..
Message :: hhh
Proccessing 1.1#N12676#10#1#172#N5#N1-#-ACK..
```

Base Station — Wireless Sensor Network

CRP KEY: hhh; SHA512; ADD NODE: N5

```
Proccessing 1.1#N51058#10#1#10#N1#N5-#-ACK..
```

Fig4: Research work Snapshot 4

6. CONCLUSION

Proposed work is a small Effort in WSN. Research outcomes show that system has better security mechanism and remains our novelty as no such SHA1 or SHA512 implements are been done which remain industry standard algorithm ,clustering bring in scalable System and Election algorithm helps to elect better cluster head and transmission of data is achieved in good fashion. In future we would like to test system on evaluation parameters like energy consumption and work on intra clustering and test the system for set of large nodes like set of 50 or more.

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.