

An Efficient Signature - Based Scheme for Energy consumption in Wireless Sensor Networks

B.Shanti¹, Molli Srinivasa Rao²

M.Tech Student, Dept of C.S.E, Viswanadha Institute of Technology and Management, Visakhapatnam, India¹

Professor, Dept of C.S.E, Viswanadha Institute of Technology and Management Visakhapatnam, India²

Abstract: Information collection strategies are extremely becoming challenging factor in the field of remote sensor systems for secure data sharing. In managing the settings of the remote sensor systems have been extensively vital issue, for example, target following and condition remote observing. Be that as it may, information can be effectively traded off by a huge of challenges, for example, information interference and information altering and so on, and this produced information will be dropped by bunch head which will be appeared in the recreations by utilizing NS2 programming. We basically concentrate on information respectability security; give a personality based total mark conspire with an assigned verifier for remote sensor systems. As per the benefit of total marks, our plan can keep information uprightness, as well as can decrease data transfer capacity and capacity taken a toll for remote sensor systems.

Keywords: Wireless Sensor Network, Id-based Cryptography, Aggregate Signature, Coalition Attack, Encryption, Decryption, Data Privacy.

I. INTRODUCTION

A Wireless Sensor Network (WSN) is a network system which consist of spatially distributed devices like wireless sensor nodes. Such devices are also capable to communicate in wireless sensor networks and that can also sense, monitor, transmit, receive or process numerous data like pressure, temperature, sound, motion, humidity etc. The individual node are able to sense their environment, processing the data locally and sending data collectively to one or more collection points in a WSN (BS). The following section discussed about various sensor deployment environments and previously deployed schemes in the proposed domain. The data transmission in WSNs can be done in two ways: (i) centralized (ii) decentralized. Centralized means such data processing and transfer can be carried out through or via the medium of a base station in WSNs [3]. Whereas, in case of distributed or clustered wireless sensor environments, every cluster has obtained a high-configuration node called a Cluster-Head (CH). A sensor node of one cluster can only communicate with the other cluster's sensor node by taking the permission of the respective cluster. It is the function of cluster-head to aggregate all the data sent by sensor nodes present in its vicinity. Eventually, cluster-heads sent all the data to the master storage known as base station (BS). The LEACH (Low-Energy Adaptive Clustering Hierarchy) protocol presented by Heinzelman et al. is a widely known and effective one to reduce and balance the total energy consumption for CWSNs. In a cluster-based WSN (CWSN), it is a better approach to keep a powerful base station which can compute or store large amount of data if required. The reason behind this approach is sensor nodes present in the respective clusters are equipped with limited energy and memory requirements and once they are deployed these nodes also need to process data of their neighboring nodes as well. Researchers have been widely studying CWSNs in the last decade in the literature, however, the implementation of the cluster-based architecture in the real world is rather complicated [10]. After rigorous analysis of previously proposed protocols like LEACH, Sec-LEACH [2], RLEACH [8], GS-LEACH, we have reached to the conclusion that all these schemes can easily address routing issues present in the WSNs but they have limited scope to provide security against high-level security attacks is still an opportunity to carry-out a detailed research and implement a cost effective efficient solution. From these results, we have also found that most of the security attacks can be protected or avoided by time-stamp based authentication schemes [11]. In this paper, we have also addressed an issue of orphan node problem by using asymmetric key mechanism rather than symmetric key mechanism for CWSNs. Mainly security of CWSNs can be divided into three categories: [i] base station security [ii] cluster-based security [iii] sensor node security. To address all these security issues, we have divided the proposed security protocol SETDTA into two processes: a) authentication process b) session establishment process.

Researchers invented Cluster-based data transmission in WSN (CWSN) to achieve network scalability and management. This maximizes lifespan of nodes and reduces consumption of bandwidth among sensor nodes. CWSN

contain cluster of sensor nodes from which one of them is selected as Cluster Head (CH). Data collected by leaf node (non-CH sensor nodes) is aggregated at CH and send it to the base station (BS).

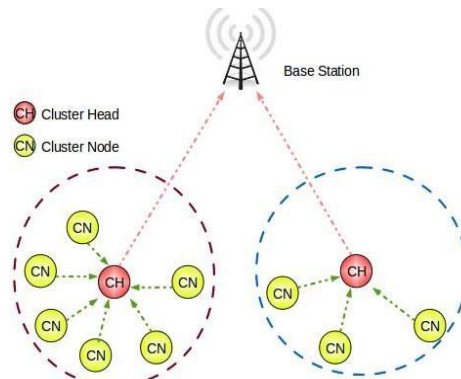


Fig 1. Clustered WSN

II. RELATED WORK

Identity-based (ID-based) cryptography

Shamir presented the personality based (ID-based) cryptography, which facilitates the key administration issue by wiping out open key testaments. In an ID-based cryptography, the client's open key is effectively produced from this present client's any one of a kind personality data, which is thought to be freely known. A trusted outsider, called the private key generator (PKG), produces and issues furtively the comparing private keys[6]for all clients utilizing an ace mystery key. Along these lines, in an ID-based mark (IBS) framework, check calculation just includes the mark match, some open parameters and the character data of underwriter, without utilizing an extra testament.

Aggregate signature scheme

Boneh et al. presented a total mark conspire, which can pack various marks created by various clients on various messages into a solitary short total mark. The total mark's legitimacy can be proportionate to the legitimacy of each mark which is utilized to create the total mark. That is to state, the total mark is legitimacy if and just if every individual endorser truly marked its unique message, separately. Consequently, total is helpful method in diminishing stockpiling expense and transfer speed, and can be an unequivocal building hinder in a few settings, for example, information collection for WSNs, securing outskirts passage conventions and vast scale electronic voting framework, and so on.

Paik, T. Tanaka, H. Ohashi and W. Chen, Big Data et al. presented a mindfulness processing goes for our last objective in software engineering to reproduce human's mindfulness and discernment. Consciousness of interpersonal organization learning in regular day to day existence is effectively empowered by enormous information society. In this paper, we examine foundation for enormous information investigation for interpersonal organization benefits, and propose TF-IDF estimation on huge information framework to know about social relations on social networks[1].Z. Fu, X. Sun, Q. Liu, L. Zhou, J. Shu, et al. introduced cloud computing is becoming increasingly popular. A large number of data are outsourced to the cloud by data owners motivated to access the large-scale computing resources and economic savings [2].

III. METHODOLOGY

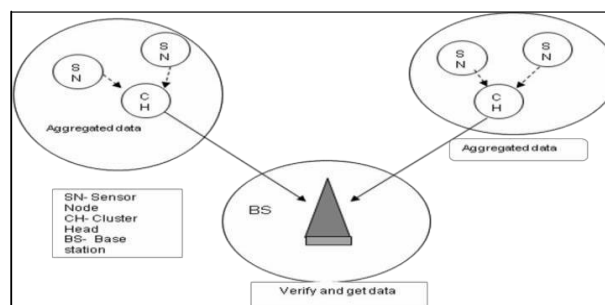


Fig 2. Clustered WSN

The above figure 1 mention system architecture of the proposed system, in which, sensor node send data to cluster head and cluster head aggregates and send data to base station. In this we use many to one network connection where many sensors which forms the group of clusters connected to the base station. Aggregator fills in as a bunch head, can create the total mark and send it to the server farm with the messages produced by the sensor hubs. At that point, through an amusement played with a challenger and an enemy, the security model of character based total mark plans is presented. What's more, in the security demonstrate, the collection calculation ought to oppose a wide range of coalition assaults.

IV. DEFINITIONS AND SECURITY MODULES

- a) **Data center** Server farm has a solid processing force and storage room. So it can handle all unique enormous information gathered by sensor hubs have a place with the server farm, and can give the information data to purchasers. Toward the starting, each server farm will get its open mystery key match (PKcenter, SKcenter), and distribute people in general key PKcenter.
- b) **Data forwarding** Sensor node has limited resources in terms of computation, memory and battery power. Data will be forwarded from sensor node to data aggregator in regular intervals. It is expected that the PKG produces private key SID_i for every sensor hub ID_i . At the point when sensor hub ID_i is conveyed, it is implanted with (param, SID_i). Each with a security parameter Additionally, B randomly generates the public-secret key pair (PKcenter, SKcenter) of data center (designated verifier), then B gives param and PKcenter to A.
- c) **Aggregator** Aggregator is an uncommon sensor hub with a specific capacity to computation and correspondence extend. It can sign messages gathering from the physical world, can get the server farm's open key PKcenter from open channel, can create the total mark from the individual marks marked by sensor hubs included aggregator itself, and can send the total mark to the server farm. We expect that the PKG produces the framework parameters param, aggregator's private key SID relating to its identifier data ID, then inserts (param, SID) in aggregator when it is conveyed.

MATHEMATICAL MODEL

1. Sensor Network.

Sensor network consisting of N sensor, we denote that the i-th sensor by S_i and the corresponding node set by $v = \{v_1, v_2, v_N\}$, $|v| = N$, Set of communication links

$E = \{e_1, e_2, \dots, e_N\}$,

Suppose that V is always connected.

2. Neighbor.

For any node whose neighbor node set are defined as follows: $V_i = \{i \in N \mid d(V_i, V_j) \leq R, n \neq i\}$,

Where, \in

N - The collection of all nodes $d(V_i, V_j)$ - the distance between node V_i , and V_j , R - Broadcasting range of nodes.

3. The energy spent for transmission of a k-bit packet over distance d is: $E_{Tx}(k, d) = k * E_{elec} + k * \epsilon_{fs} * d$ $d < d_0$ (1)

$= k * E_{elec} + k * \epsilon_{mp} * d$ $d \geq d_0$ (2)

Where,

E_{elec} - base energy required to run the transmitter or receiver circuitry ϵ_{fs} & ϵ_{mp} - Energy of the transmitter amplifier

To receive the message energy required is $E_{RX}(k) = k * E_{elec}$ (3)

4. **Elliptical curve digital signature scheme** There are curve parameters (CURVE, G, n) CURVE - The elliptical curve

G - Elliptical curve base point, a generator of the elliptical curve with large prime order n. n - Integer order of G

5 Sensor node creates a key pair,

Private key integer d_A , randomly selected in the interval $[1, n-1]$ public key curve point $Q_A = d_A * G$.

4.1 Signature signing algorithm

1. Calculate $e = \text{HASH}(m)$
2. Let z be the L_n leftmost bits of e, where L_n is the bit length of the group order n.
3. Select a cryptographically secure random integer k from $[1, n-1]$.

4. Calculate the curve point $(x_1, y_1) = k \cdot G$. (4)
5. Calculate $r = x_1 \text{ mod } n$.
5. (5) If $r = 0$, go back to step 3.
6. Calculate $s = k^{-1}(z + r \cdot dA) \text{ mod } n$. (6)
- If $s = 0$, go back to step 3.
7. The signature is the pair (r, s) .

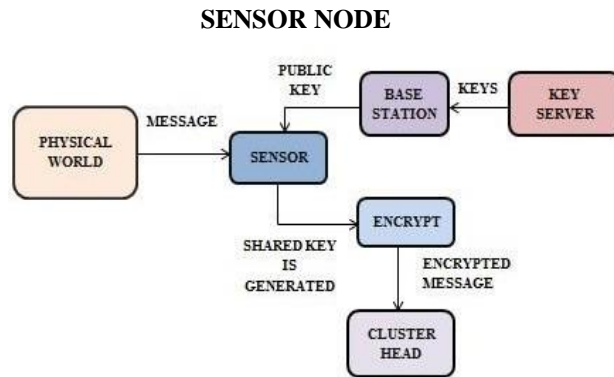


Fig 3: Block diagram for Sensor Node

- Sensor node has limited resources in terms of computation, memory and battery power. We assume that the PKG generates private key S for each sensor node ID.
- When sensor node is deployed, it is embedded with param, SID. Every sensor node ID can use its private key SID to sign messages collecting from the physical world.
- In our system, each sensor node belongs to one cluster, sends encrypted messages to their aggregator, and the messages will finally be sent to data center via aggregator.

6 Signature verification algorithm

1. Verify that r and s are integers in $[1, n-1]$. If not, the signature is invalid.
2. Calculate $e = \text{HASH}(m)$,
3. Let z be the L_n leftmost bits of e . (7)
4. Calculate $w = s^{-1} \text{ mod } n$. (8)
5. Calculate $u_1 = z \cdot w \text{ mod } n$ and $u_2 = r \cdot w \text{ mod } n$. (9)
6. Calculate the curve point

$$(x_1, y_1) = u_1 \times G + u_2 \times QA \quad (10)$$

signature is valid if $r = x_1 \text{ mod } n$, invalid otherwise.

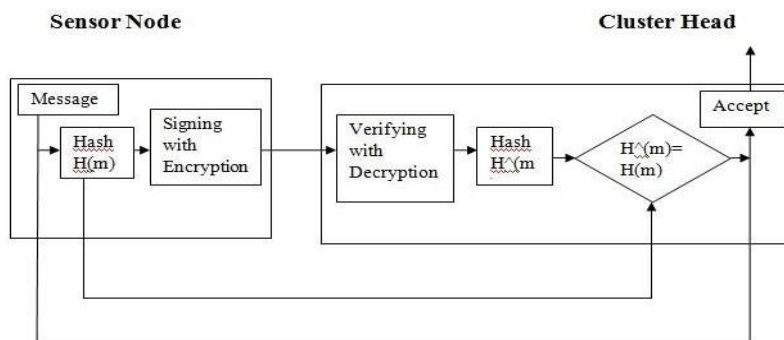


Fig 4: -Signature verification process

V. PROPOSED METHOD

Identity based Signature for WSN is used to achieve following objective-

- Reduce energy consumption than LEACH protocol.
- Provide security to clustered WSN by avoiding denial-of-service attack.

In the proposed system clustering and digital signature is implemented for balancing the load on cluster head in clustered WSN. We are considering to providing security to Multi-weight Based Clustering Algorithm (MWBCA). In MWBCA cluster head is elected by considering many factors like, Digital Signature employs a type of asymmetric cryptography. For message sent through a non-secure channel properly implemented digital signature gives the receiver reason to believe the message was sent by claimed sender. Following are the steps in the design phase for secure transmission of data between cluster node and CH.

1. Base station broadcast its information with its Master key.
2. Sensor node decides to become a CH for current round based on max of P Vi-ch value

$$P Vi-ch = \alpha * deg(vi) + \beta *(Evi_current / Evi_max) + \gamma (1/ T (V)) \quad (11)$$

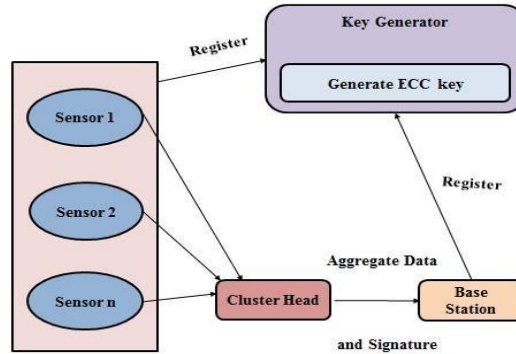


Fig 5: System architecture

Where,

deg (vi) = number of neighbor node of vi Evi_current =current energy of node vi

Evi_max = initial energy of node vi T (V) = elected time of CHvi α, β and γ = weighting factor

1. CH broadcast advertisement message (adv) to the neighboring nodes
2. Cluster node picks CH with largest received signal strength of adv message and joins to CH

Leaf sensor node transmits data to the CH with digital signature. After verification data will get transmitted to CH. During verification we check security of data. Each CH collects message from all members and and aggregate data. CH sends aggregated data to the BS.

Proposed system contains two modules –

1. Clustering Algorithm
2. Digital signature Scheme

1. Clustering Algorithm

We will model the wireless sensor networks. It is assumed that the nature of network is as follow:

- (1) All of nodes are homogeneous .Each node has certain amount of initial energy E. Each node is assigned a unique identifier (ID).
- (2) It consists of a BS, away from the nodes deployed in a square filed, through which the end user can access data from the sensor network

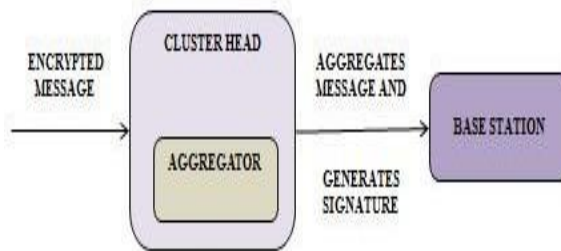


Fig 6: Block diagram for Cluster Head

CLUSTER HEAD (AGGREGATOR)

- Aggregator is a special sensor node with certain ability to calculation and communication range.
- It can sign messages collecting from the physical world, can get the data center's public key (PK) from public channel, can generate the aggregate signature and can send the aggregate signature to the data center.
- We assume that the PKG generates the system parameters param, aggregator's private key SID center corresponding to its identifier information ID, then embeds (param, SID) in aggregator when it is deployed.

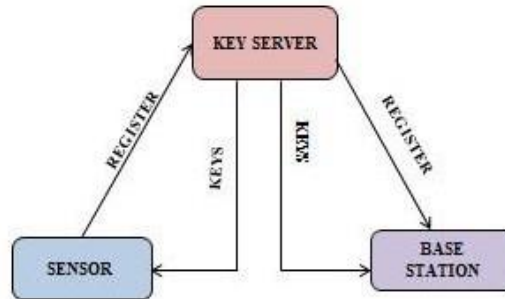


Fig 7: Block diagram for Key generation

- Private key generator is a key server which generates unique public and private keys for base station and sensor nodes.
- Private key generator uses Elliptic Curve Cryptography algorithm to generate keys.
- It also shares public keys of sensor and base station.

IDENTITY-BASED AGGREGATE SIGNATURE SCHEME

In this area, we give a protected personality based total signature conspire. We embrace Sakai et al's. mark conspire as the premise to build our IBAS plot. The plan is depicted as takes after.

Setup phase

Step 1: The challenger B runs the Setup algorithm to obtain a master secret key msk and the system parameters param with a security parameter.

Step 2: B randomly generates the public-secret key pair (PKcenter, SKcenter) of datacenter (designated verifier), then B gives param and PKcenter to A.

Query phase

Step 3: Key Generation query OS(ID): On receiving such a query, challenger B responds by running Key Generation algorithm to obtain the private key SID of the user ID, returns SID to A.

Step 4: Signing query Osig(ID,m): On receiving such a query, challenger B responds by running Signing algorithm to obtain a signature σ and returns σ to A. (B firstly runs the Key Generation algorithm if necessary).

Step 5: AggVerification query OAggV ($\{m_i, ID_i, i = 1, \dots, n\}, \sigma$): On receiving such a query, challenger B responds whether the aggregate signature is valid for the submitting tuples by running AggVerification algorithm.

Step 6: Finally, A outputs its forgery ($\{m_j, ID_j, \sigma_j, j = 1, \dots, n\}, \sigma$). A is success if The aggregate signature σ is valid on tuple $\{m_j, ID_j, \sigma_j, j = 1, \dots, n\}$. Any user can run this verification algorithm.

Step 7: At least one individual signature $\sigma_j (j = 1, \dots, n)$ is invalid. A wins if and only if it can forge a valid aggregate signature using a set of individual signatures which is involved at least one invalid single signature.

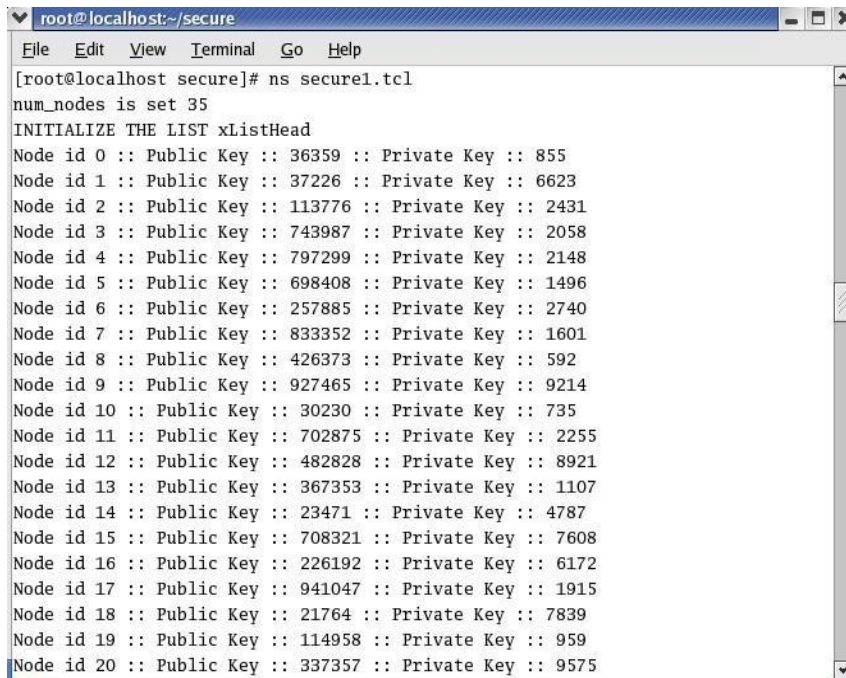
VI EXPERIMENTAL/SETUP AND RESULTS

For wireless sensor networks, simulation is performed using NS2 simulator. The above Table1 shows the typical parameters of simulation setup.

PARAMETERS

Table 1: Simulation Parameters

Simulator	NS-2.34
No of Nodes	35
Network Interface Type	Phy/Wireless Phy
Node Type	Static
MAC Protocols	MAC/802_11
Radio Propagation Model	TwoRayGround
Routing Protocol	AODV
Area of Simulation	1000x1000
Channel Type	Wireless Channel
Time of Simulation End	30.0sec
Link Type	LL
Antenna Model	Omni Antenna



```

root@localhost:~/secure
File Edit View Terminal Go Help
[root@localhost secure]# ns secure1.tcl
num_nodes is set 35
INITIALIZE THE LIST xListHead
Node id 0 :: Public Key :: 36359 :: Private Key :: 855
Node id 1 :: Public Key :: 37226 :: Private Key :: 6623
Node id 2 :: Public Key :: 113776 :: Private Key :: 2431
Node id 3 :: Public Key :: 743987 :: Private Key :: 2058
Node id 4 :: Public Key :: 797299 :: Private Key :: 2148
Node id 5 :: Public Key :: 698408 :: Private Key :: 1496
Node id 6 :: Public Key :: 257885 :: Private Key :: 2740
Node id 7 :: Public Key :: 833352 :: Private Key :: 1601
Node id 8 :: Public Key :: 426373 :: Private Key :: 592
Node id 9 :: Public Key :: 927465 :: Private Key :: 9214
Node id 10 :: Public Key :: 30230 :: Private Key :: 735
Node id 11 :: Public Key :: 702875 :: Private Key :: 2255
Node id 12 :: Public Key :: 482828 :: Private Key :: 8921
Node id 13 :: Public Key :: 367353 :: Private Key :: 1107
Node id 14 :: Public Key :: 23471 :: Private Key :: 4787
Node id 15 :: Public Key :: 708321 :: Private Key :: 7608
Node id 16 :: Public Key :: 226192 :: Private Key :: 6172
Node id 17 :: Public Key :: 941047 :: Private Key :: 1915
Node id 18 :: Public Key :: 21764 :: Private Key :: 7839
Node id 19 :: Public Key :: 114958 :: Private Key :: 959
Node id 20 :: Public Key :: 337357 :: Private Key :: 9575

```

Fig 8: Public and Private Key Generation

In the above fig 8 , for all the nodes its public and private key will be generated based on the set-up and query phase, in order to provide privacy. For example, the public key for node 0 is 36359 and private key is 855. The same procedure will be done for all the 35 nodes in the formed clusters.

```

root@localhost:~/secure
File Edit View Terminal Go Help
Sensor node data from Cluster 2 is: 74
Sensor node data from Cluster 2 is: 26
Sensor node data from Cluster 2 is: 3
Sensor node data from Cluster 2 is: 65
Sensor node data from Cluster 2 is: 94
Sensor node data from Cluster 2 is: 80
Sensor node data from Cluster 2 is: 2
Aggregated Data from Cluster Head2 is :49
A Diffie Helman Key Exchange
-----
Prime Number 13
Random Integer 7
Random Secret Key 8
-----
Cluster Head public key is 3
Sink public key is 11
-----
Cluster Head secret key is 9
Sink secret key is 9
  
```

Fig 9: Aggregates the Data From the Sensor Nodes

In the above fig 9, here all the data from the sensor nodes will be collected and it will be aggregated, in order to send to base station. Here the prime no, random integer, random secret key, cluster head public key, sink public key will be generated. This procedure will be same for all the nodes.

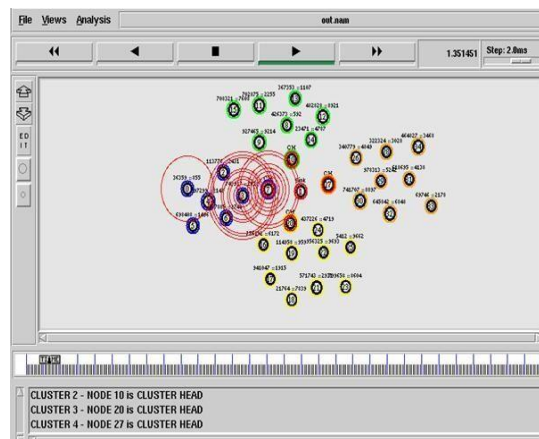


Fig 10 : Transmission of Data

In this above fig 10, we can see the transmission of data in the form of packets between cluster head and base station using simulation. We can see the transmissions going on between cluster head 7 and sensor node 0,4,3,6,2, where data will be aggregated then it will send to sink.

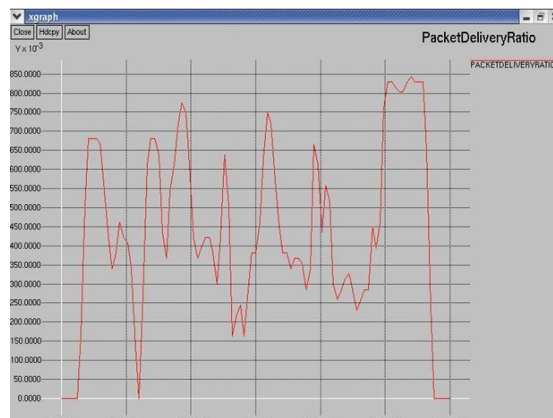


Fig 11: Packet Delivery Ratio of no of Packets v/s Time

The above fig11 shows the number of packets delivered to the base station from the aggregator. Here, the X-axis represents time and Y-axis represents no of packets. From the fig we can make out that where there is a fall in the graph, it represents the packet dropped at that time due to forged data.

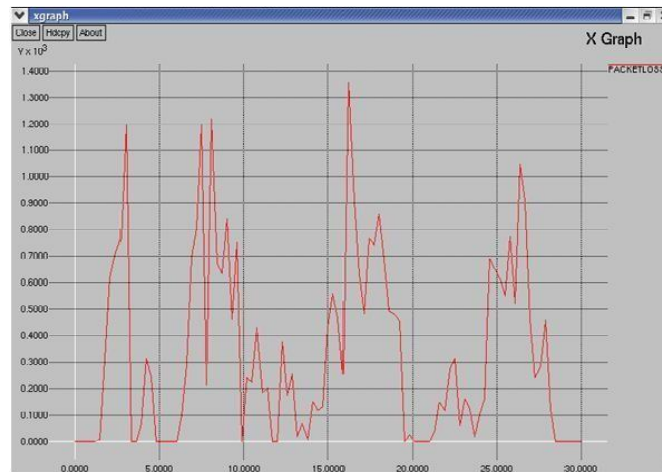


Fig 12: Packet Loss Ratio of no of Packets v/s Time

The above fig 12 shows the number of packet loss while communicating between the aggregator and the base station. Here, the X-axis represents time and Y-axis represents no of packets. From the fig we can make out that where there is a fall in the graph, it represents the packet dropped at that time, and causes the packet loss.



Fig 13: End to End Delay of no of Packets v/s Time

This fig 13 shows the number of packets dropped while transferring from aggregator to the base station. The packet drops occurs due the duplication of data. The X-axis represents the time any Y-axis represents the no of packets. Here from the above figure we can make out that first the delay will be very high after implementing id-based aggregate schema the delay is reduced.

VII. CONCLUSION AND FUTURE SCOPE

Here in this ID-based aggregate signature scheme for WSNs, we will compress many signatures generated by sensor nodes into a short one, i.e., it can reduce the communication and storage cost. Moreover, it is proved that IBAS scheme is secure in random oracle model, and it has also proved that aggregate signature can resist coalition attacks, that is to say the aggregate signature is valid if and only if every single signature used in the aggregation is valid, and the communication of data from sensor nodes to cluster head and from the cluster head to base station is shown in the simulations that uses the NS2 software. During this process the data which has been forged will be dropped from the cluster head and also reduces the end to end delay from one node to other and therefore security can be provided to WSNs.

For better security issues we can implement an asymmetric key approach in key generation in future.

REFERENCES

- [1] 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.
- [2] 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.
- [3] A. Manjeshwar, Q.-A. Zeng, and D.P. Agrawal, "An Analytical Model for Retrieval in Wireless Sensor Networks Using Enhanced APTEEN Protocol," IEEE Trans. Parallel & Distributed Systems, vol. 13, no. 12, pp. 1290-1302, Dec. 2002.
- [4] L.B. Oliveira et al., "SecLEACH-On the Security of Clustered Sensor Networks," Signal Processing, vol. 87, pp. 2882-2895, 2007. [5] 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.
- [6] 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.
- [7] W. Diffie and M. Hellman, "New Directions in Cryptography," IEEE Trans. Information Theory, vol. IT-22, no. 6, pp. 644-654, Nov. 1976.
- [8] A. Shamir, "Identity-Based Cryptosystems and Signature Schemes," Proc. Advances in Cryptology (CRYPTO), pp. 47-53, 1985.
- [9] D.W. Carman, "New Directions in Sensor Network Key Management," Int'l J. Distributed Sensor Networks, vol. 1, pp. 3-15, 2005.
- [10] R. Yasmin, E. Ritter, and G. Wang, "An Authentication Framework for Wireless Sensor Networks Using Identity- Based Signatures," Proc. IEEE Int'l Conf. Computer and Information Technology (CIT), pp. 882-889, 2010.
- [11] H. Lu, J. Li, and H. Kameda, "A Secure Routing Protocol for Cluster-Based Wireless Sensor Networks Using ID- Based Digital Signature," Proc. IEEE GLOBECOM, pp. 1-5, 2010.
- [12] 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
- [13] Zhiping FAN, Zhengzhe JIN, "A Multi-weight Based Clustering Algorithm for Wireless Sensor Networks" PRZEGLĄD ELEKTRO TECHNICZNY (Electrical Review), 2012.

BIOGRAPHIES

B. Shanti, M.Tech., Student, Department: Computer Science & Engineering (CSE) Viswanadha Institute of Technology and Management, Andhra Pradesh, India.



Mollu Srinivasa Rao received his M.Tech., degree in Computer Science & Technology from Andhra University in 2003 and Ph.D. degree in Computer Science & Systems Engineering from Andhra University in 2018. He is currently working as Professor and Head of the Department, Computer Science and Engineering Department, Viswanadha Institute of Technology and Management, Andhra Pradesh, India. His research interests include Mobile Ad hoc Networks, Sensor Networks, and soft computing techniques.