A Secure and Efficient ID-Based Aggregate Signature Scheme for Wireless Sensor Networks

Ms. Krithika Pa[1],Smt. Jayasri B.S[2]
[1]M.Tech, [2]Associate Professor
Information Technology1, Department of Computer Science and Engineering2, NIE Mysore

Abstract **-** Affording secure and efficient big data aggregation methods is very attractive in the field of wireless sensor networks research. In real settings, the wireless sensor networks have been broadly applied, such as target 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 era, digital universe grows in stunning speed which is produced by emerging new services, such as social network [1] [2], cloud computing [3] [4] [5] [6] [7] and internet of things [9] [10]. Big data are gathered by omnipresent wireless sensor networks, aerial sensory technologies, software logs, information sensing mobile devices, microphones, cameras, etc [11]. And the wireless sensor network is one of the highly anticipated key contributors of the big data in the future networks [12].

Wireless sensor networks (WSNs), with a large number of cheap, small and highly constrained sensor nodes sense the physical world [13], has very broad application prospects [14] both in military and civilian usage, including military target tracking and surveillance [15], animal habitats monitoring [16], biomedical health monitoring [17] [18], critical facilities tracking [19]. 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 [20], and a number of schemes have been presented [21] [22] [23] [24] [25].

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 [26], which eases the key management problem by 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. [27] 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 [22], securing border gateway protocols [28] and large scale electronic voting system [29], etc.

In this paper, 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 and storage cost for WSNs. The main contribution of this paper is fourfold which are as follows

- First, we give the system models which have 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, Key Generation, 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.
- 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, some related work about aggregate signature schemes is introduced. Section III presents the system model and security model of ID-based aggregate signature schemes. Finally, Section VIII 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. [27] introduced the concept and structure of aggregate signature schemes in 2003. After that, many aggregate signature schemes have been presented [30] [31] [32] [33]. 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.ID-based cryptography [26] 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.

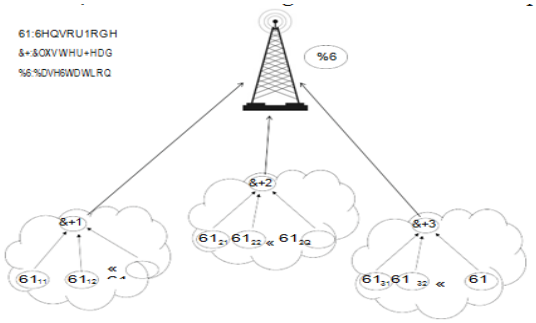

Figure1: Cluster-Based Network

Since then, many ID-based aggregate signature schemes have been presented [34] [35] [36] [37]. Up to now, a great many aggregate signature schemes have rapidly emerged in various settings, such as [38] [39] in PKIs and [40] [41][42] [43] [44] in Certificate less Public Key Cryptography (CL-PKC), respectively. Both [43] and [45] show security drawbacks of the certificate less aggregate signature scheme in[42] 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 [43] [46] [47]. 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 ARCHITECTURE

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: datacenter, aggregator and sensors 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 ($P K_{center}$, SK_{center}), and publish the public key $P K_{center}$.
- **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 $P K_{center}$ 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.

- **Sensor node** has limited resources in terms of computation, memory and battery power. 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.

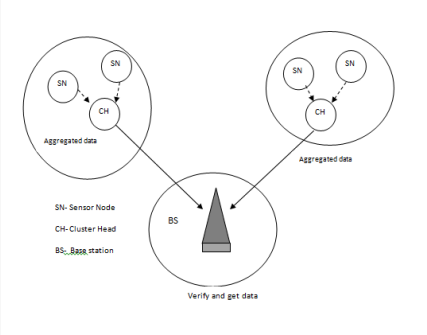

Figure 2: System model

IV. EXISTING SYSTEM

Identity-based (ID-based) cryptography: Shamir introduced the identity-based (ID-based) cryptography, which eases the key management problem by 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, 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.

Aggregate signature scheme: 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.

V. PROPOSED SYSTEM

- Combining the highlights of aggregate signature scheme and ID-based cryptography, an ID-based aggregate signature (IBAS) scheme is proposed for WSNs in cluster-based method. The adversary in 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.
- System model is designed as 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.
- A secure identity-based aggregate signature scheme for wireless sensor networks with a designated verifier. Proposed scheme is composed of six probabilistic polynomial time (PPT) algorithms: Setup, Key Generation, Signing, Verification, Aggregation and Agg Verification.
- The detailed security proof is given based on the computational Diffie-Hellman assumption in random oracle model. The security proof indicates that ID based aggregate signature scheme for wireless sensor networks can ensure the integrity of the data and reduce the communication and storage cost.

Advantages: ID-based aggregate signature scheme not only can protect data integrity, but also can reduce bandwidth and storage cost for WSNs.

VI. CONCLUSION

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. In this paper, 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 is presented. Moreover it is proved that the IBAS scheme is secure in random oracle model based on the CDH assumption, and it is 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. In the future work, we will focus on designing more efficient data aggregation schemes.

VII. 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),
[2]. E. Hargittai 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,"
[4]. I. Hashem, I. Yaqoob, N. Anuar, et al., "The rise of "big data" on cloud computing: Review and open research issues,"

[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,"
[6]. H. Li, D. Liu, Y. Dai and T. Luan, "Engineering Searchable Encryption of Mobile Cloud Networks:
[7]. X. Liu, B. Qin, R. Deng, Y. Li, "An Efficient Privacy-Preserving Out- sourced Computation over Public Data,"
[8]. X. Liu, R. Choo, R. Deng, R. Lu, "Efficient and privacy-preserving out- sourced calculation of rational numbers,"
[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,"
[10]. H. Li, R. Lu, L. Zhou, B. Yang, X. Shen, "An Efficient Merkle Tree Based Authentication Scheme for Smart Grid,"
[11]. C. Chen, C. Zhang, "Data-intensive applications, challenges, techniques and technologies:
[12]. D. Takaishi, H. Nishiyama, N. Kato and R. Miura, "Toward Energy Efficient Big Data Gathering in Densely Distributed Sensor Networks,"
[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,"
[14]. I.F. Akyildiz, W. Su, Y. Sankara subramaniam and E. Cayirci, "A survey on sensor networks,"
[15]. Ghosal, "Analysis of a prediction-based mobility adaptive tracking algorithm,"
[16]. A. Mainwaring, J. Polastre, R. Szewczyk, D. Culler and J. Anderson, "Wireless Sensor Networks for Habitat Monitoring,"
[17]. X. Lin, R. Lu, X. Shen, Y. Nemoto and N. Kato, "Sage: a strong privacy- preserving scheme against global eavesdropping for e health systems,"
[18]. R. Lu, X. Lin and X. Shen, (2013) "SPOC: A secure and privacy- preserving opportunistic computing framework for mobile-healthcare emergency,"
[19]. N. Xu, S. Rangwala, K.K. Chintalapudi, D. Ganesan, A. Broad, R. Govindan and D. Estrin, "A Wireless Sensor Network for Structural Monitoring,"
[20]. J. Yick, B. Mukherjee and D. Ghosal, "Wireless sensor network survey,"
[21]. N. Pereira, R. Gomes, B. Andersson, and E. Tovar, "Efficient Aggregate Computations in Large-Scale Dense WSN,"
[22]. X. Liu, H. Zhu, J. Ma, Q. Li and J. Xiong, "Efficient attribute based se- quential aggregate signature for wireless sensor networks,"
[23]. Y. Zhang, L. Sun, H. Song, et al., "Ubiquitous WSN for Healthcare: Recent Advances and Future Prospects,"
[24]. M. Rezvani, A. Ignjatovic, E. Bertino et al., "Secure Data Aggregation Technique for Wireless Sensor Networks in the Presence of Collusion Attacks,"
[25]. R. Alves, L. Gabriel, B. Trevizan, et al., "Assisting Physical (Hydro) Therapy With Wireless Sensors Networks
[26]. A. Shamir, "Identity-based cryptosystems and signature schemes.
[27]. D. Boneh, C. Gentry, B. Lynn and H. Shacham, "Aggregate and verifiably encrypted signatures from bilinear maps", in Proc. Eurocrypt 2003, Warsaw, Poland. LNCS, pp. 416-432,2003.
[28]. S. Kent, C. Lynn, K. Seo, "Secure Border Gateway Protocol," IEEE Journal of Selected Areas in Communications
[29]. J. Koning, D. Dubois, "Suitable properties for any electronic voting system,"
[30]. A. Lysyanskaya, S. Micali, L. Reyzin and H. Shacham, "Sequential aggregate signatures from trapdoor permutations",
[31]. A. Boldyreva, C. Gentry, A. O'Neill and D.H. Yum, "Ordered multisig- natures and identity-based sequential aggregate signatures, with applications to secure routing",
[32]. J.H. Ahn, M. Green and S. Hohenberger, "Synchronized aggregate signatures: new definitions, constructions and applications",
[33]. Z. Shao, "Enhanced aggregate signatures from pairings," in Proce. CISC 2005,LNCS3822, Springer-Veralg,pp.140-149,2005.
[34]. J. Xu, Z. Zhang and D. Feng, "ID-Based Aggregate Signatures from Bilinear Pairings,"
[35]. G. Gentry and Z. Ramzan, "Identity-based aggregate signatures," in Proc. Public Key Cryptography, LNCS vol.3958,pp.257-273,2006.
[36]. J. Herranz, "Deterministic identity-based signatures for partial aggregation,"TheComputerJournal,vol.49,no.3,pp.322-330,2006.
[37]. S.S.D. Selvi, S.S. Vivek, J. Shriram et al., "Identity based partial aggregate signature scheme without pairing," in Proc. 35th IEEE. Sarnoff Symposium (SARNOFF), pp. 1-6,2012.
[38]. J. Li, K. Kim, F.Zhang and X.Chen, "Aggregate proxy signature and verifiably encrypted proxy signature,"
[39]. Y. Wen, J. Ma and H. Huang, "An Aggregate Signature Scheme with Specified Verifier,"
[40]. Z. Gong, Y. Long, X. Hong and K. Chen, "Two certificate less aggregate signatures from bilinear maps,"
[41]. L. Zhang, B. Qin, Q. Wu and F. Zhang, "Efficient many-to-one authentication with certificate less aggregate signatures,"
[42]. H. Xiong, Z. Guan, Z. Chen and F. Li, "An efficient certificate less aggregate signature with constant pairing computations,"
[43]. F. Zhang, L. Shen and G. Wu, "Notes on the security of certificate less aggregate signature schemes," Information Sciences, vol. 287, pp. 32-37, 2014.
[44]. S. Horng, S. Tzeng, P. Huang, X. Wang et al, "An efficient certificate less aggregate signature with conditional privacy-preserving for vehicular sensor networks," Information Sciences,vol.317,pp.48-66,2015.
[45]. D. He, M. Tian and J. Chen, "Insecurity of an efficient certificate less aggregate signature with constant pairing computations," Information Sciences,vol.268,pp.458-462,2014.
[46]. K.A. Shim, "On the Security of a Certificate less Aggregate Signature Scheme," IEEE COMMUNICATIONS LETTERS, vol. 15, no. 10,pp. 1136-1138,2011.
[47]. N. Viet and W. Ogata, "Certificate less Aggregate Signature Schemes with Improved Security," Ieice Transactions on Fundamentals of Electronics Communications &Computer Sciences, e98.a(1), pp. 92-99,2015.
[48]. D. Xing, Z. Cao and X. Dong, "Identity based signature scheme based on cubic residues,"
[49]. R. Sakai, K. Ohgishi and M. Kasahara, "Cryptosystems based on pairing,"
[50]. J.Shao, R.LuandX.Lin,"Fine grained data sharing in cloud computing for mobile devices,"