International Journal of Scientific Engineering and Technology ISSN : 2277-1581
Volume No. 6, Issue No. 9, PP : 327-331 1 Sept. 2017

A New approach of Secure Aggregate Signature Scheme for Wireless Sensor Networks

Ananda Kumar K S,Dr.Balakrishna R, Abhilasha.K,Apoorva.R, DivyaBharathi.J
Department of Information Science and Engineering ,RajaRajeswari College of Engineering, Bangalore, India
Corresponding Email : anandgdk@gmail.com

Abstract:Managing secure and effective enormous information collection strategies are extremely alluring in the field of remote sensor systems. In genuine settings, the remote sensor systems have been extensively connected, for example, target following and condition remote observing. Be that as it may, information can be effectively traded off by a huge of assaults, for example, information interference and information altering and so on, and these 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: **Big Data, Coalition Attack, Identity Based Data Aggregation, Unforgeability, Wireless Sensor Network.**

I.INTRODUCTION

In big data era[3], digital universe grows in stunning speed which is produced by emerging new services, such as social networking. Big data are gathered by omnipresent wireless sensor networks, aerial sensory technologies, software logs, information-sensing mobile devices, microphones, cameras, etc. Remote sensor systems (WSNs), with a substantial number of shabby, little and profoundly compelled sensor hubs sense the physical world, has extremely expansive application prospects both in military and regular citizen utilization, including military target following and observation, creature living spaces checking, biomedical wellbeing observing, basic offices following. It can be used in some hazard environments, such as in nuclear power plants. Due to the remarkable advantages, comprehensive attention has been devoted to WSNs, and a number of schemes have been presented. In WSNs, sensor nodes are usually resource-limitedand power-constrained, they always suffer from the restricted storageand processing resources [4].

Therefore, different from traditional networks, WSNs have their inherent resource constraints and design limitations, such as low bandwidth, short communication range, limited amount of energy, and limited processing and storage in every sensor node. Data aggregation[5] technique is considered as a Holy Grail to reduce energy consumption for WSNs. However, the technique still has the inherent security problems, such as eavesdropping, reply attacks, data forge and data tampering, etc.

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 outskirt 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].

International Journal of Scientific Engineering and Technology ISSN : 2277-1581
Volume No. 6, Issue No. 9, PP : 327-331 1 Sept. 2017

III.METHODOLOGY

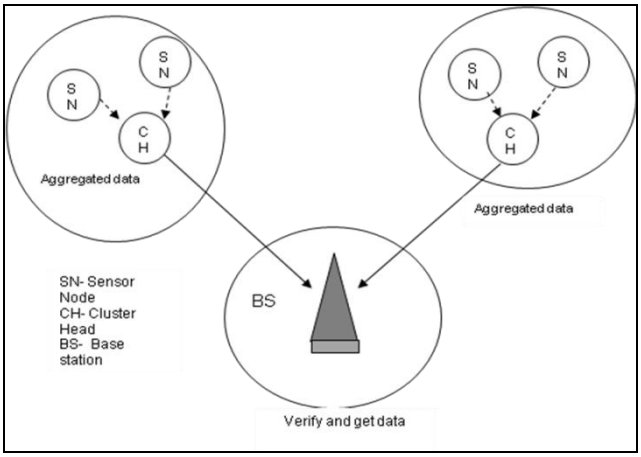

Fig.1. Cluster Based Network.

The above figure1 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

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.

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 SIDi for every sensor hub IDi. At the point when sensor hub IDi is conveyed, it is implanted with (param, SIDi). Each sensor hub IDi can utilize its private key SIDi to sign messages gathering from the physical world. In our framework, every sensor hub has a place with one bunch, sends messages and its marks to their aggregator, and the messages will at last be sent to server farm by means of aggregator.

Data security - The challenger B runs the security algorithm to obtain a master secret key msk and the system parameters param 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.

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.

V.IDENTITY-BASED AGGREGATESIGNATURE SCHEME USING PPT

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 andthe 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: KeyGeneration query OS(ID): On receiving such a query, challenger B responds by running KeyGeneration 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 byrunning Signing algorithm to obtain a signature σ and returns σ to A. (B firstly runs the KeyGeneration algorithm if necessary).

Step 5: AggVerification query OAggV ({mi, IDi, i = 1, . . . ,n}, σ): On receiving such aquery, challenger B responds whether the aggregate signature is valid for the submitting tuples by running AggVerification algorithm.

Step 6: Finally, A outputs its forgery ({mj ,IDj , σj , j = 1, . . . , n}, σ∗). A is success if The aggregate signature σ∗ is valid on tuple {mj ,IDj , σj , j = 1, . . . , n}. Any user can run this verification algorithm.

Step 7: At least one individual signature σj(j = 1, . . . , n) isinvalid. 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.RESULT ANALYSIS

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

SIMULATION PARAMETERS	PARAMETER VALUE

International Journal of Scientific Engineering and Technology
Volume No. 6, Issue No. 9, PP : 327-331
ISSN : 2277-1581
1 Sept. 2017

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

Table 1: Simulation Parameters

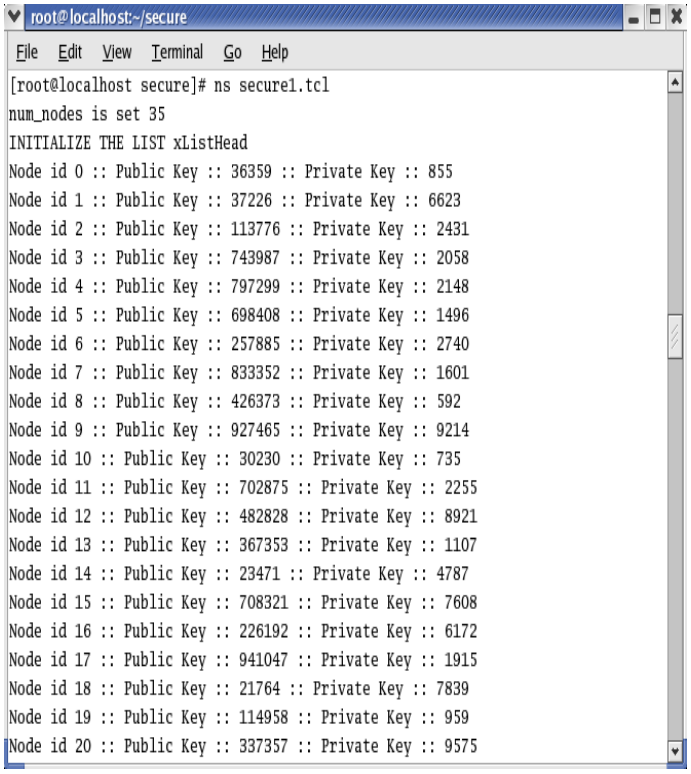

Fig 2: Public and Private Key Generation

In the above figure 2, 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.

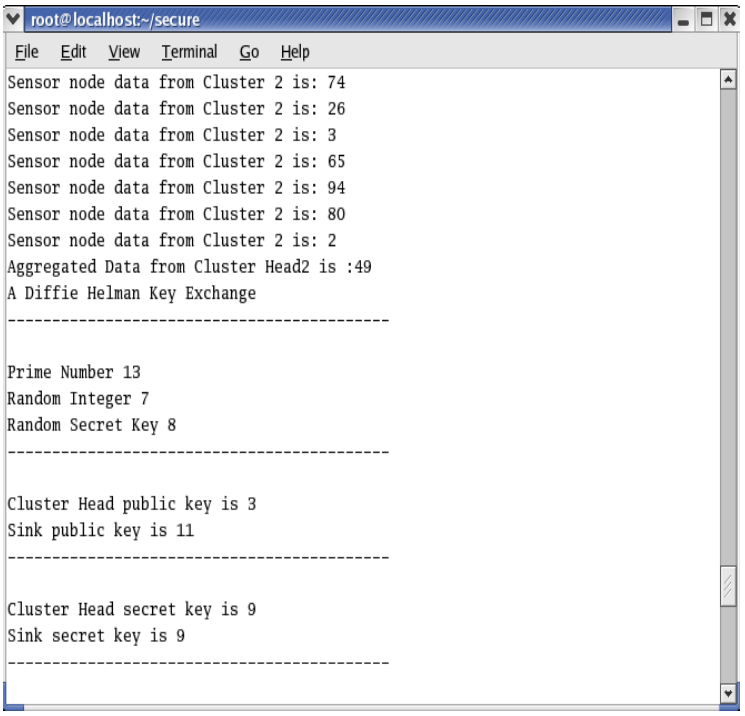

Fig 3: Aggregates the Data From the Sensor Nodes

In the above fig 3, 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.

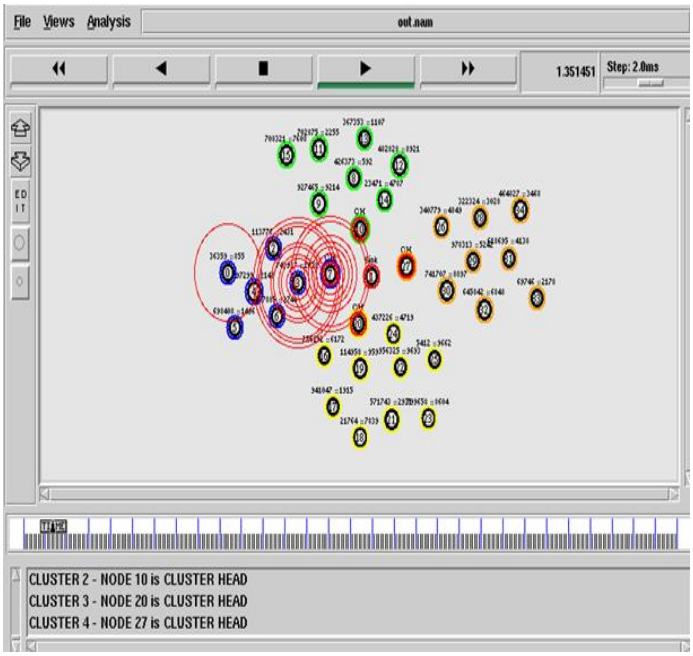

Fig 4: Transmission of Data

In this above figure 4, 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.

International Journal of Scientific Engineering and Technology
Volume No. 6, Issue No. 9, PP : 327-331
ISSN : 2277-1581
1 Sept. 2017

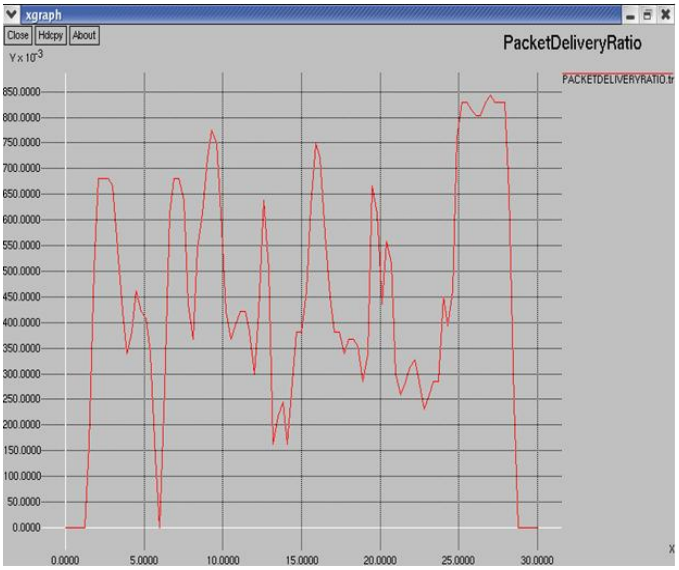

Fig 5: Packet Delivery Ratio of no of Packets v/s Time

The above fig 5 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.

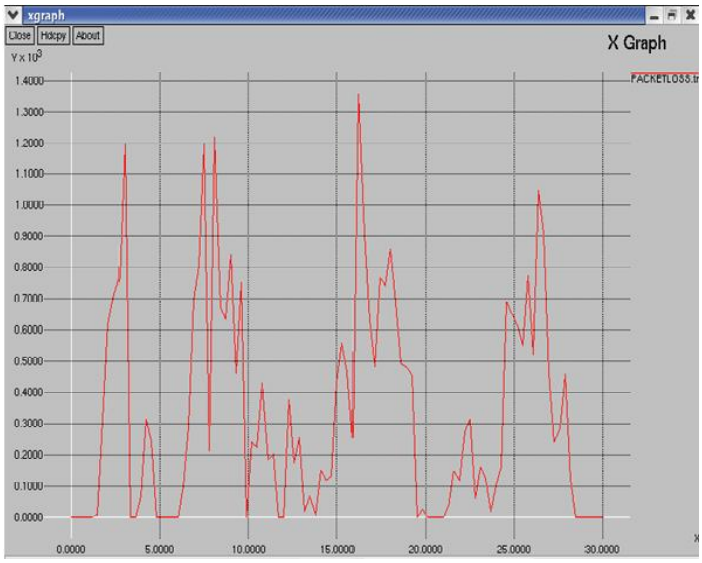

Fig 6: Packet Loss Ratio of no of Packets v/s Time

The above fig 6 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.

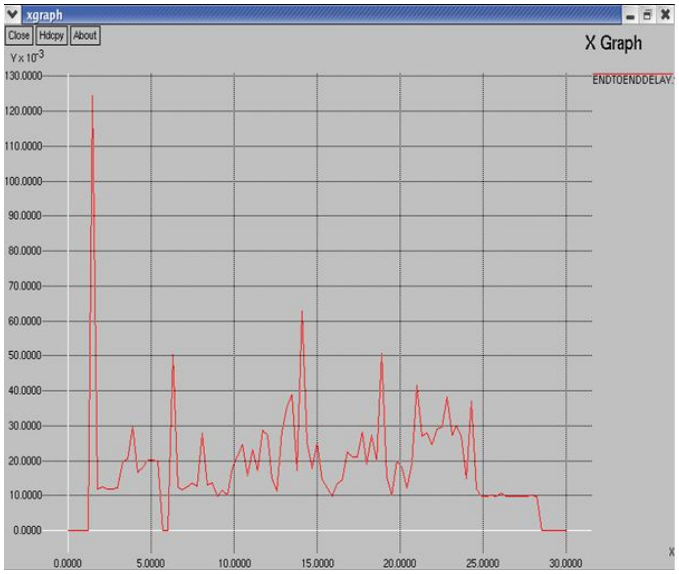

Fig 7: End to End Delay of no of Packets v/s Time

This fig 7 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

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.

ACKNOWLEDGEMENTS

The authors would like to express sincere thanks for encouragement and constant support provided by the Management RRGI, Principal, HOD Dept of ISE, RajaRajeswari College of Engineering, Bangalore-74, India during this research work.

REFERENCES

i. *I. Paik, T. Tanaka, H. Ohashi and W. Chen, "Big Data Infrastructure for Active Situation Awareness on Social Network Services,"BigData(BigDataCongress),IEEE International Congress on. IEEE, pp.411-412, 2013*

ii. *Z. Fu, X. Sun, Q. Liu, L. Zhou, J. Shu, "Achieving Efficient Cloud Search Services: Multi-keyword Ranked Search over Encrypted Cloud Data Supporting Parallel Computing," IEICE Transactions on Communications, vol. E98-B, no. 1, pp.190-200, 2015.*

iii. *I. Hashem, I. Yaqoob, N. Anuar, et al., "The rise of "big data" on cloud computing: Review and open research issues," Information Systems, vol.47, no. 47, pp. 98-115, 2015.*

iv. *H. Li, Y. Yang, T. Luan, X. Liang, L. Zhou and X. Shen, Enabling Finegrained Multi-keyword Search Supporting Classified Sub-dictionaries over Encrypted Cloud Data,"IEEE Transactions on Dependable and SecureComputing, DOI10.1109/TDSC.2015.2406704, 2015.*

v. *H. Li, D. Liu, Y. Dai and T. Luan, "Engineering Encryption of Mobile Cloud Networks: When QoE Meets QoP," IEEE WirelessCommunications, vol. 22, no. 4, pp. 74-80, 2015.*

vi. *X. Liu, B. Qin, R. Deng, Y. Li, "An Efficient Privacy-Preserving Outsourced Computation over Public Data," IEEE Transactions on ServicesComputing, 2015, doi: 10.1109/TSC.2015.2511008.*

vii. *Ananda Kumar K S; Balakrishna R; "Development of Energy- Efficient and Data Collection Protocol For heterogeneous Wireless Sensor Networks" ITSI Transactions on Electrical and Electronics Engineering (ITSI-TEEE), ISSN (PRINT): 2320 – 8945, Volume -4, Issue -2, 2016*

viii. *X. Liu, R. Choo, R. Deng, R. Lu, "Efficient and privacy-preserving outsourced calculation of rational numbers,"IEEE Transactions on Dependable and Secure Computing, 2016, doi: 10.1109/TDSC.2016.2536601.*

ix. *Ananda Kumar K S, BalakrishnaR "Comparative Analysis of Delay and Throughput using IEEE 802.11 and Receiver Centric-MAC Protocol in Wireless Sensor Networks", IEEE International Conference on Innovations in Power and Advanced Computing Technologies [i-PACT2017], April 21-22,2017 VIT, Vellore.*