AN IMPROVED SECURITY MECHANISM FOR WIRELESS SENSOR NETWORKS

Lokana S[1], Lokashree S[2], Dr.M.V.Sathyanarayana[3]

[12]pg Scholar, Rajeev Institute of Technology, Hassan, Karnataka, (India)
[3]director(Training&Placement), Dept Of Ece, Rajeev Institute of Technology,
Hassan, Karnataka, (India)

ABSTRACT

Secure data transmission is very important in wireless sensor networks.Clustering is one of the most effective way to increase the system performance of WSN. Wireless communication is one of the most important communication methods in our day to day life due to providing its devices with portability and rapid hardware cost reduction. A secure data transmission for cluster based WSNs are called SET-IBS and SET-IBOOS.In this paper the feasibility of the SET-IBS and SET-IBOOS protocols with respect to security analysis against major attacks is proposed.ECC algorithm is used for Encryption and Decryption. The calculations and simulations are also provided to illustrate the efficiency of the algorithm proposed.

Keywords: Clustering, Wireless Sensor Network, SET- IBS, SET-IBOOS.

I. INTRODUCTION

The wireless sensor network is comprised of small size, low power, and light weight, affordable wireless nodes called sensor nodes that are utilized in physical or environmental condition. The individual nodes have the capacity to sense their environments, which process the information data locally, and send the data to one or more collection points in a WSN. The sensor nodes will have the ability to communicate either among each other or directly with a base station. These types of nodes are heavily utilized in an agreed geographical area to self-organize into ad-hoc wireless networks to assemble and collect data. The ad hoc nature of sensor networks constitutes remarkable challenges with their reliability, efficiency and security. Hence, advanced security measures are required to address these unique sensor networks security challenges.The cost of data transmission is costlier than that of processing the data.

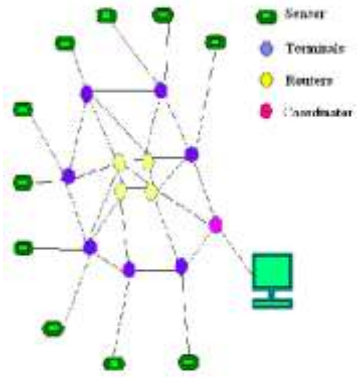


Fig: WSN Architecture

Efficient and reliable data transmission is one of the foremost issues for WSNs. Data in wireless sensor network are bound either downstream to nodes from a sink node or upstream to a sink node from nodes. Wireless sensor network are a kind of application specific network. Cluster Network consists of large number of Sensor Nodes that are grouped into different clusters. Each Cluster in network is comprised of a single Cluster Head (CH) sensor node that will be elected independently and cluster member nodes or leaf (non CH) joins the cluster that depends upon the receiving signal strength. Here, Cluster Head (CH) will get sensed data from the leaf (non CH) and combines the sensed data and then transfers it to the base station.

II. RELATED WORK

Wireless sensor networks (WSNs) have recently attracted much interest in the research community due their wide range of applications. Due to distributed nature of these networks and their deployment in remote areas, these networks are vulnerable to numerous security threats that can adversely affect their proper functioning. Hence; this problem is more crucial if the network is utilized for some mission-critical applications such as in a military. Accidental node failure is also very likely for deployment in real-life scenarios. Due to constraints in resources in the sensor nodes, older security mechanisms with a huge overhead in communication and computation are infeasible in sensor network. Therefore, Security in WSN is a highly challenging task [2].

A wireless sensor network (WSN) which is comprised of a large number of small sized sensors can be an efficient tool for assembling data in various kinds of environments. The data gathered by each and every sensor is relayed to the base station that forwards the data to end users. Clustering approach is introduced in WSNs since it has proved effectiveness to provide better data aggregation and also scalability for large sensor networks. Clustering approach conserves limited energy resources of the sensors [3].

Networking hundreds of inexpensive micro sensor nodes will allow users to effectively monitor remote environment by combining the data from the individual sensor nodes. Low-energy adaptive clustering hierarchy (LEACH) is an architecture for the micro-sensor networks which combines the ideas of media access and energy-preserving cluster-based routing together with the application-specific data aggregation to achieve excellent performance in terms of system latency, lifetime, and also application-perceived quality. LEACH includes a unique distributed cluster formation methodology that enables the self-organization of massive number of nodes as well as algorithms for adapting clusters and rotating cluster head positions to evenly share the energy load among all the nodes, and techniques to enable distributed signal processing to save communication resources [4].

WSNs are a class of ad hoc networks. They will find an increasing deployment in coming years, since they enable trustworthy monitoring as well as analysis of untested and unfamiliar environments. Advancements in technology have made it possible to have tiny, low powered sensor devices equipped with programmable computing, wireless communication capability, and multiple parameter sensing [5].

III. CLUSTER NETWORK ARCHITECTURE

Cluster wireless sensor networks have the following features:

- It includes two kinds of nodes:

Sensor nodes: These will have a limited energy and can sense their own residual energy.

Base Station (BS): These will not have any energy restriction.

- Sensor nodes will sense the environment at a fixed rate and they always have information to send to the BS.

- Cluster head CH will perform data aggregation and Base Station will receive the compressed data.
- All sensor nodes will use direct transmission or multi-hop transmission to communicate with the BS.
- The lifespan of sensor network is the total amount of time previous to the first sensor node runs out of power.

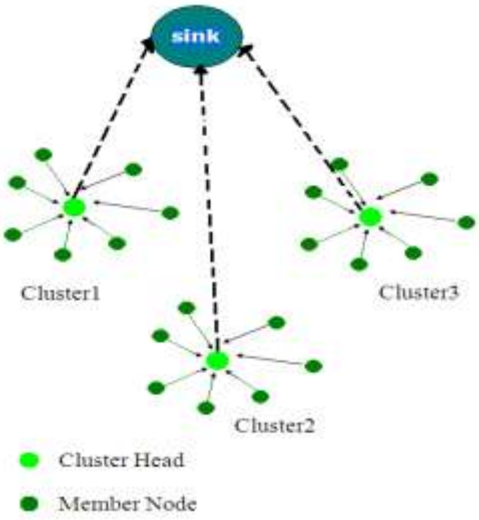


Fig: Cluster Network Architecture

IV. SECURITY IN WSNS

The security in wireless sensor networks includes:

Availability: The node must be able to utilize the resources and the network must be available for the flow of data.

Integrity: Assurance that the information is reliable and accurate.

Confidentiality: The set of rules limiting access to the information. The messages communicated from a sensor network must be confidential i.e. messages must be protected from attacker.

Authentication: Whether the messages are transferred from the node, it claims to be.

The major security attacks:

1. *Message deception*: The attacker modifies the message contents which violates integrity of the message.
2. *Traffic Analysis*: There is a high probability that the attacker analyze the communication patterns even if the message is encrypted.
3. *Selective forwarding*: The adversary may drop or delay the data flow.
4. *Sinkhole attacks*: The attacker attracts the traffic to a compromised node.
5. *Wormholes*: The attacker who is closer to the base station can completely disrupt the traffic by tunneling messages over a low latency link.

6: *False node*: The attacker adds a fake node to inject malicious data.

7. *Malfunctioning node*: The malfunctioning node generates inaccurate data which harms integrity of the sensor network especially if the node is cluster head.
8. *Passive information* Gathering: If the information from sensor networks are not encrypted, then the adversary can easily collect the information.

V. IBS AND IBOOS FOR CWSNS

Secure and efficient data transmission is exclusively significant and is demanded in many practical WSNs.Hence Secure and Efficient data Transmission (SET) protocols, called SET-IBS and SET-IBOOS are introduced, by using the Identity-Based digital Signature (IBS) scheme and the Identity-Based Online/Offline digital Signature (IBOOS) scheme. It is introduced in order to reduce the computation and storage costs to authenticate the encrypted sensed data, by employing digital signatures to message packets, which are systematic in communication and applying the key management for security and reliability. In both the protocols, pairing parameters are distributed and loaded before in all sensor nodes by the BS initially, that swamps the key escrow problem in ID-based crypto-systems.

5.1 The Proposed Set-Ibs Protocol

In SET-IBS scheme the time is split into consecutive time intervals. Time stamps are denoted by Ti for leaf-to-CH communication and Tt for BS-to-node communication. User’s public key is denoted by IDp under an IBS scheme. The respective private pairing parameters are preloaded in the sensor nodes during the protocol initialization. If a sensor node wishes to authenticate itself to other node, it need not obtain its private key at the starting of a new round. During node revocation, the BS broadcasts the compromised node IDs to all sensor nodes; each node then stores the revoked IDs within the current round. An additively homomorphic encryption scheme is adopted to encrypt the plaintext of sensed data; where in a specific operation is performed on the plaintext which is equivalent to the operation performed on the ciphertext. This method allows effective aggregation of encrypted data at the CHs and the BS and hence guarantees data confidentiality. In the protocol initialization, the base station performs the following operations of key predistribution to all the sensor nodes:

Setup phase:

Step1: Bs=>GS :< IDbs, Ti, nonce>

Step2: CHa=>GS :< IDa, Ti, adv, Za, Ca>

Step3: Lb→CHa:< IDa, IDb, Ti, join, Zb, Cb>

Step4: CHa=>GS :< Ida, Ti, sched (.., IDb/tb...), Za, Ca>

Steady-state phase:

Step5: Lb→CHb:< Ida, IDb, tb, Cb, Zb, Cb>

Step6: CHa→Bs :< IDbs, Ida, Ti, F, Za, Ca>

Description:

Step1: The BS broadcasts its information to all the nodes.

Step2: The elected CHs broadcast their information.

Step3: A leaf node joins the cluster of a CH a.

Step4: A CH a broadcasts the scheduled message to its members.

Step5: A leaf node b transmits the sensed data to its CH a.

Step6: A CH a transmits the aggregated data to the BS [6].

5.2 The Proposed Set-Iboos Archıtecture

In order to lower the computation and storage costs of signature signing process in the IBS scheme, SET-IBS is improved by the introduction of IBOOS for security in SET-IBOOS. The protocol is initialized in the similar manner as that of SET-IBS; the operations are as follows:

Setup phase:

Step1: Bs=>GS :< IDbs, Ti, nonce>

Step2: CHa=>GS :< IDa, Ti, adv, Ra, Za, Xa>

Step3: Lb→CHa :< IDa, IDb, Ti, join, Rb, Zb, Xb>

Step4: CHa=>GS :< Ida, Ti, alloc (.., IDb/tb ...), Ra, Za, Xa>

Steady-state phase:

Step5: Lb→CHb :< Ida, IDb, tb, Cb, Rb, Zb, Xb>

Step6: CHa→Bs :< IDbs, Ida, Ti, F, Ra, Za, Xa>

Description:

Step1: The BS broadcasts its information to all the nodes.

Step2: The elected CHs broadcast their information.

Step3: A leaf node joins the cluster of a CH a.

Step4: A CH a broadcasts the allocation message.

Step5: A leaf node b transmits the sensed data to its CH a.

Step6: A CH a transmits the aggregated data to the BS.

Notations:

=>,→ : Broadcast and unicast transmission.

Lb, Cha, GS :leaf node, Cluster Head, Set of sensor nodes.

Ti, tb : Time stamps denoting time slot for transmission in set up and steady phases.

Ida, IDbs : The IDs of sensor node a and the BS.

Cb, Fa : The encrypted sensed data of node b and the aggregated data of CH a.

adv,join,alloc,
sched :Message string types which denote the advertisement join_request,allocation messages and schedule messages.

<Za,Ca> :The ID based digital signature concatenated with data from node a.

<Za,Xa> :The online signature of node a concatenated with Data [6].

5.3 Enhancement Algorıthm

ECC algorithm is used. Elliptic curve cryptography (ECC) is an approach to the public-key cryptography which is based on the algebraic structure of elliptic curves over finite fields. One of the major benefits in comparison with non-ECC cryptography is that the same level of security is provided by keys of smaller size. Elliptic curves are applicable for encryption, digital signatures, pseudo-random generators and other tasks. They also are useful in integer factorization algorithms that have applications in cryptography.

Encryption

```
  Random          r = new Random ();
             BigIntegerP =BigInteger.probablePrime(3, r);
            Big Integer Q = BigInteger.probablePrime(3, r);
           Big Integer N =P.multiply (Q);
             Random rand3 = new Random ();
             Int kval= N.intValue ();
```

```
        Int kres=rand3.nextInt (kval-1);
        BigInteger k=BigInteger.valueOf (kres);
        BigInteger b1=k.multiply (P);
        BigInteger M=new BigInteger(msg.getBytes ());
        BigInteger b2=M.add (b1);
        Encmsg=b1+","+b2;
```

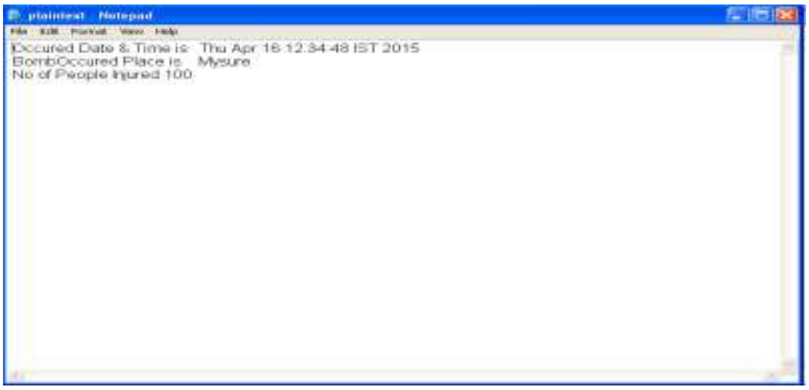
Decryption

```
String spt[]=encrypted_data.split(",");
        BigInteger b1=new BigInteger (spt[0]);
        BigInteger b2=new BigInteger (spt[1]);
        BigInteger m=b2.subtract (b1);
        Stringfiledata=NewString (m. toByteArray ());
            return filedata;
```

VI. RESULTS

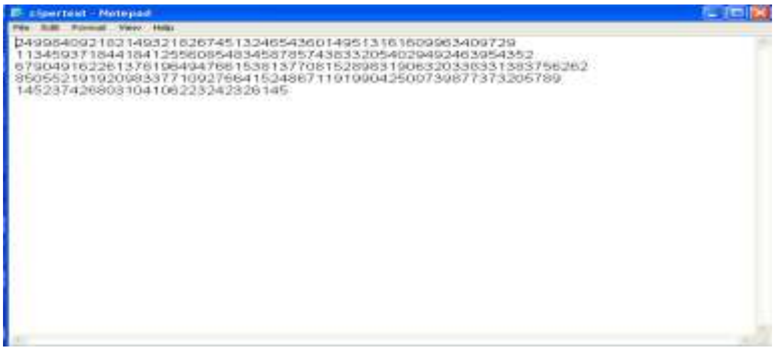
In this paper, we first reviewed data transmission issues and the security issues in CWSNs.We then presented two secure and efficient data transmission protocols for CWSNs, SET-IBS, and SET-IBOOS. We also provided feasibility of the proposed SET-IBS and SET-IBOOS with respect to the security requirements and analysis against routing attacks. SET-IBS and SETIBOOS are efficient in communication and applying the IDbased cryptosystem, which achieves security requirements in CWSNs. Lastly, we implemented ECC algorithm which is highly secure and it makes the hacking task complicated. With respect to both computation and communication costs, SET-IBOOS has less security overhead and is preferred for secure data transmission in CWSNs.An example snapshot is shown below.

Plain text for before applying ECC algorithm:



```
Occured Date & Time is:  Thu Apr 16 12:34:48 IST 2015
BombOccured Place is   Mysure
No of People Injured 100
```

Cipher text after applying the ECC algorithm



```
2499840921821493216267451324654360149513161609963409729
113459371844184125560854834587857438332054029492463954352
679049162261376196494766153813770815289831906320338331383756262
860552191920983377109276641524867119199042500739877373205789
145237426808104108223242326145
```

REFERENCES

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

[2] Y. Wang, G. Attebury, and B. Ramamurthy, "A Survey of Security Issues 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 Algorithms for Wireless Sensor Networks," Computer Comm., vol. 30, nos. 14/ 15, pp. 2826-2841, 2007.

[4] 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.

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

[6] Huang Lu, Jie Li and Mohsen Guizani,"Secure and Efficient Data transmission for Cluster Based Wireless Sensor Networks", IEEE Trans. Parallel & Distributed Systems, vol. 25, no. 3, March.2014.