International Journal on Emerging Technologies **10**(1): 54-58(2019)

ISSN No. (Print) : 0975-8364
ISSN No. (Online) : 2249-3255

Secure and Efficient Data Communication for Hierarchal Cluster using Identity based Signatures

Sangamesh Kalyane[1] and Nagaraj B. Patil[2]
[1]Research scholar, Department of Computer Science and Engineering, BKIT, Bhalki (Karnataka), INDIA
[2]Department of Computer Science and Engineering, Govt. Engineering College, Raichur (Karnataka), INDIA

(Corresponding author: Sangamesh Kalyane)
(Received 09 February 2019, Revised 02 April 2019 Accepted 12 April 2019)
(Published by Research Trend, Website: www.researchtrend.net)

ABSTRACT: In resource constrain WSN; affording security is a challenging issue. Applications of WSN have been broadly applied in environment monitoring, military and object tracking. Secure communication between sensors is strongly needed to avoid malicious activity. Node can become compromise by attacks which lead to dropping packets and data tampering, thus sensor nodes have to be secure to prevent from attackers hacking on privacy and misuse of private data. In this paper we proposed an improved diffie-hellman identity based group signature (IBGS) scheme with Base station (BS) as a verifier for WSN. Our scheme provides secure data integrity and also reduces network overhead by using small constant pairing number. Efficiency of the proposed scheme is simulated on network simulator and parameters are evaluated in terms of delay, packet delivery ratio and network overhead.

Keywords: Cluster based WSN, ID-based signature, Secure communication, WSN

I. INTRODUCTION

Wireless sensor network comprise of nodes deployed random or structured depending on scenarios. Nodes are capable of sensing and computing data from their environment, and send the data to one or multiple collection point known as sink or base station [1, 15]. Sensor node suffers from limited battery, resource constrain, storage and processing. WSN are subjected to types of attacks such as eavesdrop, flood attack, Sybil attack so on. Once the node becomes compromise by adversaries, information becomes non secretive and entire network will be affected [2, 16, 18]. Securing large scale sensor network from attackers is a major issue. Therefore security mechanism is required to provide integrity, confidentiality and authentication. For large scale sensor network, clustered architecture provides more benefits with local collaboration and routing [3, 17]. In cluster hierarchical architecture are often used. Cluster head (CH) is responsible to collect and aggregate data collected from cluster members (CM) and forward it to base station (BS). For energy efficient cluster method LEACH protocol was proposed by Heinzelman *et al* [3], to reduce the energy consumption of the CH by rotating CH randomly and to balance the load among the CH's. Adding security to dynamic clusters is a challenging. Cryptography based digital signature using asymmetric key management is most critical security services [4]. In Identity-based signature (IBS) scheme, factor integers derives the public key identity from identity based cryptography. Shamir's [5] ID based cryptography eliminates public key certificates and eases key management problem.ID-based signature system verification process involves pairing of signatures and public parameter and signer identity to generate certificate less key verification. In this paper by combining the highlights of digital signature and ID based signature we proposed an improved ID based group signature (IBGS) scheme for hierarchal cluster architecture. IBGS not only provides data integrity also reduce storage cost and low network overhead. The main contributions of this paper are.

-System model have three components: 1) Base station (BS), 2) Cluster head (CH), and 3) number of sensor nodes called Cluster members (CM). CH is responsible to generate signatures and send it to base station with message generated by cluster members. Attackers are introduced into network and our scheme should resist attacks.

-IBGS composed of four phase 1) setup phase, 2) Key Generation phase, 3) Signing phase and 4) Verification phase.

-Our scheme can ensure data integrity and reduce communication overhead.

-Analysis of comparative performance is evaluated. Simulation results shows IBAS scheme is efficient in terms of the computational delay, communication cost and storage overhead.

The rest of this paper is organized as follows. In Section II describe the related work carried out. Section III describes the propose system model and IBGS scheme. In section IV the performance analysis and relative simulation are conducted. Finally we draw the conclusion on the proposed scheme in section V.

II. RELATED WORKS

Recently security and privacy issues have been studied and analysed in WSN, Enhanced Identity-based cryptography technique proposed by Sumalatha [8] for group key management scheme towards multicasting group keys using PKI in distributed environments.

This scheme is suitable for real time applications and provides security in distributed manner. Jathe [9]

proposed hybrid cryptography with RSA approach, this approach mainly concentrates on encrypting and decrypting data using private and public keys. This approach has an activation node monitors the path in which data is sent from source to destination with the signatures. Zamani and Zubair [10] propose a cryptographic keying algorithm, the plan of this technique is providing secure methods for handling sensitive data. Key supervision contains keys for generation which are used for encryption and decryption, distribution and maintenance which involves sharing of keys among nodes in network and to store those keys in key pools. Maintenance of generated keys involves in updating of keys at regular time intervals, etc. Lu *et al* [11] proposed a secure routing protocol using ID-based digital signature for clustered WSNs. In the proposed protocol, cluster heads are selected based on the RSS signal strength. Cluster head communicate directly to base station. In the proposed secure routing protocol, node id is used to generate public key and corresponding to private keys without any auxiliary for transmission of data. The proposed secure protocol is more efficient in communication but, suffers from high-computation paring cost. Sharma *et al.* [12] have proposed heterogeneous clustering for WSNs. In this scheme, to conserve energy the concept of sun nodes with static clustering scheme has been introduced. Energy-efficient clustering routing protocols [13] have better performance for WSNs. In these protocols, the senor nodes are divided into number of small groups as clusters, the CH performs aggregation techniques and then forwards that data to the BS.

A. Preliminaries

Bilinear Pairing. For two cyclic groups G and Kwhose orders are denoted by prime p. For G and $|G| = |K|$ let the generator be. Map of $\hat{e} : G \times G \rightarrow K$ for a bilinear paring to be satisfied for the following properties

1. Bilinearity: For $Q_1, Q_2 \in G$ and $\tau, \upsilon \in Z_p^*$, $\hat{e}(\tau Q_1, \upsilon Q_2) = \hat{e}(Q_1, Q_2)^{\tau\upsilon}$.
2. Nondegeneracy : $\hat{e}(P, P) \neq 1_K$, where 1_K is K identity
3. Computation: For all $P_1, P_2 \in G$ there exist an efficient computing algorithm $\hat{e}(P_1, P_2)$.

Bilinear map $\hat{e}$ is derived from weil [6] or Tate pairing [7] on ECC curves. Calculating each operation on $\hat{e}(P,P)$ is a pairing operation. This operation has more complex computation in cryptographic schemes. By reducing pairing operations, efficient the scheme will be in terms of less overhead.

Definition:

Computational Diffie–Hellman Problem (CDH) is given as:

Elements for computation $P, \tau P, \upsilon P \in G$ to compute $\tau\upsilon P \in G$ chosen randomly $\tau, \upsilon \in Z_p^*$

Let A be attacker. $A's$ probability to solve the CDH is given as

$Adv_A^{CDH} = P_r[A(P, \tau P, \upsilon P) = \tau\upsilon P : \tau, \upsilon \in Z_p^*]$

Where τ *and* υ are uniform random scalars from Z_p^* and choice of $P \in G$ and the coin tosses of A.

III. SYSTEM MODEL

Network consists of WSN nodes which are hierarchically represented in set SN1,SN2...SNn, base station, cluster head and cluster members in the network. The cluster head is responsible to collect data from cluster members and aggregate the data and forward the aggregated data to base station. Cluster head are equipped with more bandwidth and transmitting power to increase the efficiency in transmitting data within its communication range. The architecture model is as shown in figure

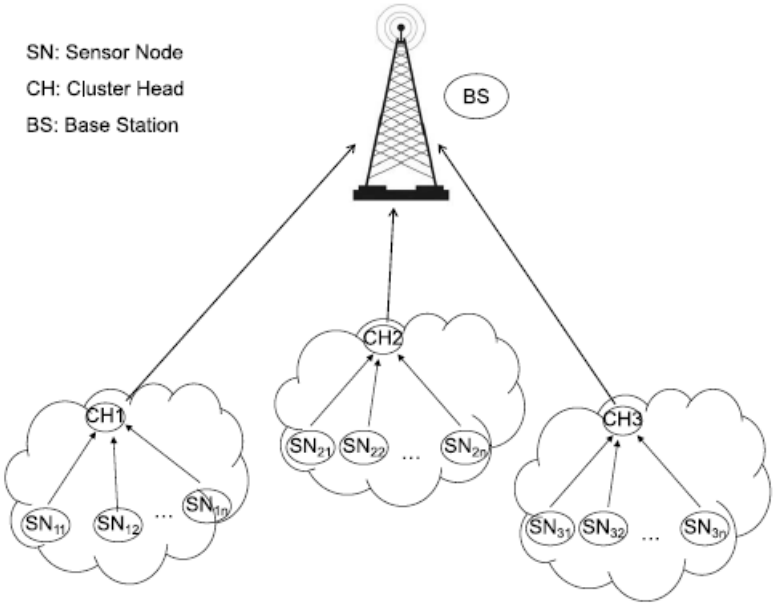

Fig. 1. Network Model.

Network model consist of three parts 1) Base station (BS), 2) Cluster head (CH) and 3) Sensor nodes.

(i) Base station has infinite computation resource and energy, to process data collected from sensor nodes.

(ii) BS receives public-secrete pairing key $(PK_{center}, SK_{center})$ and publishes public key PK_{center}

(iii) CH collects data from sensor nodes and monitors the group by authenticating nodes through its signature. CH can get BS's public key through secure channel, aggregates signatures signed by sensors (cluster members) and forwards the aggregate signatures to BS.

(iv) Public key generator generates each sensor node ID and private keys S_{ID_i}, after nodes deployment it is embedded with $(param, S_{ID_i})$. Sensor node ID_i uses its private key S_{ID_i} to sign messages collecting from sensing area. Each sensor belonging to particular cluster sends message and its signature to CH and finally sent to BS.

A. Security Model for IBGS

An IBGS scheme consists of following algorithms phases: 1) setup phase, 2) Key Generation phase, 3) Signing phase 4) Verification phase.

Setup phase: Setup algorithm is run by the challenger B to obtain master key msk and system parameters $param$ with l as a security parameter. B randomly generates public-secrete pairing key $(PK_{center}, SK_{center})$ of BS , then B gives $param$ and PK_{center} to A

Queries: Attacker A may access oracles adaptively as follows:

- Key Generation Request: On receiving request, challenger B replies by running Key Generation algorithm to generate private key S_{ID} of the user and returns S_{ID} to A.
- Signing Request: On receiving signing request, challenger B replies by executing sign algorithm to generate signature σ and returns σ to A.
- Verification Request: On verification request, B responds whether is it a valid signature by running verification algorithm.

Attacker forgery: Attacker Aoutputs its forgery

$$(\{ID_j, \sigma_j, j = 1 \ldots . n\}, \sigma^*)$$

A wins game if attacker forges a valid signature by using set of individual signatures.

B. Proposed IBGS scheme algorithm

Setup phase: Assume two cyclic group $G_1 and\ G_2$ of prime order p with security parameter l. Let $\hat{e}: G_1 \times G_1 \rightarrow G_2$ is a bilinear pairing and P be arbitrary generator of G_1. Hash function $H_1, H_2, and\ H$. $H_1, H_2: \{0,1\}^* \rightarrow G_1$, and $H: G_2 \rightarrow Z_p^*$.

PKG chooses $x, y \in Z_p^*$ randomly to compute $P_0 = xP, PK_{center} = y$ then the parameter $param = \{\hat{e}, G_1, G_2, P, p, H_1, H_2, H, P_0\}$ master key$msk = x$. The BS public-secrete verification key pair $(PK_{center} = yP, SK_{center} = y)$.

C. Key Generation Phase

By sensor node identity ID_i computes $Q_i = H_1(ID_i)$ and its correspondence private key is given as $S_i = xQ_i$

D. Signing Phase

For message signingm_i, sensor node ID_i with its private key S_i generates $t_i \in Z_p^*$ and computes

$$T_i = t_i P$$
$$h_i = H_2(T_i, ID_i, m_i)$$
$$U_i = S_i + t_i h_i$$

The signature is $\sigma = (U_i, T_i, ID_i, m_i)$

E. Verification Phase

The verifier computes $Q_i = H_1(ID_i)$ and $h_i = H_2(T_i, ID_i, m_i)$ with given $(\sigma, param)$ then accepts if the following equation holds good:

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

IV. PERFORMANCE EVALUATION

The proposed IBGS scheme is simulated in event driven simulation tool and performance evaluation is evaluated in terms of computation delay and transmission overhead. We conduct iterations in simulations using ns-2. The configuration of the simulation is shown in the below table 1.

Table 1: Simulation Parameters.

Parameters	Values
Deployment Layout	Cluster
Deployment Area	800 × 800
No of nodes	80
Bandwidth	2Mb
Mobility Model	Random Mobility Model
Traffic Type	CBR
Transmission Range	250 mts
Attacker Nodes	2-10
Initial Energy	30 Joules
Propagation Model	Two ray ground
MAC Type	802_11

The simulation has been carried on different scenarios and network parameter has been evaluated. CH is elected based on high residual energy and the dynamic CH is formed on the rotation basis. CH is responsible to authenticate sensor nodes and forward the information to BS.

A. Computation Delay

Delay is most important issue in WSN which can affect valuable data. Comparison of proposed scheme and other verification scheme in terms of time cost required by cryptographic operations in signing and verification is compared. Let T_{par} be time to perform one pairing operation. T_h indicates time to calculate hash operation and T_{mul} represents time to execute one point multiplication on elliptic curve. Since these operation dominates speed of signature generation and signature verification. We compare proposed IBGS scheme with Shiang-Feng batch verification scheme respectively in terms of computational delay and overhead. Firstly we observe time required to sign the message, in shiang-feng considers timestamp T_i before signing messages, this scheme uses more time in signing keys and authenticating nodes. The delay and message verifying signature graphs are shown in Fig. 2 and 3.

B. Transmission Overhead

The proposed IBGS scheme avoids malicious activity in the network and increases network rate in presence of attackers. Proposed system can capture hidden keys from the nodes before distribution and updates keys to detect compromise node. Transmission overhead is calculated based computation of signature, pseudo identity and timestamp. If the number of messages increases, overhead of the network increases linearly. The transmission over head of proposed IBGS scheme is less compared to feng scheme graph is shown in Fig. 4.

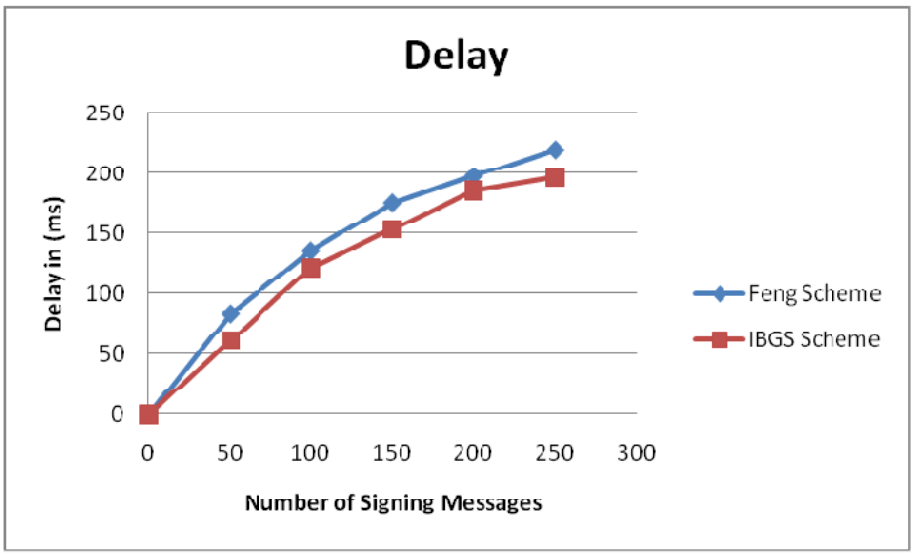

Fig. 2. Delay graph.

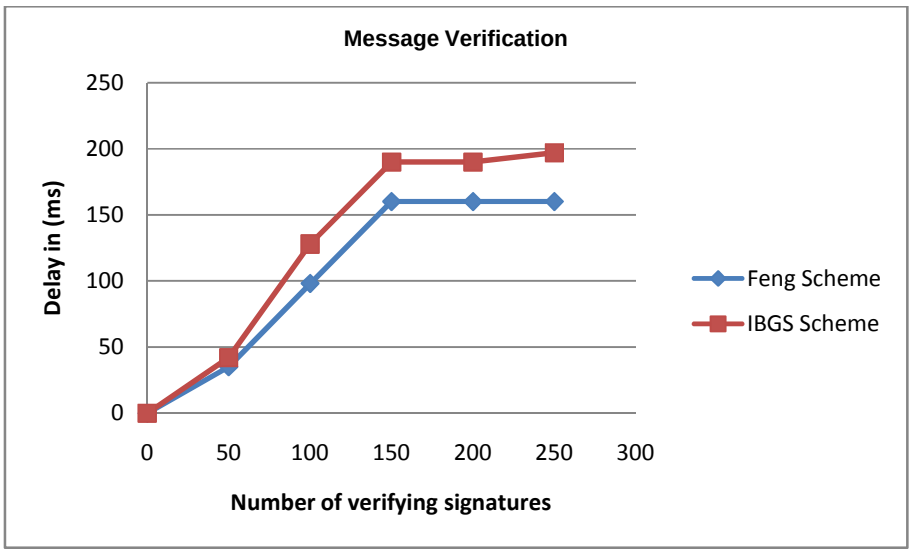

Fig. 3. Verifying signature graph.

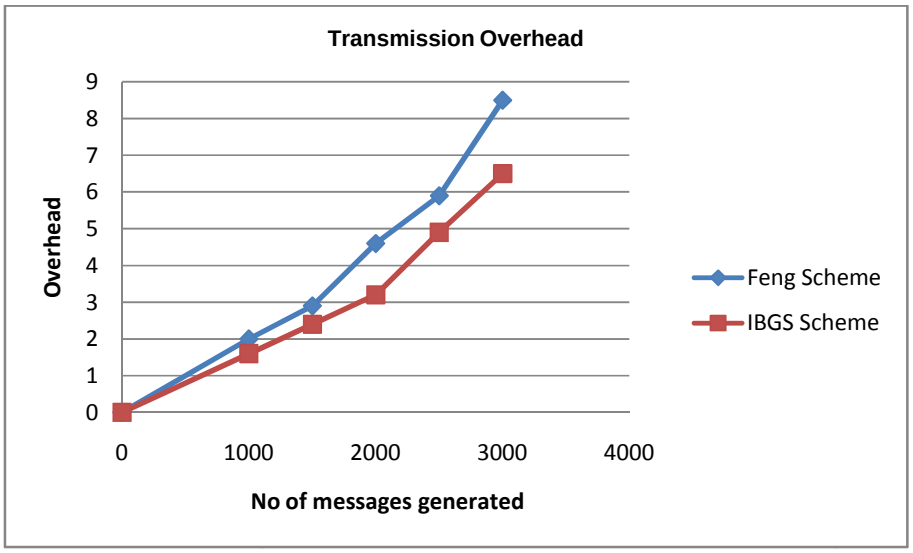

Fig. 4. Network Overhead.

V. CONCLUSION

Sensor nodes are resource constrained and has limited battery power, high computation increases network overhead. To reduce network overhead and to secure the network an efficient identity based cryptography schemes has to be developed. In this paper we present, an improved diffie-hellman identity based group signature (IBGS) scheme with Base station (BS) as a verifier for WSN. Our scheme provides secure data integrity and also reduces network overhead by using small constant pairing number. Simulation analysis shows the efficiency in verifying signatures. Simulation results shows the efficiency of IBVS scheme for average message delay and less communication overhead compared to existing scheme.

Conflict of interest: No

Acknowledgement: We would like to thank Visvesvaraya Technological University, Belagavi for providing the required facility to complete the project within stipulated time.

REFERENCES

[1]. T. Hara, V.I. Zadorazhny, and E. Buchmann (2010). "Wireless Sensor Network Technologies for the Information Explosion Era, Studies in Computational Intelligence", *Springer-Verlag*, 278.

[2]. Y. Zhu, Y. Fang, and Y. Zhng (2008). "Securing wireless sensor networks: a survey," *IEEE Communications Surveys and Tutorials*, **10**(3): 6–28.

[3]. A.A. Abbasi and M. Younis (2007). "A Survey on Clustering Algorithms for Wireless Sensor Networks," *Computer Comm*., **30**(14/15): 2826-2841.

[4]. W. Diffie and M. Hellman, (1976). "New Directions in Cryptography," *IEEE Trans. Information Theory*, **IT-22**(6): 644-654.

[5]. Shamir (1984). "Identity-based cryptosystems and signature schemes," in *Proc. CRYPTO*, 196, Santa-Barbara, CA, USA, 47–53.

[6]. D. Boneh and M. Franklin (2003). "Identity-based encryption from the Weil pairing," *SIAM J. Comput.*, **32**(3): 586–615.

[7]. A. Miyaaji, M. Nakabayashi, and S. Takano (2001). "New explicit conditions of elliptic curve traces for FR-reduction," *IEICE Trans. Fundam.*, **E84-A**(5): 1234–1243.

[8]. Sumalatha, P. & Sathyanarayan, B. (2015). Enhanced Identity Based Cryptography for Efficient Group Key Management in WSN. *International Journal of Application or Innovation in Engineering & Management* (*(IJAIEM),* **4**(6): 2319–4847.

[9]. Jathea, S. & Dhamdhere, V. (2015). Hybrid Cryptography for Secure Superior Malicious Behavior Detection and Prevention System for MANET's. *International Journal of Innovative Research in Science, Engineering and Technology*, **4**(7): 5673–5680.

[10]. Zamani, A. & Zubair, S. (2014). Key Management Scheme in Mobile Ad Hoc Networks. *International Journal of Emerging Research in Management & Technology*, **3**(4): 157–165.

[11]. Huang Lu, Jie Lee, and Hisao Kameda "A Secure Routing Protocol for Cluster-based Wireless Sensor Networks Using ID-based Digital Signature" *IEEE Global Communication Conference*, 1-5.

[12]. A. Sharma, K. Goel, A. Bindal, and A.K. Bindal (2016). "Static energy efficient clustering scheme for heterogeneous wireless sensor networks (seecs)", in *Proc. 9th Int. Conf. Contemp. Comput., (IC3)*, 1-6.

[13]. W. Zhang, G-Han, and L. Zhang (2017). ''E2hrc: An energy-efficient heterogeneous ring clustering routing protocol for wireless sensor networks,'' *IEEE Access*, **5**(1): 1702-1713.

[14]. Sajyth R.B. and Sujatha, G. (2018), "Design of Data Confidential and Reliable Bee Clustering Routing Protocol in MANET", *2018 International Conference on Computer Communication and Informatics (ICCCI - 2018)*, Coimbatore, INDIA.

[15]. Prashant Sangulagi, Shilpa Patne and A. V. Sutagundar (2015). "A New Approach for Energy Efficient Routing and Aggregation in Wireless Sensor Network", *International Journal on Emerging Technologies, (Special Issue on NCRIET-2015)* **6**(2): 320-326.

[16]. Amit Kumar Singh (2015). "Identity-Based Key Distribution for Wireless Sensor Networks using Cryptographic Techniques", *International Journal on Emerging Technologies,* **6**(1): 69-72.

[17]. Prachi Pathak and Mohd. Amjad Quaz (2017). "Issues, Challenges and Solution for Security in Wireless Sensor Networks: A Review", *International Journal of Electrical, Electronics and Computer Engineering,* **6**(1): 04-11.

[18]. Motwani, Anand and Vimal, Dhote, (2016). "Optimized AODV Routing for Effective Attack Security in Wireless Sensor Networks", *International Journal of Electrical, Electronics and Computer Engineering,* **5**(1): 33-40.

How to cite this article: Kalyane, Sangamesh and Patil, Nagaraj B. (2019). Secure and Efficient Data Communication for Hierarchal Cluster using Identity based Signatures. *International Journal on Emerging Technologies,* **10**(1): 54-58.