ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 4, April 2018

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

[1] Y.Kalyani, [2] N.Yedukondalu, [3] Sk.Alma, [4]T.Sujitha, [5] S.Sindhu Priya
[2] Assistant Professor, Dept of CSE
[1][2][3][4] Narayana Engineering College, Gudur

Abstract: Affording secure and economical massive knowledge aggregation ways is incredibly enticing within the field of wireless device networks (WSNs) analysis. In real settings, the WSNs are broadly speaking applied, comparable to target pursuit and atmosphere remote watching. However, knowledge will be simply compromised by a colossal of attacks, comparable to knowledge interception and knowledge meddling, etc. during this paper, we have a tendency to principally concentrate on knowledge integrity protection, provide Associate in Nursing identity-based mixture signature (IBAS) theme with a chosen booster for WSNs According to the advantage of mixture signatures,our theme not solely will keep knowledge integrity, however can also scale back information measure and storage value for WSNs. what is more, the protection of our IBAS theme is strictly bestowed supported the procedure Diffie–Hellman assumption in random oracle model.

INTRODUCTION

IN massive knowledge era, digital universe grows in beautiful speed that is created by rising new services, appreciate social network, cloud computing, and net of things. massive knowledge area unit gathered by ubiquitous wireless detector networks (WSNs), aerial sensory technologies, code logs, information-sensing mobile devices, microphones, cameras, etc. and also the WSN is one in every of the extremely anticipated key contributors of the large knowledge within the future networks. WSNs, with an outsized variety of low-cost, small, and extremely strained detector nodes sense the physical world, has terribly broad application prospects each in military andcivilian usage, as well as military target pursuit and police work, animal habitats watching, medical specialty health watching, and significant facilities pursuit. It will Manuscript received January twenty eight, 2016; revised March sixteen, 2016; accepted April eight, 2016. Date of publication April twenty one, 2016; date of current version April twenty eight 2017. This work was supported partly by the National technology analysis and Development Program (863 Program) beneath Grant 2015AA016007, and partly by the National Nature Science Foundation of China beneath Grant U1405255, Grant 61170298, Grant 61502237, and Grant 61572198. L. Shen is with the varsity of applied science and Technology, Xidian University, Xi'an 710071, China, and conjointly with the varsity of applied science and Technology, city traditional University, city 210023, China (e-mail: shenlimin@njnu.edu.cn). J. Ma and M. Miao area unit with the varsity of applied science and Technology, Xidian University, Xi'an 710071, China. X. Liu is with the varsity of knowledge Systems, Singapore Management University, Singapore 188065. F. dynasty is with the Department of knowledge analysis, Zhengzhou informatics and Technology Institute, Zhengzhou 450001.

In 2003, Bonehet al. introduced associate degree combination signature theme, which might compress multiple signatures generated by completely different| completely different} users on different messages into one short combination signature. the combination signature's validity will be admire the validity of each signature that is employed to come up with the combination signature. that's to mention, the combination signature is validity if and on condition that every individual signer extremely signed its original message, severally. Hence, aggregation is helpful technique in reducing storage price and bandwidth, and may be a decisive building block in some settings, appreciate knowledge aggregation for WSNs, securing border entryway protocols and enormous scale electronic voting system, etc.

Unfortunately, most of the prevailing combination signature schemes cannot resist a sort of sensible and powerfulattacks — coalition attacks. Coalition attack will generate a sound combination signature by exploitation some invalid single signatures with the collusion of 2 or additional signers. If such associate degree attack is self-made, the corresponding combination signature can pass the validation whereas some single signatures wont to generate it area unit invalid. this implies that a sound combination signature might fail to prove the validity of each individual signature concerned within the aggregation. This reality clearly violates the protection goal for combination signature schemes. So, during this paper, we are going to primarily target planning the

All Rights Reserved © 2018 IJERCSE

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 4, April 2018

combination signature theme which might resist coalition attacks.

SYSTEM MODEL

Security needs in WSNs primarily area unit confidentiality, integrity, credibility, quantifiability and adaptability, etc. in a very knowledge aggregation theme for WSNs, it's vital that no knowledge falsify throughout transmissions. Thus we tend to primarily target the info integrity protection in our system. The most thought of our system model is to shield knowledge integrity whereas reducing information measure and storage price for WSNs. Our IBAS system consists of 3 components
:
1) Knowledge center;
2) Aggregator
3) Detector node.
1) Knowledge center features a sturdy computing power and space for storing. thus it will method all original massive knowledge collected by detector nodes belong to the info center, and may offer data} information to customers. At the start, each knowledge center (as the selected champion in our IBAS scheme) can receive its public-secret key try (PKcenter, SKcenter), and publish the general public key PKcenter.

2) Somebody may be a special detector node with an explicit ability to calculation and communication vary. It canto the info center. we tend to assume that the PKG generates the system parameters param, aggregator's personal key SID admire its symbol data ID, then embeds (param, SID) in somebody once it's deployed.

3)Detector node has restricted resources in terms of computation, memory, and battery power. we tend to assume that the PKG generates personal key SID for everydetector node IDi. once detector node ID is deployed, it's embedded with (param, SIDi). Each detector node IDican use its personal key SIDito sign messages aggregation from the physical world. In our system, every detector node belongs to at least one cluster, sends messages and its signatures to their somebody, and also the messages can finally be sent to knowledge center via somebody. sign messages aggregation from the physical world, will get the info center's public key PKcenter from public channel, will generate the combination signature from the individual signatures signed by detector nodes enclosed somebody itself, and may send the combination signature.

SECURITY PROOF

In this section, first, we tend to offer security proof of the higher than signature theme concerned in our IBAS theme in random oracle model, then prove the protection of the combination algorithmic program.

Theorem 1: Let H1 associate degreed H2 be random oracles and there exists an opposer A against our theme with advantage
Oonce running in time t, creating at the most dkeytimes KeyGeneration queries, ds times linguistic communication queries, and di times random oracle queries to Hi (1 = one, 2). Then, there exists associate degree algorithmic program B to resolve the CDH drawback with likelihood
≥1 d1and running in time t ≤t + (d1+d2+dkey+4ds)•τsca, where τsca denotes the time required for computing a scalar multiplication. Proof: Assume A will break the EUF-CMA security of the theme, then we are able to construct a CDH thinker
B UN agency is given a random instance (P, uP, vP) of the CDH drawback. Next, we are going to show that however B will use A to get the worth of uvPin G1.
At the start, B sets P0 = uPand generates system parameters param= , The hashfunctions H1 and H2 function random oracles controlled by B.
B chooses a random integer index λ ∈[1, d1], let the λth queryto H1 is on the target identity ID.
B responds to A's queries as follows. (These queries contain
Hi(i= 1, 2) queries, KeyGeneration queries and signingqueries. All pairs of query/answer area unit maintained in lists.)

PERFORMANCE ANALYSIS

In this section, we tend to assess the performance of our IBAS theme. we tend to offer the outline of some notations to be utilized in this section in Table I.

A. Comparison of Un-Aggregation and Aggregation Schemes
We offer the performance comparison of 2 versions of un-aggregation and aggregation schemes during this section, and un-agg and agg denote the un-aggregation and aggregation schemes, severally. we tend to 1st review the talents of every part in our theme. detector node has restricted resources in terms of computation, memory, and battery power, somebody features a sure ability to calculation and communication vary and it works as a

All Rights Reserved © 2018 IJERCSE

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 4, April 2018

special detector node, and knowledge center features a sturdy computing power and space for storing. So, our scheme's objectives try to scale back the communication price and storage price of somebody and detector node. while not loss of generality, we tend to assume the aggregator's identity is IDnin a cluster that has n detector nodes . The performance in terms of communication and computation price is shown as follows.

1) Communication Cost: The comparison of communication cost (Table II) indicates that the aggregate scheme can reduce (n −1)|G1| transmission in one data aggregation process, at the same time, can reduce (n −1)|G1| storage cost. Therefore, our theme is associate degree economical knowledge aggregation technique for the WSNs.

2) Computation Cost: Let Pairing,M1,M2, and Exp be the computation price of a pairing operation in G2, a scalar multiplication calculation in G1, a multiplication calculation in G2, associate degreed an mathematical operation operation in G2, severally. Notice that the verification equation.Efficiency Comparison In this section, we tend to offer the potency comparison of our CLAS theme with some existing pairing-based schemes (Table IV). Our IBAS theme and Xuet al.'s theme simply accomplish partial aggregation, then need linear variety of pairings, and ours is required additional pairings in aggregation verification method. aristocracy and Ramzan had constant variety of pairing operations throughout the aggregation verification, but, their theme has some security weaknesses that are reportable in. Selviet al. had a trivial weakness that is alike to the theme of and also the signature theme in is settled, that's to mention, the signature generated by a user on a message remains identical.

CONCLUSION

Due to the restricted resources of detector nodes in terms of computation, memory, and battery power, secure and energy save knowledge aggregation ways ought to be designed in WSNs to scale back the energy price of knowledge assortment, processing, and knowledge transmission. During this paper, we tend to gift associate degree IBAS theme for WSNs, which might compress several signatures generated by detector nodes into a brief one, i.e., it will scale back the communication and storage price. Moreover, we've got tried that our IBAS theme is secure in random oracle model supported the CDH assumption, and that we even have tried that our combination signature will resist coalition attacks, that's to mention the combination signature is valid if and on condition that each single signature utilized in the aggregation is valid. In our future work, we are going to target planning additional economical knowledge aggregation schemes.

REFERENCES

I. Paik, T. Tanaka, H. Ohashi, and W. Chen, "Big data infrastructure foractive situation awareness on social network services," in Proc. IEEE Int. Congr. Big Data (BigDataCongr.), Santa Clara, CA, USA, 2013,pp. 411–412.

[2] E. Hargittai, "Is bigger always better? Potential biases of big data derived from social network sites," Ann. Amer. Acad. Polit. Soc. Sci., vol. 659,no. 1, pp. 63–76, 2015.

[3] Z. Fu, X. Sun, Q. Liu, L. Zhou, and J. Shu, "Achieving efficient cloud search services: Multi-keyword ranked search over encrypted cloud data supporting parallel computing," IEICE Trans. Commun., vol. E98-B, no. 1, pp. 190–200, Jan. 2015.

(3) Z. Fu, X. Sun, Q. Liu, L. Zhou, and J. Shu, "Achieving efficient cloud search services: Multi-keyword ranked search over encrypted cloud data supporting parallel computing," IEICE Trans. Commun., vol. E98-B,no. 1, pp. 190–200, Jan. 2015.

All Rights Reserved © 2018 IJERCSE