International Journal of Science Engineering and Advance Technology

A secure data transmission using efficient aggregate signature scheme to verify data in wireless sensor N/W

Ganti Dinesh Kumar[1], G K Havilah [2], M. Veerabhadra Rao [3]
[1]Final M.Tech Student,[2]Asst.Professor, [3]Head of the Department
[1, 2, 3]Dept of Computer Science and Engineering
[1, 2, 3]Prasiddha College of Engineering and Technology, Ananthavaram-Amalapuram-533222, E.g.dt, A.P.

ABSTRACT:
We stretch an ID-based aggregate signature (IBAS) scheme for WSNs in cluster-based method . The opponent in our refuge model has the competence to presentation any alliance attacks. If an opponent can use some solitary signatures counting invalid ones to make a valid aggregate signature approximately that the attack is successful. In detail, our ID-based aggregate signature scheme not only can defend data integrity, but also can lessen bandwidth and storage cost for WSNs. we largely attention on data integrity shield, give an identity-based aggregate signature scheme with a selected verifier for wireless sensor networks. Outline not only can keep data integrity, but also can cut bandwidth and storage cost for wireless sensor networks.

KEYWORDS: attacker, signatures, identity

1 INTRODUCTION:

The user's public key is effortlessly generated from this user's any sole identity information which is expected to be openly recognized. A right-hand third party, called the private key generator (PKG), makes and subjects clandestinely the consistent private keys for all users by a master secret key. Consequently, in an ID-based signature (IBS) system, verification algorithm only contains the signature pair, some public parameters and the uniqueness information of signer, deprived of consuming an additional certificate. The aggregate signature's legitimacy can be alike to the soundness of every signature which is used to cause the aggregate signature. That is to say, the amassed signature is strength if and only if each specific signer really retained its original message, separately. Later, aggregation is advantageous procedure in falling 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.

2 LITERATURE SURVEY:

1] The wished-for confirmation outline ponders the smart meters with computation-constrained properties and puts the tiniest addition overhead on them. Complete security breakdown directs its security strength, explicitly, bounciness to the replay attack, the message injection attack, the message analysis attack, and the message modification attack. In tallying, all-embracing show assessment proves its efficacy in terms of addition difficulty and communication overhead.

2] We proposition two certificateless aggregate signature schemes, which are the first aggregate signature schemes in the CL-PKC. The first scheme CAS − 1 cuts the costs of communication and signer-side computation but misses on storage, while CAS − 2 decreases the storage but martyrs the communication.. Our patterns do not prerequisite the public key certificate any longer and do the trust level 3, the same level with traditional PKI. Together of the schemes are established safe in the random oracle model (ROM) by presumptuous the difficulty of the computational Diffie-Hellman(CDH) problem ended groups with bilinear maps.

3 PROBLEM DEFINTION:

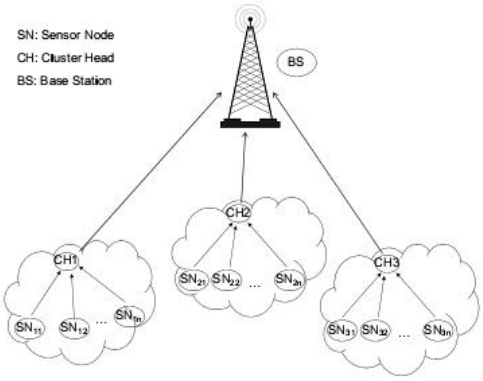
The aggregate signature's cogency can be equal to the cogency of each signature which is used to make the aggregate signature. The aggregate signature is cogency if and only if each individual signer actually signed its original message, correspondingly. Henceforth, aggregation is valuable method in plummeting storage cost and bandwidth, and can be a conclusive building block in certain settings, such as data aggregation for WSNs, securing border gateway protocols and large scale electronic voting system, etc.

4 PROPOSED APPROACH:

The system ideal which have three components: data center, aggregator and a big number of sensor nodes. Aggregator works as a cluster head, can crop the aggregate signature and direct it to the data center with the messages made by the sensor nodes. Formerly, done a game played with a contender and an rival, the security model of identity-based aggregate signature schemes is familiarized. And in the security model, the aggregation algorithm should struggle all kinds of coalition attacks.

Our scheme is self-possessed of six probabilistic polynomial time (PPT) algorithms: Setup, Key Generation, Signing, Verification, Aggregation and AggVerification. The exhaustive security proof is given based on the computational Diffie-Hellman assumption in casual oracle model. The safekeeping proof directs that our ID-based aggregate signature scheme for wireless sensor networks can warrant the reliability of the data and shrink the statement and loading price.

5 SYSTEM ARCHITECTURE:



6 PROPOSED METHODOLOGY:

Data center

Data center has a stout computing power and storage space. So it can development all novel big data poised by sensor nodes fit in to the data center, and can run the data information to clients. At the be-ginning, every data center will have its public-secret key pair (PKcenter ,SKcenter), and circulate the public key PKcenter.

Aggregator

Aggregator is a special sensor node with definite facility to design and communication range. It can badge messages amassing from the corporeal world, can get the data center's public key PKcenter from public channel, can create the aggregate signature from the distinct signatures engaged by sensor nodes encompassed aggregator itself, and can send the aggregate signature to the data center.

Sensor node

Sensor node has restricted resources in terms of computation, memory and battery power. When sensor node ID I is arrayed, it is embedded with (param, SIDi). Every sensor node ID i can use its private key SIDi to sign messages gathering from the physical world. In our scheme, all sensor nodes fits 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 indiscriminately spread with a constant distribution. Casually select one of the organized nodes as the source node. The site of the sink is arbitrarily strong-minded.

We assess our future method with admiration to PDR, E2E latency, PLR and Energy consumption.

7 A NEW IBA 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: Key Generation 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

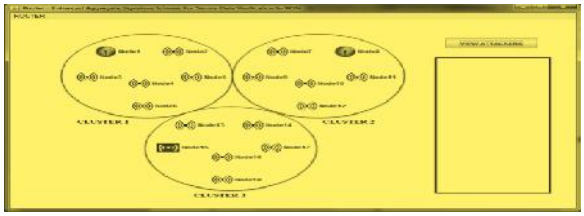
Step5: Aggregation Phase:

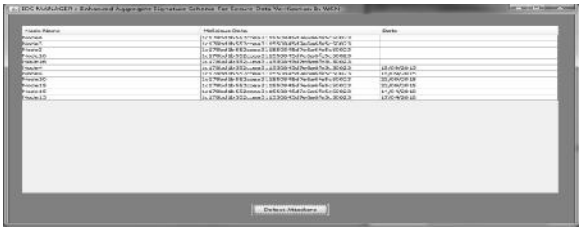
a) In this phase an aggregate subset of sensor nodes belong to one cluster, each sensor node with the identity *IdI* provides a signature on a message Gained the data center's public key *PKcenter*from public channel.

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.

8 RESULTS:





Results shows the attacks in IDS Manager.

EXTENSION WORK:
Proposing ECC 160 bit algorithm for identity based signature scheme which moderates communication and calculation slide.

9 CONCLUSION:
Sensor nodes in positions of calculation, remembrance and battery power, protected and energy-save data aggregation methods should be calculated in WSNs to diminish the vigor cost of data collection, data processing and data transmission. We extant an ID-based aggregate signature scheme for WSNs, which can bandage numerous signatures made by sensor nodes into a short one, i.e., it can shrink the communication and storage cost. We have attested that our IBAS scheme is safe and sound in random oracle model based on the CDH postulation, and we also have demonstrated that our aggregate signature can attack coalition attacks, that is to around the aggregate signature is effective if and only if every single signature used in the accretion is valid. In our future work, we will concentration on wily more competent data aggregation schemes.

10 REFERENCES:

[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 Sup-porting 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] LiminShen, 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.