International Journal of Science Engineering and Advance Technology, IJSEAT, Vol. 6, Issue 3 | ISSN 2321-6905 March- 2018

International Journal of Science Engineering and Advance Technology

Enhanced Aggregate Signature Scheme For Secure Data Verification In Wireless Sensor Network

[1] Rentala Mounika [2]Nadella Sunil
[1]Final Master of Science in Computer Science, Ideal College Of Arts and Science, Vidyuth Nagar, Kakinada, East Godavari Dist, AP, India.
[2]Associate Professor, Department of Computer Science, Ideal College Of Arts and Science, Vidyuth Nagar, Kakinada, East Godavari Dist, AP, India.

ABSTRACT:
In tangible, the wireless sensor networks have been approximately practical, such as target tracking and environment remote monitoring. But, data can be simplybargained by a huge of doses, such as data capture and data meddling, etc. In this paper, we chieflyeffort on data integrity protection, give an identity-based aggregate signature outline with a voted verifier for wireless sensor networks. Bestowing to the improvement of aggregate signatures, our outline not only can preserve data integrity, but also can condense bandwidth and storage cost for wireless sensor networks. Moreover, the security of our identity-based aggregate signature organization is carefully open based on the computational Diffie-Hellman conjecture in unsystematic vision typical.

KEYWORDS: Aggregator, Data center, Sensor node.

1INTRODUCTION:

Big data are collected by ubiquitous wireless sensor networks, aerial sensory technologies, software logs, information-sensing mobile devices, microphones, cameras and so on. And the wireless sensor network is one of the extremely expected key contributors of the big data in the upcoming networks. Wireless sensor networks (WSNs), with a large amount of inexpensive, minor and extremely forced sensor nodes intelligence the bodily ecosphere, has very wide-ranging application predictions together in military and civilian usage, with military target tracking and scrutiny, animal habitats specialist care, biomedical health monitoring, grave facilities tracking. It can be hand-me-down in certain threat environments, such as in nuclear power plants. Due to the remarkable advantages, inclusive attention has been enthusiastic to WSNs, and a number of structures have been existing. In WSNs, sensor nodes are frequently resource-limited and power-constrained; they always agonize from the constrained packing and giving out possessions.

2LITERATURE SURVEY:

Wisden joins two originaldevices, dependable data transport by a hybrid of end-to-end and hop-by-hop recovery, and low-overhead data time-stamping that does not need /worldwide clock harmonization. We also revision the applicability of wavelet-based density techniques to overwhelmed the bandwidth limitations imposed by low power wireless radios. We label our application of these devices on the Mica-2 motes and assess the presentation of our application. We also bang experiences from organizing Wisden on a big construction.

The aggregate signature is figured by having each signer, in go, add his signature to it. We demonstration to grasp this in such a way that the scope of the aggregate signature is self-governing of n. This makes consecutive aggregate signatures a usual embryonic for certificate chains, whose length can be summary by aggregating all signatures in a chain. We give aedifice in the accidental oracle model founded on relations of expert trapdoor variations, and show how to instantiate our scheme based on RSA.

3PROBLEM DEFINTION:

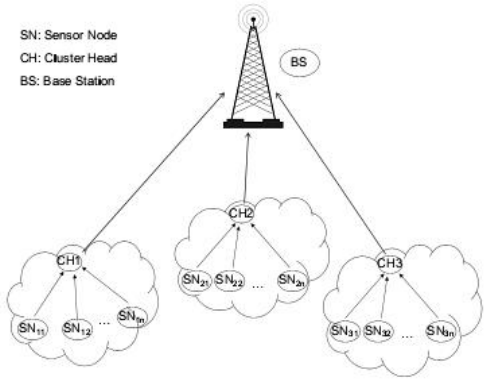
An aggregate signature system can poultice manifold signatures produced by diverse users on different messages into a sole short aggregate signature. The aggregate signature's legitimacy can be correspondent to the soundness of every signature which is used to create the aggregate signature. That is to say, the aggregate signature is soundness if and only if each individual signer indeed signed its inventive message, separately. From now, aggregation is useful procedure in tumbling storage

cost and bandwidth, and can be a significant building block in some settings, such as data aggregation for WSNs, securing border gateway protocols and large scale electronic voting system, etc.

4PROPOSED APPROACH:

We Suggest an ID-based aggregate signature (IBAS) arrangement for WSNs in cluster-based method. Aggregator works as a cluster head, can harvest the aggregate signature and send it to the data center with the messages created by the sensor nodes.. And in the security model, the aggregation algorithm should attack all kinds of coalition attacks. Second, we give a locked identity-based aggregate sig-nature scheme for wireless sensor networks with a nominated verifier (data center). Third, the exhaustive have nimpervious is given based on the computational Diffie-Hellman theory in random oracle model. Fourth, concluded the inquiry of reasonable show, we exhibit that our identity-based aggregate signature pattern is proficient in terms of the announcement and packing overhead.

5SYSTEM ARCHITECTURE:



6PROPOSED METHODOLOGY:

Data center
Data center has a stout computing power and storage space. So it canprogress all inventive big data placid by sensor nodes belong to the data center, and can afford the data information to consumers. At the be-ginning, every data center as the nominated verifier in our IBAS scheme will collect its public-secret key pair (PKcenter, SKcenter), and put out the public key PKcenter.

Aggregator
Aggregator is a singular sensor node with convincedskill to calculation and communication range. It can sign messages assembling from the physical world, canget the data center's public key PKcenter from public channel, can create the aggregate signature from the individual signatures hired by sensor nodes contained within aggregator itself, and can show the aggregate signature to the data center. We adopt that the PKG engenders the system parameters param, aggregator's private key SID equivalent to its identifier information ID, then embeds (param, SID) in aggregator when it is arrayed.

Sensor node
Sensor node has inadequate resources in terms of computation, memory and battery power. We adopt that the PKG generates private key SIDi for each sensor node IDI. When sensor node ID I is arrayed, it is implanted with (param, SIDi). Every sensor node ID i can use its private key SIDi to badge messages accumulating from the physical world. In our coordination, each sensor node have its place to one cluster, sends messages and its signatures to their aggregator, and the messages will lastly be sent to data center via aggregator.

Performance evaluation
All sensor nodes are aimlesslysprinkled with anunbroken distribution. Erratically select one of the installed nodes as the source node. The location of the sink is casuallyunwavering. We estimate our proposed method with veneration to the following metrics: PDR, E2E latency, PLR and Energy ingesting.

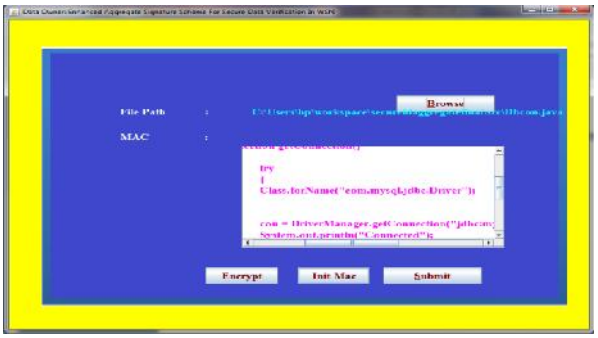
7ENHANCED IDENTITY BASED AGGREGATE SIGNATURE SCHEME
Step1: Setup Phase:
a) Initiation of a master secret key *msk*and the system parameters *param*with a security parameter *l.*
b) Generates the public-secret key pair (*PKcenter, SKcenter*) of data center using ECC-160bit Algorithm.
Step2: KeyGeneration Phase:
a) Computing sensor nodes corresponding private key using sensor id and hash value.
Step3: Signature Generation:
a) It is done by using message m, sensor node id and corresponding private key S.
Step4: Signature Verification:
a) Verification is done and accepts matching the current generated signature and earlier signature
Step5: Aggregation Phase:

a) In this phase an aggregate subset of sensor nodes belong to one cluster, each sensor node with the identity *IdI* provides a signature on a message Gained the data center's public key *PKcenter*from public channel.

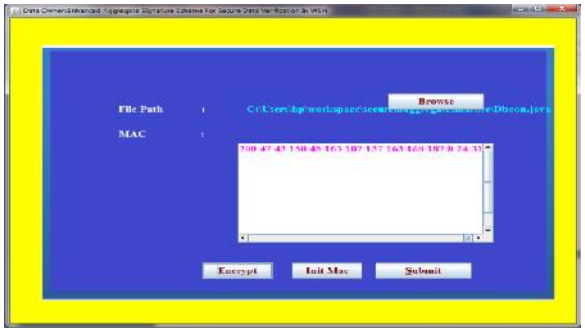
Step6: Aggregate Verification:

a) Verification of an aggregate signature on the original messages generated by the sensor nodes belong one cluster with the identity *IDI*, The data center with public-secret key pair.

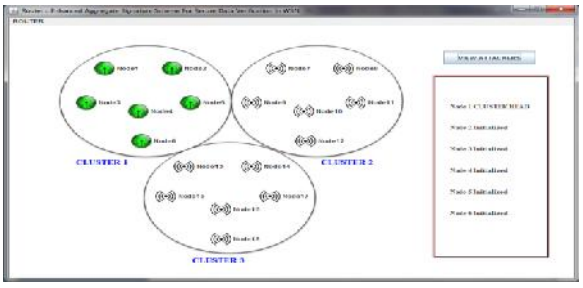
8RESULTS:



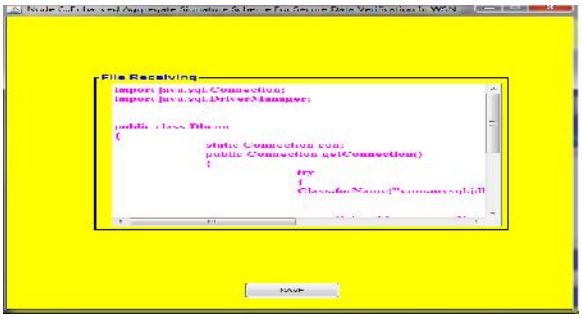
Select a Text Document.



Message is Encrypted.

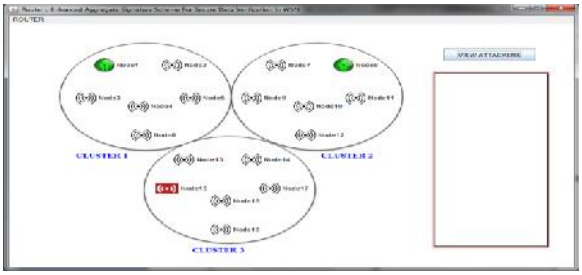


Clusters are Initiated.

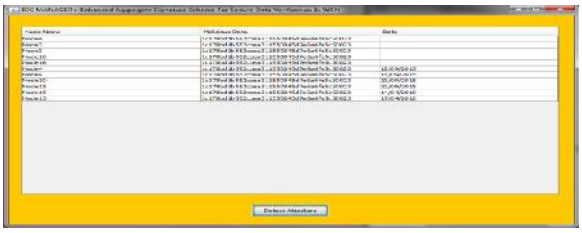


Data Sent Successfully to Node C.

ATTACKS:



Node 15 is attacked.



It Displays the attacks in IDS Manager.

EXTENSION WORK:

Proposing ECC 160 bit algorithm for identity based signature scheme which diminishes communication and calculation overhead.

9CONCLUSION:

We extant an ID-based aggregate signature scheme for WSNs, which can wrap many crosses produced by sensor nodes into a short one, i.e., it can decrease the communication and storage cost. Furthermore, we have demonstrated that our IBAS scheme is protected in accidental oracle model based on the CDH assumption, and we also have shown that our aggregate signature can struggle coalition attacks, that is to say the combined signature is legal if and only if every single signature used in the aggregation is valid.

10REFERENCES:

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

[2]E. Hargittai, "Is Bigger Always Better? Potential Biases of Big Data Derived from Social Network Sites," Annals of the American Academy of Political & Social Science, vol. 659, no. 1, pp. 63-76, 2015.

[3]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.

[4] 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.

[5] H. Li, Y. Yang, T. Luan, X. Liang, L. Zhou and X. Shen, "Enabling Fine grained Multi-keyword Search Supporting Classified Sub-dictionaries over Encrypted Cloud Data," IEEE Transactions on Dependable and Secure Computing, DOI10.1109/TDSC.2015.2406704, 2015.

[6] H. Li, D. Liu, Y. Dai and T. Luan, "Engineering Searchable Encryption of Mobile Cloud Networks: When QoE Meets QoP," IEEE Wireless Communications, vol. 22, no. 4, pp. 74-80, 2015.

[7] X. Liu, B. Qin, R. Deng, Y. Li, "An Efficient Privacy-Preserving Out-sourced Computation over Public Data," IEEE Transactions on Services Computing, 2015, doi: 10.1109/TSC.2015.2511008

[8] X. Liu, R. Choo, R. Deng, R. Lu, "Efficient and privacy-preserving out-sourced calculation of rational numbers," IEEE Transactions on Depend-able and Secure Computing, 2016, doi: 10.1109/TDSC.2016.2536601.

[9]H. Li, X. Lin, H. Yang, X. Liang, R. Lu, and X. Shen, "EPPDR: An Efficient Privacy-Preserving Demand Response Scheme with Adaptive Key Evolution in Smart Grid," IEEE Transactions on Parallel and Distributed Systems, vol. 25, no.8, pp. 2053-2064, 2014.

[10] H. Li, R. Lu, L. Zhou, B. Yang, X. Shen, "An Efficient Merkle Tree Based Authentication Scheme for Smart Grid," IEEE SYSTEMS Journal, vol. 8, no.2, pp. 655-663, 2014.

[11] C. Chen, C. Zhang, "Data-intensive applications, challenges, techniques and technologies: A survey on Big Data," Information Sciences, vol. 275, no. 11, pp. 314-347, 2014.

[12] D. Takaishi, H. Nishiyama, N. Kato and R. Miura, "Toward Energy Efficient Big Data Gathering in Densely Distributed Sensor Networks," Emerging Topics in Computing IEEE Transactions on, vol. 2, no. 3, pp.388-397, 2014.

[13] M.M.E.A. Mahmoud and X. Shen, "A cloud-based scheme for protecting source-location privacy against hotspot-locating attack in wireless sensor networks," IEEE Trans. Parallel Distrib.Syst., vol. 23, no. 10, pp. 1805-1818, 2012.

[14] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci, "A survey on sensor networks," IEEE Commun.Mag., vol. 40, no. 8, pp. 102-114, 2002.

[15]J. Yick, B. Mukherjee and D. Ghosal, "Analysis of a prediction-based mobility adaptive tracking algorithm," in Proc. Broadband Networks, 2nd International Conference on, IEEE, pp. 753-760, 2005.

[16] Limin Shen, Jianfeng Ma, Member, IEEE, Ximeng Liu, Member, IEEE, Fushan Wei and Meixia Miao, A Secure and Efficient ID-Based Aggregate Signature Scheme for Wireless Sensor Network, 2017.

RentalaMounika is a student of Ideal College of Arts and Science Kakinada. Presently she is in Final Master of Science in Computer Science this college and affiliated to Adikavi Nannaya University, Rajamahendravaram, Andhra Pradesh. Her area of interest includes Computer Networks and Web Designing, all current trends and techniques in Computer Science.

Mr. Nadella Sunil, Presently working as Director and Associate Professor in P.G. Department of Computer Science, Ideal College of arts and Sciences, Kakinada. He obtained M.Sc., (Applied Mathematics) from Andhra University, M. Phil in Applied Mathematics from Andhra University and M.Tech (CSE) from University College of Engineering, JNTUK. Received Professor I. Venkata Rayudu Shastabdi Poorthi Gold Medal, applied Mathematics Prize and T.S.R.K. Murthy Shastabdi Prize from Andhra University. Have Lecturer Ship in both Mathematical Sciences, Computer Sciences and Applications disciplines. Presently Pursuing Ph.D in Computer Science from JNTU Kakinada.