ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 6, Special Issue 12, July 2017

A Secure Effective Id -Based Cluster Signature Strategy for Wireless Sensor Networks

Manjunath Varchagal[1]

Asst. Professor, Department of ISE, SVIT College, Rajanukunte, Karnataka, India[1]

ABSTRACT: Affording secure and effective large information aggregation technology is very interesting in the area of wireless sensor networks investigation. In real settings, the wireless sensor networks have been widely applied, such as objective or target follow or tracking and environment remote monitoring. However, data can be easily compromised by a vast of attacks, such as data interception and data tampering, etc. In this paper, we mainly focus on data integrity protection; give an identity-based aggregate signature scheme with a designated verifier for wireless sensor networks. According to the advantage of aggregate signatures, our scheme not only can keep data integrity, but also can reduce bandwidth and storage cost for wireless sensor networks. Furthermore, the security of our identity-based aggregate signature scheme is rigorously presented based on the computational Diffie-Hellman assumption in random oracle model.

KEYWORDS: Big data, wireless sensor network, identity based, data aggregation, unforgeability, aggregate signature, coalition attack, designated verifier.

I. INTRODUCTION

In big data or alongside huge information era, advanced universe grows in staggering velocity which is processed Eventually Tom's perusing developing new services, for example, such that social network, cloud registering What's more web for things. Enormous information are assembled Eventually Tom's perusing inescapable remote sensor networks, flying tangible technologies, programming logs, information-sensing portable devices, microphones, cameras, and so forth. And the remote sensor system will be a standout amongst the profoundly foreseen key contributors of the huge information later on networks. Remote sensor networks (WSNs), for an expansive amount for cheap, little What's more Exceedingly compelled sensor hubs sense those physical world, need exceptionally expansive provision prospects both clinched alongside military Furthermore citizen usage, including military focus following and surveillance, creature natural surroundings monitoring, biomedical wellbeing monitoring, incredulous offices following. It could be utilized within a portion danger environment, for example, over atomic force plants. Because of the momentous advantages, far reaching consideration need been committed on WSNs, What's more a number about schemes need been exhibited.

In WSNs, sensor nodes are usually resource-limited and power-constrained; they always suffer from the restricted storage and processing resources. 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 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. Hence, designing a secure and efficient data aggregation method is very significant for WSNs. In 1984, Shamir introduced the identity-based (ID-based) cryptography, which eases the key management problem by

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 6, Special Issue 12, July 2017

eliminating public key certificates. In an ID-based cryptography, the user's public key is easily generated from this user's any unique identity information (e.g. the serial number, a mobile phone number, an email address, etc), which is assumed to be publicly known.

A trusted third party, called the private key generator (PKG), generates and issues secretly the corresponding private keys for all users using a master secret key. Therefore, in an ID-based signature (IBS) system, verification algorithm only involves the signature pair, some public parameters and the identity information of signer, without using an additional certificate.In 2003, Boneh et al. introduced an aggregate signature scheme, which can compress multiple signatures generated by different users on different messages into a single short aggregate signature. The aggregate signature's validity can be equivalent to the validity of every signature which is used to generate the aggregate signature. That is to say, the aggregate signature is validity if and only if each individual signer really signed its original message, respectively. Hence, aggregation is useful technique in reducing storage cost and bandwidth, and can be a decisive building block in some settings, such as data aggregation for WSNs, securing border gateway protocols and large scale electronic voting system, etc. And combining the highlights of aggregate signature scheme and ID-based cryptography, we give an ID-based aggregate signature (IBAS) scheme for WSNs in cluster-based method (Fig. 1). The adversary in our security model has the capability to launch any coalition attacks. If an adversary can use some single signatures including invalid ones to generate a valid aggregate signature, we say that the attack is successful. In fact, our ID-based aggregate signature scheme not only can protect data integrity, but also can reduce bandwidth. Personal use is permitted content may change prior to final publication and also storage cost for WSNs. The main contributions of this paper are fourfold.

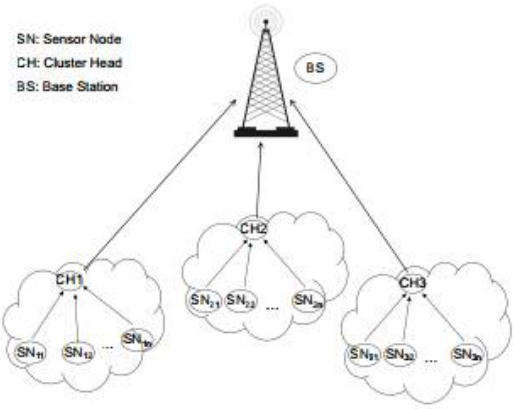

Fig. 1. Cluster-Based Network

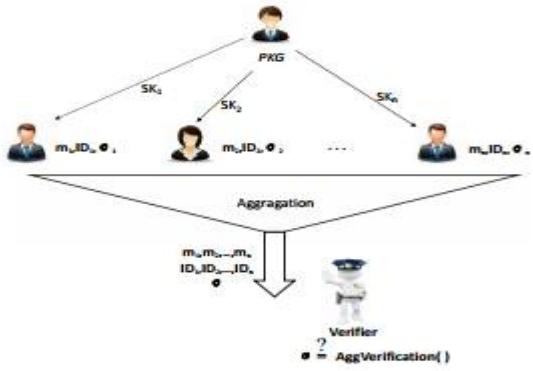

Fig. 2. ID-Based Aggregate Signature Scheme

• **First,** we give the system model which has three components: data center, aggregator and a large number of sensor nodes. Aggregator works as a cluster head, can produce the aggregate signature and send it to the data center with the messages generated by the sensor nodes. Then, through a game played with a challenger and an adversary, the security model of identity-based aggregate signature schemes is introduced. And in the security model, the aggregation algorithm should resist all kinds of coalition attacks.

• **Second,** we give a secure identity-based aggregate signature scheme for wireless sensor networks with a designated verifier (data center). Our scheme is composed of six probabilistic polynomial time (PPT) algorithms: Setup, KeyGeneration, Signing, Verification, Aggregation and Agg-Verification.

• **Third,** the detailed security proof is given based on the computational Diffie-Hellman assumption in random oracle model. The security proof indicates that our ID-based aggregate signature scheme for wireless sensor networks can ensure the integrity of the data and reduce the communication and storage cost.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 6, Special Issue 12, July 2017

• **Fourth,** through the analysis of comparative performance, we demonstrate that our identity-based aggregate signature scheme is efficient in terms of the communication and storage overhead. The rest of the paper is organized as follows. In the following section, we introduce some related work about aggregate signature schemes. Section III presents the system model and security model of ID-based aggregate signature schemes. Our ID-based aggregate signature scheme is presented in Section IV. In section IV, we analyze the performance of our IBAS scheme in terms of communication and computation cost. Finally, Section V is the conclusions.

II. RELATED WORK

The aggregate signature scheme can generate a compressed signature from many signatures generated by different users on different messages. Boneh et al. introduced the concept and structure of aggregate signature schemes in 2003. After that, many aggregate signature schemes have been presented. However, there still exist a lot of problems in the above schemes. In traditional public key infrastructures($PKIs$), the user's public key is not related to the user's identity information; in fact, it is a "random" string. So there needs a trusted certificate authority to generate certificates which can ensure the relationship between the user and the cryptographic keys. This improves the communication overhead, computation and storage cost and would influence the efficiency of the aggregate signature scheme.
Cluster-Based Network cryptography solved these problems. In an ID-based cryptography, the user's public key is any publicly known and unique identity information, such as the serial number, and the user no longer needs a certificate to prove its identity. Since then, many ID-based aggregate signature schemes (Fig. 2) have been presented. Up to now, a great many aggregate signature schemes have rapidly emerged in various settings, such as in PKIs and in Certificateless Public Key Cryptography (CL-PKC), respectively show security drawbacks of the certificate less aggregate signature scheme by demonstrating some kinds of attacks. Unfortunately, most of the existing aggregate signature schemes cannot resist a kind of practical and powerful attacks coalition attacks. Coalition attack can generate a valid aggregate signature by using some invalid single signatures with the collusion of two or more signers. If such an attack is successful, the corresponding aggregate signature will pass the validation while some single signatures used to generate it are invalid. This suggests that a valid aggregate signature may fail to prove the validity of every individual signature involved in the aggregation. This fact obviously violates the security goal for aggregate signature schemes. So, in this paper, we will mainly focus on designing the aggregate signature scheme which can resist coalition attacks.

III. SYSTEM MODEL AND SECURITY MODEL

A. SYSTEM MODEL

Security requirements in WSNs mainly are confidentiality, integrity, authenticity, scalability and flexibility, etc. In a data aggregation scheme for WSNs, it is important that no data falsify during transmissions. So we mainly focus on the data integrity protection in our system. The main consideration of our system model is to protect data integrity while reducing bandwidth and storage cost for WSNs. Our IBAS system consists of three parts (Fig. 3): Data Center, aggregator and sensor node.

• **DATA CENTER** has a strong computing power and storage space. So it can process all original big data collected by sensor nodes belong to the data center, and can provide the data information to consumers. At the beginning, every data center (as the designated verifier in our IBAS scheme) will receive its public-secret key pair (PK_{center},SK_{center}), and publish the public-key PK_{center}.

- **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 $PKcenter$ from public channel, can generate the aggregate signature from the individual signatures signed by sensor nodes included aggregator itself, and can send the aggregate signature to the data center. We assume that the PKG generates the system parameters param, aggregator's private key S_{ID} corresponding to its identifier information ID, then embeds (param, S_{ID}) in aggregator when it is deployed.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 6, Special Issue 12, July 2017

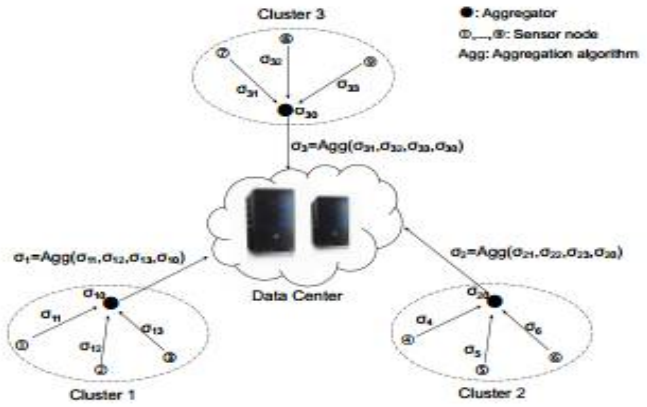

Fig. 3. Our System

- **SENSOR NODE** has limited resources in terms of computation, memory and battery power. We assume that the PKG generates private key S_{IDi} for each sensor node IDi . When sensor node ID_i is deployed, it is embedded with (param, S_{IDi}). Every sensor node ID_i can use its private key S_{IDi} to sign messages collecting from the physical world. In our system, each sensor node belongs to one cluster, sends messages and its signatures to their aggregator, and the messages will finally be sent to data center via aggregator.

B. SECURITY MODEL OF IBAS

An IBAS scheme is comprised of six PPT algorithms: Setup, KeyGeneration, Signing, Verification, Aggregation and AggVerification. Obviously, the goal of an adversary is the existential forgery of an aggregate signature. An IBAS scheme is secure if the basic signature scheme involved is existentially unforgeable against adaptive chosen message attacks (EUF-CMA secure, and the aggregation algorithm should stand up against all kinds of coalition attacks. Most of the former security models only consider the security of the basic signature scheme and the forgery of an aggregate signature, and do not consider the coalition attacks. So we mainly focus on the security of aggregation algorithm. When attacking the aggregation algorithm, the purpose of an adversary is to forge a valid aggregate signature while using some invalid individual signatures. The following is a game played with a challenger B and an adversary A.

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 data center (designated verifier), then B gives param and $PKcenter$ to A.

Queries Phase

Step 3: KeyGeneration query O_s(ID): On receiving such a query, challenger B responds by running KeyGeneration algorithm to obtain the private key S_{ID} of the user ID, returns S_{ID} to A.

Step 4: Signing query O_{sig}(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 KeyGeneration algorithm if necessary.)

Step 5: AggVerification query O_{AggV} ({mi, ID_i, i = 1, . . . ,n}, σ): 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 , σj , j = 1, . . . , n}, σ∗). A is success if The aggregate signature σ∗ is valid on tuple {m_j ,ID_j σ_j , j = 1, . . . , n}.

Step 7: At least one individual signature σ_j(j = 1, . . . , 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.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 6, Special Issue 12, July 2017

IV PERFORMANCE ANALYSIS

In this section, evaluating the performance of our IBAS scheme. We give the description of some notations to be used in this section in TABLE I.

A. Comparison of Un-aggregation and Aggregation Schemes we give the performance comparison of two versions of un-aggregation and aggregation schemes in this section, and un-agg and agg denote the un-aggregation and aggregation schemes, respectively. We firstly review the abilities of each component in our scheme. Sensor node has limited resources in terms of computation, memory and battery power, aggregator has a certain ability to calculation and communication range and it works as a special sensor node, data center has a strong computing power and storage space. So, our scheme's objectives are trying to reduce the communication cost and storage cost of aggregator and sensor node. So, our scheme's objectives are trying to reduce the communication cost and storage cost of aggregator and sensor node.

Without loss of generality, we assume the aggregator's identity is IDn in a cluster which has n sensor nodes $\{ID1, ID2, \ldots, IDn\}$. The performance in terms of communication and computation cost is shown as following. Without loss of generality, we assume the aggregator's identity is IDn in a cluster which has n sensor nodes $\{ID1, ID2, \ldots, IDn\}$. The performance in terms of communication and computation cost is shown as following.

Table I:Definition of Notation

Notation	Definition
agg	aggregation scheme
$un\text{-}agg$	un-aggregation scheme
$\|M\|$	the overall length of $\{m_1, m_2, \ldots, m_n\}$
$\|M'\|$	the overall length of $\{m_1, m_2, \ldots, m_{n-1}\}$
$\|ID\|$	the overall length of $\{ID_1, ID_2, \ldots, ID_n\}$
$\|ID'\|$	the overall length of $\{ID_1, ID_2, \ldots, ID_{n-1}\}$
M_1	the computation cost of a scalar multiplication calculation in G_1
M_2	the computation cost of a multiplication calculation in G_2
exp	the computation cost of an exponentiation operation in G_1
Exp	the computation cost of an exponentiation operation in G_2
$Pairing$	the computation cost of a pairing operation in G_2

1) **Communication Cost:** The comparison of communication cost indicates that the aggregate scheme can reduce (n − 1)|G1| transmission in one data aggregation process, simultaneously, can reduce (n − 1)|G1| storage cost. Therefore, our scheme is an efficient data aggregation method for the wireless sensor networks.

Table ii: Performance comparison of computation cost

	$un\text{-}agg$	agg
Each sensor node	$2M_1$	$2M_1$
Aggregator	0	$n \cdot Pairing + M_1$
Data center (Verification)	$2n \cdot Pairing + n \cdot M_2$	$(n+1) \cdot Pairing + (n+1) \cdot Exp + (2n+1) \cdot M_2$

2) Computation Cost: Let P airing, M1, M2 and Exp be the computation cost of a pairing operation in G2, a scalar multiplication calculation in G1, a multiplication calculation in G2 and an exponentiation operation in G2, respectively.

B. Efficiency Comparison In this section, we give the efficiency comparison of our CLAS scheme with some existing pairing based schemes (TABLE III).

Scheme just achieve partial aggregation, and then require linear number of pairings, and ours is needed more pairings in aggregation verification process. Generally it has constant number of pairing operations during the aggregation verification, but, their scheme has some security weaknesses which have been reported and it has a trivial weakness

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 6, Special Issue 12, July 2017

which is alike to the scheme. And the signature scheme is deterministic, that is to say, the signature generated by a user on a message remains the same.

V. CONCLUSION AND FUTURE ENHANCEMENT

Due to the limited resources of sensor nodes in terms of computation, memory and battery power, secure and energy save data aggregation methods should be designed in WSNs to reduce the energy cost of data collection, data processing and data transmission. An ID-based aggregate signature scheme for WSNs, which can 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 based on the CDH assumption, and 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. Designing more efficient data aggregation schemes may be future work.

REFERENCES

[1] I. Paik, T. Tanaka, H. Ohashi and W. Chen, "Big Data Infrastructure for Active Situation Awareness on Social Network Services," Big Data (BigData 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 Finegrained 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 Outsourced Computation over Public Data," IEEE Transactions on Services Computing, 2015
[8] 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.
[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