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

Scholar. Jubber Salim Nadaf¹, Prof. Dr. Shuhas Patil ²

¹ Dept. Computer Engineering Bharati Vidyapeeth Deemed University College of Engineering
Pune-41Maharashtra

²Dept. Computer Engineering Bharati Vidyapeeth Deemed University College of Engineering
Pune-41Maharashtra

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 in 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 in 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

Applications OF WSN:

Fig2: WSN Application Area

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

2.1 WSN [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 100 or 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:

3. TABULATED LITERATURE SURVEY

<table>
<thead>
<tr>
<th>Sr.n o</th>
<th>Author</th>
<th>Abstract</th>
<th>Technique</th>
<th>Limitation(s)</th>
<th>Scope</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Heinzelma n</td>
<td>work focus on energy effective cluster focused LEACH (low energy adaptive clustering hierarchy), achieving better life.</td>
<td>[1.] Adaptive cluster.</td>
<td>Intra cluster communication</td>
<td>Constraint based.</td>
</tr>
</tbody>
</table>
| 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                  |
<p>| 3     | Abbasi      | This work presents procedures in WSN’s for clustering and comparative examination on | [1.] Variaable convergence time | No comparativ                         | WNS’s better design    |</p>
<table>
<thead>
<tr>
<th>Page</th>
<th>Author</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>167</td>
<td>Zhang</td>
<td>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.</td>
</tr>
<tr>
<td>168</td>
<td>Pradeepa</td>
<td>Article focuses on design and issues related to WSN development.</td>
</tr>
<tr>
<td>169</td>
<td>Rebecca</td>
<td>Leader selection procedure in dynamic network is presented. TORA brings scalable and stable system.</td>
</tr>
<tr>
<td>170</td>
<td>Wendi</td>
<td>LEACHES a protocol architecture for energy effective and better clustering algorithm for application specific domain.</td>
</tr>
</tbody>
</table>

**Algorithms:**

1. Linked cluster Algorithms (LCA)
2. Adaptive clustering
3. Random competition based clustering
4. Hierarchical clustering
5. Energy-Efficient Hierarchical Clustering (EEHC)
6. Algorithm for Cluster Establishment
7. Hybrid Energy-Efficient Distributed Clustering (HEED):

**Overhead:**

- More than 3 tier design

**Research Work:**

- Development of algorithm and system design we show consider clustering issues.

**Algorithm Evaluation:**

- Algorithm developed are mostly for Flat network and fail for dynamic one. Development of algorithm is constraint based.
<table>
<thead>
<tr>
<th>No.</th>
<th>Author</th>
<th>Description</th>
<th>Implementation</th>
<th>Testing/Validation</th>
<th>Conclusion</th>
</tr>
</thead>
</table>
| 9   | Rajeshwar  | 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. | proposed protocol will be the efficient solution to increase the lifetime of sensor network |
| 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  
| 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 |
4. Phase 4: Primary authentication of slave nodes.
5. Phase 5: Secondary authentication of slave nodes.

Fig 3: Proposed System Architecture
4. PROPOSED SYSTEM

Proposed Algorithm

- Work 1

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

```java
```

Process: Clustering of nodes () // grouping

1. Node - power
2. C1:n2, n3 (5, 3, 2) ➔ 5

3. Sha1 Process

```java
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++) {
        }
        A = H[0];
        B = H[1];
        C = H[2];
        D = H[3];
        E = H[4];
        for (int j = 20; j < 40; j++) {
            F = (B & C) | ((~B) & D);
            // K = 05A827999;
            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 = 06ED9EB1;
            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

```java
try {
    Digest digester = new Digest();
    String z = string;
    System.out.println("Message: "+z);
    jTextBrowse.setText(""+z);
    System.out.println("Output: "+thedigest);
    DBUtils.addHashValue(thedigest,z);
} catch (NoSuchAlgorithmException e) {
    e.printStackTrace();
}
```

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Algorithm1[SHA1]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication overhead[n4,n3,n2,n1]</td>
<td>4.56</td>
</tr>
<tr>
<td>Authentication overhead[n5,n7,n2,n8]</td>
<td>4.32</td>
</tr>
<tr>
<td></td>
<td>4.5 (Avg)</td>
</tr>
</tbody>
</table>

Fig1: Research work Snapshot 1

Fig2: Research work Snapshot 2
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


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.