© 2017 IJSRST | Volume 3 | Issue 8 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X
Themed Section: Scienceand Technology

ID-Based Data Integrity Scheme Using Cluster Method For Wireless Sensor Networks

M. Mohammed Mohiddin
PG Scholar, JNTUA College of Engineering, Ananthapuramu, Andhra Pradesh, India

ABSTRACT

The main goal of the data aggregation schemes in wireless sensor networks is to gather and aggregate data in an energy efficient manner so that network lifetime is enhanced. However, the technique still has the inherent security problems and can be easily compromised by a vast of attacks, such as reply attacks, data interception and data tampering, etc. Hence, the goal is to design a secure and efficient data integrity scheme, given an Identity-based aggregate signature with a designated verifier for wireless sensor networks. In this model the sensor nodes are grouped into clusters for efficient data transmission, Clustering is an effective way to enhance the system performance of wireless sensor networks. This model can not only keep data integrity but also can reduce bandwidth and storage cost for wireless sensor networks. The security of this scheme is provably secure in the random oracle model under the computational Diffie–Hellman assumption.

Keywords: Wireless Sensor Network, Id-based Cryptography, Data Aggregation, Aggregate Signature, Data Integrity, Coalition Attack, Elliptic Curve Cryptography, Verifier, Encryption, Decryption.

I. INTRODUCTION

A wireless sensor network (WSN) is a wireless network consisting of spatially distributed autonomous devices using sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. These sensor nodes, which consist of sensing, data processing, and communicating components, result in the idea of sensor networks based on collaborative effort of a large number of nodes. Such sensor nodes could be deployed in home, military, science, and industry applications such as transportation, health care, disaster recovery, warfare, security, industrial and building automation, and even space exploration.

In WSNs, data aggregation refers to the use of aggregation techniques to reduce the amount of bytes required to code the different pieces of information and, thus, the traffic load which needs to be processed within the network.Because of these advantages a lot of attention has been paid to WSNs [1]. Sensor nodes are usually resource-limited and power-constrained; they always suffer from the restricted storage and processing resources.

The concept of aggregate signature was first introduced by Boneh et al. at Eurocrypt 2003 [2]. The aggregate signatures are digital signatures where anyone, given n signatures on n messages from n users, can combine all of these signatures into a single short signature. The resulting signature can convince a verifier that the n users indeed signed the n corresponding messages. By this way, aggregate signature can greatly reduce the computational and communication overhead.Hence, aggregation is useful technique in reducing storage cost and bandwidth.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.

This paper proposes a model combining the features of aggregate signature scheme and ID-based cryptography to give an ID-based data integrity scheme using cluster method for WSNs.The security of this model can resist all kind of coalition attacks [3]. The aggregate signature scheme is valid if and only if every individual signature used in the aggregation is valid.

This paper is classified as following: In section-II the basic details of Aggregate Signature schemes and ID

IJSRST1738215 | Received:25Nov 2017 | Accepted : 25Dec 2017 | November-December-2017[(3)8: 983-989]

based cryptography is discussed. In section-III and section-IV the complete system and security model of ID-based data integrity scheme is analysed and reviewed and to show how to resist all kinds of coalition attacks. The design and implementation is discussed in section-V. The Simulation results and performance analysis of this implementation of ID based data integrity scheme is discussed in Section-VI and section-VII. Finally, the section-VIII deals with the conclusion.

II. RELATED WORK

The concept of aggregate signature was introduced by Boneh et al in 2003. The main feature of Aggregate signatures is that it allows an efficient algorithm to aggregate n signatures of n distinct messages from n different users into one single signature. The resulting aggregate signature can convince a verifier that the n users did indeed sign the n messages.

To let a signature scheme function, the public key has to be bound with the identity of the owner of the public key. Traditionally, this is provided by the public key infrastructure (PKI) in which a third party known as certificate authorities (CAs), issue digital certificates to bind a user and his public key. In this scheme, before using the public key of a user, the participant must first verify the certificate of the user, which results in a large amount of computing and storage cost to manage certificates, to overcome these problems Shamir introduced the identity-based public key cryptography (ID-PKC) [4] to simplify certificate management in PKI systems. In this scheme, 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. Hence, ID-PKC suffers from a key escrow problem which implies that all the users have to fully trust PKG.

To address the key escrow problem of ID-PKC scheme, Al-Riyami and Paterson [5]invented a new scheme called certificateless public key cryptography (CLPKC). CL-PKC also exploits a third party called Key Generation Center (KGC) to help a user to generate his private key. However, the KGC can merely determine part of the private key for each user. In CL-PKC, the user computes the resulting private key with the partial private key resulted from the KGC and the secret information chosen by the user. As a result, CL-PKC systems avoid the key escrow problem.

Since then, many ID-based aggregate signature schemes have been presented [6] [7].But, most of the existing CLAS schemes cannot sustain a type of practical and harmful attacks called coalition attacks [8]. If a coalition attack can generate a valid aggregate signature using a few invalid single signatures with the collusion of two or more signers. If this attack is succeeded then the aggregate signature will pass the validation. This indicates that a valid aggregate signature may fail to prove the validity of every single signature involved in the aggregation. So, this paper mainly focuses on designing the secured and efficient aggregate algorithm which can resist such coalition attacks.

III. SYSTEM ARCHITECTURE

The main aim of this system model is to protect data integrity while reducing bandwidth and storage cost for WSNs.The system architecture consists of four components namely:

- ✓ Key Generator
- ✓ Base Station
- ✓ Aggregator
- ✓ Sensor Nodes

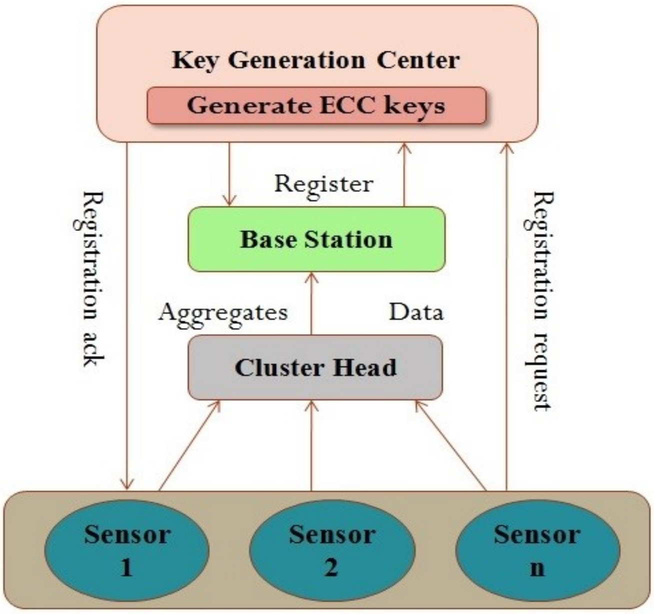

Figure 1. Architecture of the system

Key Generatoris a key server which generates unique public and private keys for base station and sensor nodes and uses Elliptic Curve Cryptography algorithm to generate keys.It also shares public keys of sensor nodes and base station.

Base Stationpossesses much more computational power and larger memoryand it is often connected to a better source of energy. The base station's primary goal is to gather sensed data from sensor nodes in WSN. Sensed data can be stored, visualized and analyzed.

Aggregatoris one of the important methods for prolonging the network lifetime in wireless sensor networks (WSNs). It involves grouping of sensor nodes into clusters and electing cluster heads (CHs) for all the clusters. CHs collect the data from respective cluster's nodes and forward the aggregated data to base station.

Sensor Nodes are used by wireless sensor nodes to capture data from their environment. They are hardware devices that produce a measurable response to a change in a physical condition like temperature or pressure. Each sensor node belongs to one cluster, sends encrypted messages to their aggregator, and the messages will finally be sent to data center via aggregator.

IV. SECURITY MODEL

An ID-based Data-Integrity signature (IBDS) scheme is a tuple of probabilistic polynomial-time algorithms.
The description of each algorithm is as follows.
Setup, KeyGeneration, Sign, Verify, Aggregation, VerifyAgg.

Setup: This algorithm is run by a key generation center (KGC). G1, G2 are two cyclic groups of prime order p. Let ê: G1 × G1 → G2 be a bilinear pairing, and let P be an arbitrary generator of G1. H1, H2 and H are full-domain collision resistant hash functions. H1, H2: {0, 1}* → G1, H: G2 $\rightarrow Z^*_p$. KGC chooses x,yє Z^*_p randomly and computes P0 = xP, PK_{ctr} = yP. Then the system parameters are param = {ê,G1,G2, P, p,H1,H2,H, P0}, the master secret key is msk = x. The data center's public-secret verification key is (PK_{ctr} = yP, SK_{ctr} = y).

Key Generation: This algorithm takes a user's identity ID_i. Compute Q_i=$H_1(ID_i)$ and the sensor node's corresponding private key is $D_i = xQ_i$. The KGC sends D_i to the user ID_ithrough a secure channel.

Sign: This algorithm takes a system parameters params, a message mi, an identity ID_i and corresponding private key D_i as input, and outputs an individual signature σ on the message mi for the user with identity ID_i and generates t_iє Z_p*

$$T_i = t_iP,$$
$$h_i = H2(T_i, ID_i,m_i),$$
$$U_i = D_i + t_ih_i.$$

Verify: This algorithm takes a system parameters params, an identity ID_i, a message m_i and an individual signature σ as input the verifier computes $Q_i = H_1(ID_i)$ and $h_i = H_2(T_i, ID_i,m_i)$, then accepts if the following equation holds:

$$\hat{e}(U_i, P) = \hat{e}(P_0,Q_i)\ \hat{e}(T_i, h_i).$$

Aggregation: This algorithm is run by an aggregate signature generator and allows the generator to compress multiple single signatures into an aggregate signature. Each sensor node with the identity ID_i provides a signature $\sigma_i = (U_i, T_i, ID_i, m_i)$ on a message m_iє {0, 1}of its collection, i = 1, · · · , n. the aggregator computes

$$r = H(\hat{e}(U1, PK_{ctr}), \cdots, \hat{e}(Un, PK_{ctr})),$$
$$U = r.\sum_{i=1}^{n} U_i$$

σ = (U, T_1, · · · ,T_n) is the aggregate signature with identities {ID_1, ID_2, . . . , ID_n} on messages {m_1,m_2, . . ,m_n} respectively.

VerifyAgg: To verify the validity of an aggregate signature ∑Agg = (U, V, W) for message-identity pairs {(m1, ID1),. . . ,(mn,IDn)}, the verifier computes agg
$Q_i = H_1\ (ID_i)$, hi=H_2 (Ti,mi, IDi), for i=1,.. ,n, and checks.

$$\hat{e}(U,P) = \prod_{i=1}^{n} \hat{e}(p_0, Q_i)^{r'}\hat{e}(T_{i,}h_i)^{r'}$$

Where

$$r' = H(\hat{e}(P_0, Q_1)^y.\hat{e}(T_1, h_1)^y..\hat{e}(P_0, Q_n)^y.\hat{e}(T_n, h_n)^y).$$

V. DESIGN AND IMPLEMENTATION

A. Design

In this model implementation is done by combining the highlights of aggregate signature scheme and ID-based cryptography, given an ID-based Data Integrity scheme (IBDIS) using cluster method for WSNs. This model mainly focuses on designing the aggregate signature scheme which can verify each and every individual signature of sensor nodes to resist attacks. The sensor nodes are grouped into clusters so that network lifetime of nodes is increased and simultaneously reduces bandwidth and storage cost.

The new aggregate signature scheme results in a short aggregate signature that is valid if and only if every individual signature involved in the aggregation is valid.

In order to provide the end-to-end confidentiality, Elliptic curve cryptography (ECC) is used. ECC is a public key cryptography approach based on the algebraic structure of elliptic curves over finite fields where the elliptic curves are defined over prime fields Fp, where p is a large prime number. For current cryptographic purposes, an elliptic curve is a plane curve over a finite field (rather than the real numbers) which consists of the points satisfying the equation.

$$y^2 = x^3 + ax + b \bmod p$$

Along with a distinguished point at infinity denoted ∞.

Where a, b ∈Fp such that $4a3 + 27b^2 \neq 0 \pmod{p}$.

For dealing the security risks, secure data aggregation scheme must provide the following security requirements.

Confidentiality: ensures that the plaintext can only be accessible by the authorized user. All data captured must be encrypted and prevent intermediate node to access to the plaintext.

Integrity: ensures that the received data has not been altered, either maliciously or accidentally, during transmission.

Authenticity: ensures that the received data is sent by the claimed sender.

Availability: ensures the survivability of the network despite denial of service attacks.

Freshness: ensures that each message is recent and no old messages replayed by an attacker.

Efficiency: a security protocol must be efficient in term of computation and communication overhead in order to preserve energy and prolong the network life time.

ECC algorithm is probabilistic in nature and the security relies on the hardness of algorithm. However, when considering security against active adversaries, a verification of the data integrity is needed in order to ensure that all the data were ported successfully, each sensor of the network computes a tag using HMAC algorithm on cipher text, and every intermediate node then verify the data integrity, execute the homomorphic operation if the verification hold; otherwise, the packet will be dropped, with this process the data integrity of all packet is maintained and all senders are authenticated.

B. Implementation

The Implemented model of the proposed system consists of three major components known as data center, aggregator and sensor nodes which are in large numbers. 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.
The complete block diagram of the implementation is shown in the following:

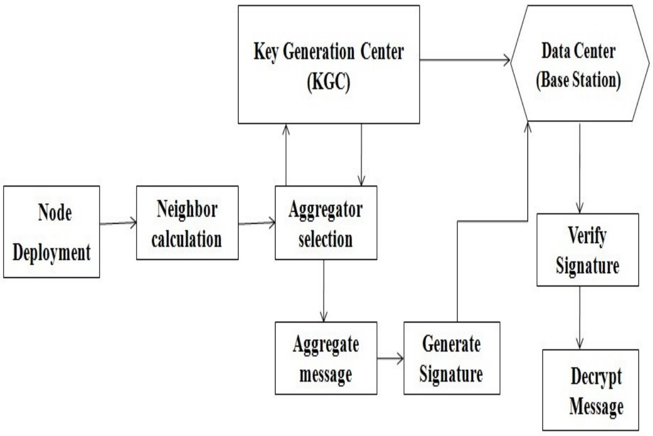

Figure 2. Block Diagram of the System

This paper proposed an improvement for ID-Based Aggregate Signature Scheme by providing an initial approximation of trustworthiness of sensor nodes which makes the data not only coalition free, but also more secure and efficient. The implementation is described below:

- ✓ Sensor nodes, if they want to transmit messages, first they want to register with key server, for this case we make use of key generator to generate unique keys like public and private keys using Elliptic Curve Cryptography (ECC). The same procedure repeats for cluster head and even for base station.
- ✓ Sensors in order to send the messages to the cluster head they make use of public key of base station and its own private key to generate a shared key for encrypting the message.
- ✓ This encrypted message is sent to the cluster head, where cluster head will aggregate the message and produces the aggregate data and signature for it and sends to the base station.
- ✓ In base station in order to decrypt the message sent form the cluster head it make use of public key of the sensor and using its own private key it generates a shared key which will decrypt the sent messages.
- ✓ If the decrypted message is same as the encrypted messages then we can say that the matching is successful.

VI. SIMULATION RESULTS

The code is developed and simulated in the Network simulation (NS) tool. The sensor nodes are grouped into clusters and appropriate cluster heads are selected to reduce the energy consumption and increase the network lifetime.

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 centre has a strong computing power and storage space. So, our scheme's objectives are trying to reduce the communication cost and computation cost of aggregator and sensor node without loss of generality.

In the following, we evaluate our scheme in terms of

- ✓ Average Energy Consumption
- ✓ Computation Overhead
- ✓ Communication Overhead

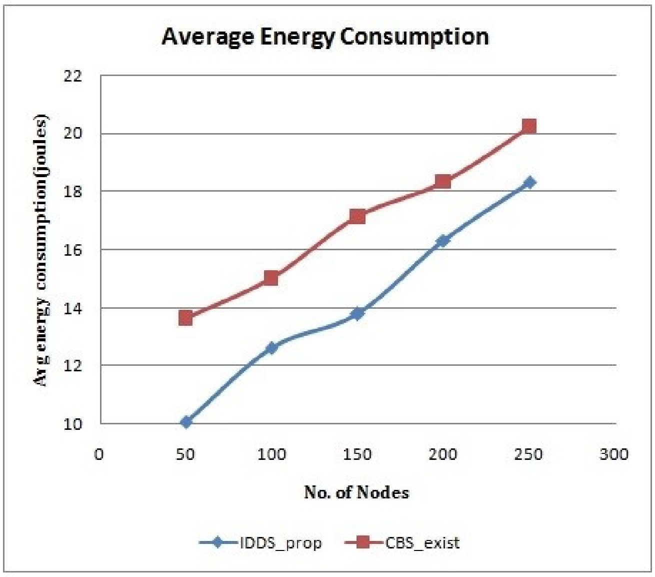

Figure 3: Average Energy Consumption

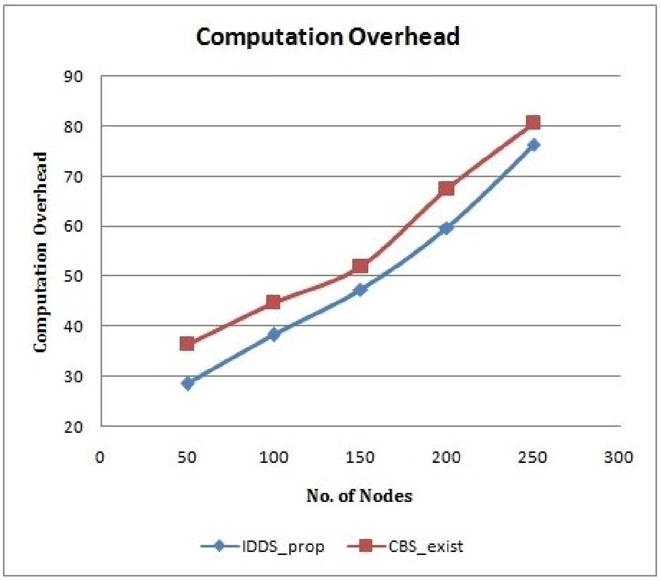

Figure 4: Computation Overhead

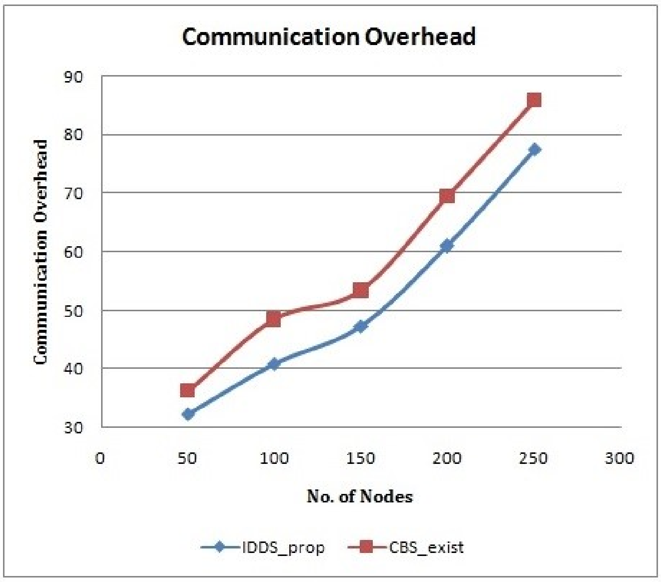

Figure 5: Communication Overhead

VII. PERFORMANCE EVALUATION

The performance comparison is obtained by comparing our ID-based data Integrity scheme (IDDS) with the Certificate Based scheme (CBS) as following.

Energy Consumption: The energy consumed is decreased when compared to the previous scheme from the (figure 3) graph, because of the clustering of nodes vast amount of load on nodes is reduced.

Computation Overhead: Computation Overhead is obtained by calculating the number of routing packets to number of packets sent. The comparison graph (figure 4) shows that the computation overhead is improved and reduced by a fare margin.

Communication Cost: The comparison of communication cost (figure 5) indicates that the aggregate scheme can reduce transmission in one data aggregation. It is performed by calculating the number of routing packets to number of received packets.

VIII. CONCLUSION

This paper raised data transmission and security issues and proposed an ID-based data Integrity scheme using cluster method for WSNs, which protects data integrity and resist coalition attacks. This scheme consists of cluster heads which can compress many signatures generated by sensor nodes into a single one. The experimental results show that our IDDS scheme can not only reduce communication overhead and computation overhead but also can reduce Energy consumption. It is also proved that this scheme can stand up against any coalition attacks, as aggregate signature is valid if and only if every individual signature involved in the aggregation is valid. In future work, the aim is to improve the performance of the aggregation scheme by using a novel cluster-head choice technique to extend network lifetime and reliability.

IX. REFERENCES

[1]. J. Yick, B. Mukherjee and D. Ghosal, "Wireless sensor network survey,"Computer Networks, vol. 52, pp. 2292-2330, 2008.

[2]. 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.

[3]. F. Zhang, L. Shen and G. Wu, "Notes on the security of certificateless aggregate signature schemes," Information Sciences, vol. 287, pp. 32-37, 2014.

[4]. A. Shamir, "Identity-based cryptosystems and signature schemes," in Proc .CRYPTO 1984, Santa Barbara, California, USA, August 19-22,Springer-Verlag, Berlin LNCS, vol. 196, pp. 47-53, 1984.

[5]. S. Al-Riyami, K. Paterson, Certificateless public key cryptography, in: ASIACRYPT 2003, LNCS, vol. 2894, 2003, pp. 452–473.

[6]. L. Zhang, B. Qin, Q. Wu and F. Zhang, "Efficient many-to-one authentication with certificateless aggregate signatures," Computer Networks, vol.

[7]. 54, no. 14, pp. 2482-2491, 2010.

[8]. H. Xiong, Z. Guan, Z. Chen and F. Li, "An efficient certificateless aggregate signature with constant pairing computations," Information Sciences, vol. 219, no. 10, pp. 225-235, 2013.

[9]. F. Zhang, L. Shen and G. Wu, "Notes on the security of certificateless aggregate signature schemes," Information Sciences, vol. 287, pp. 32-37,2014.