International Journal of Engineering Research and Advanced Technology (IJERAT)

E-ISSN : 2454-6135

DOI: http://dx.doi.org/10.7324/IJERAT.2018.3200

Volume.4, Issue 3

March-2018

Data Integrity Protection for Wireless Sensor Network Using Key Establishment Scheme

R.Abirami[1], R.Manimegali[2], M.Vidhyadharshini[3], A.M.SenthilKumar[4], M.S.Vijaykumar[5] and S.Santhiya [5]

[1- 3] Dept. of CSE, HOD[4] and Assistant professor[5-6]

Tejaa Shakthi Inst. of Tech. for Women

Coimbatore, Tamil Nadu

India

ABSTRACT

Present secure and efficient big data aggregation methods are 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 disputed by a vast of attacks, such as data interruption. In this paper, we mainly focus on data integrity protection give a key establishment scheme with designed verifier for wireless sensor networks. According to the merits of aggregate signatures, our key establishment scheme not only can keep data integrity, and it can reduce bandwidth and storage cost for wireless sensor networks. Furthermore, the security of our key establishment scheme rigorously presented based on RSA algorithm.

Keywords: *Wireless sensor network, key establishment scheme, RSA algorithm, data integrity*

I. INTRODUCTION

In big data technology, digital universe grows in stunning speed which is produced by emerging new services, such asocial network, cloud computing and internet of things. Big data are gathered by wireless sensor networks from everywhere, software logs, information-sensing mobile devices, microphones, cameras, etc. And the wireless sensor network is one of the highly expected key contributors of the big data in the future networks.

Wireless sensor networks (WSNs), with a large number of cheap, small and highly constrained sensor nodes sense the physical world, has very broad application prospects both in military and civilian usage, including military target tracking and surveillance, animal habitats monitoring, biomedical health monitoring, critical facilities tracking. It can be used in some hazard environments, such as in nuclear power plants. Due to their makeable advantages, comprehensive attention has been devoted to WSNs. Data aggregation technique is used to reduce energy consumption for WSNs. However, the technique still has the inherent security

Problems, such as snoop on, reply attacks, data modifying etc. Hence, proposing a secure and efficient data aggregation method is very significant for WSNs.

Before system they only provide data protection between sensor nodes and aggregator. Aggregator itself is not secured and we concentrate secure aggregation when the single sensor nodes might be secured and might be sending false data to the aggregator. We have to protect data integrity between aggregator and base station.

In this paper, key establishment scheme is used for providing secure data transmission between aggregator and base station in WSNs. It is used to protect data integrity. The ABE (Attributed Based Encryption) is recent approach of public key encryption.

2. PRELIMINARIES

The following is some basic notions required in this paper, containing the computational RSA algorithm complexity assumption.

2.1 Assumptions

Let k be the security parameter. Let positive integer N be the product of two k-bit, distinct odd prime's p; q. Let e be a randomly chosen positive integer less than and relatively prime to _ (N) = (p □ 1) (q □ 1). Given (N; e) and a random y 2 Z_N, it is hard to compute x such that x^e _ y mod N.

In the Strong RSA assumption, the adversary is given (N; y) and succeeds by producing any integer pair (e; x) such that e > 1 and x^e= y mod N. The standard RSA version is much more restrictive on the adversary.

RSA assumption where N = pq is the product of two safe primes p = 2p0 + 1 and q = 2q0 + 1.

2.2 Bilinear Groups and the CDH Assumption

Let G and GT be groups of prime order p. A bilinear map is an e_cient mapping e : G _ G ! GTwhich is both: (bilinear) for all g 2 G and a; b Zp, e(ga; gb) = e(g; g)ab; and (non-degenerate) ifg generates G, then e(g; g) 6= 1.

3. SYSTEM MODEL AND SECURITY MODEL

A. System Model

Security in WSNs mainly are integrity, scalability, confidentiality, authenticity and flexibility. 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 KES system consists of three parts: datacenter, aggregator and sensor node (Fig.1).

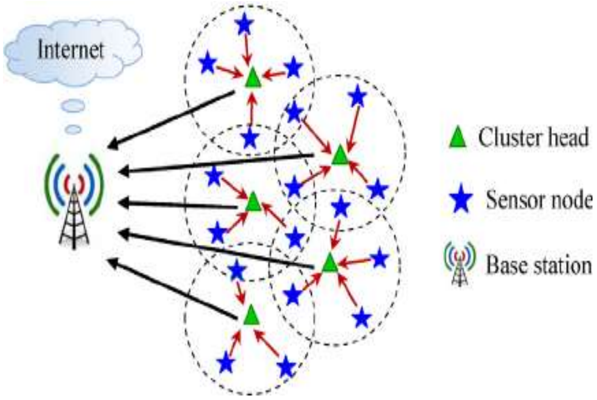

Figure 1. Cluster Based Network

Base station used by organizations for the r storage, processing, or distribution of data. Beginning of the process base station receive its public secret key from the key server.

Cluster head act as a aggregator, can provide the digital (aggregated) signature and send it to the base station with the message generated by the number of sensor nodes.

Sensor node has some resource including computation, memory and battery power. We consider that the key server generates the private key (PR), for each sensor node. Each sensor node use its private key for sending its data. In our model each sensor node belongs to one cluster head and send data and its key to their cluster and the data will be finally send to the base station through the cluster head.

B. Security Model of KES.

In an information technology that has provide the significant advances in crypto to in network protect the data integrity and confidentiality of data is astounding.

Before using key establishment schemes, there are a number of security elements that must be generated. Some of these elements must be kept private and some are made public. These elements include, key generation, validation and authentication of static and dynamic public-key key-pairs.

Key establishment can begin once the system parameters are generated and the public-keys distributed throughout the system. In Key establishment scheme two (or more) entities establish a shared secret key. In our key establishment scheme consist of three algorithm: key generation, verification and signature creation.

Obviously, the goal of intruder is the existential forgery of a signature. Most of the security model consider only the security of signature scheme and forgery of an aggregate

Signature, and do not consider the intruder's attack. When attacking the aggregation algorithm, the purpose of intruder is to forge a validate signature while using the some invalid signature.

KEY GENERATION

To generate key in between sensor node and aggregator using Random key generation algorithm. When a sensor node register with the key server, key server verifies the sensor node. After verification key server generates the private key for every registered sensor node. If the sensor node wants to send a message to the cluster head, it sends the message with its key provided by the key server.

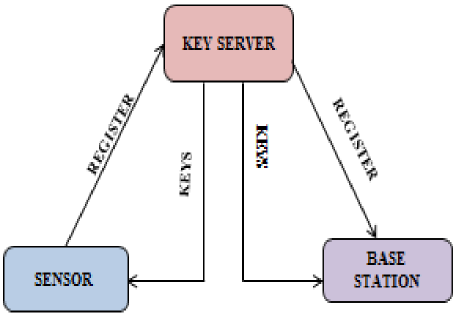

Figure (2) key generation

AGGREGATE VERIFICATION

Key server generate the key for aggregator and send that key to the base station. Aggregator request the public key from the base station, base station verify the aggregator with the corresponding aggregator key. If it is match it send public key to the aggregator. Aggregator generate the aggregate signature using sensor node's key and data center's public key.

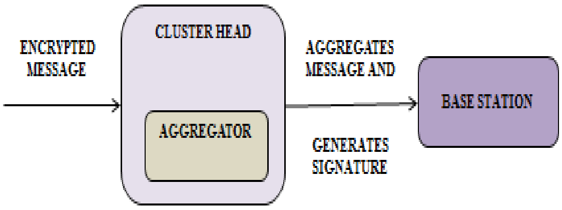

Figure3. Aggregate verification

GENERATE AGGREGATE SIGNATURE

It can sign messages collecting from the sensor node, and can get the data center's public key (PK) from public channel, using the sensor node's signature and data center's public it will Generate the aggregate signature. It can send the aggregate signature to data center.

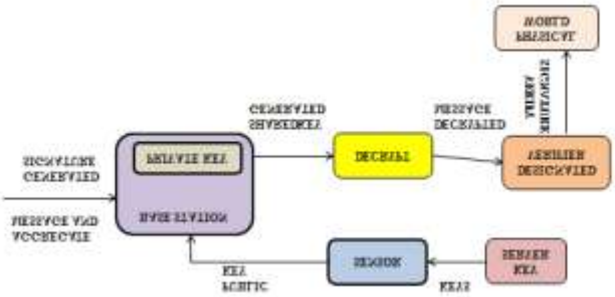

Figure 4. Generate aggregate signature.

DOI : 10.7324/IJERAT.2018.3200

IV. CONCLUSION

Sensor nodes has limited number of resources such as 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, we present Key Establishment 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.

Key establishment scheme provide secure data transfer between cluster head and base station and finally provide the secure data transmission between aggregator and base station. In our future work, we will focus on designing more efficient data aggregation schemes.

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]. 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,” IEEE Transactions on Dependable and Secure Computing, DOI10.1109/TDSC.2015.2406704, 2015.

[4]. X. Liu, B. Qin, R. Deng, Y. Li, “An Efficient Privacy-Preserving Outsourced Computation over Public Data,” IEEE Transactions on Services Computing, 2015, doi: 10.1109/TSC.2015.2511008.2327-4662 (c) 2016 IEEE. IEEE Internet of Things Journal IEEE INTERNET OF THINGS JOURNAL, VOL. NO: 8

[5] 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.

[6] M.M.E.A. Mahmoud and X. Shen, “Acloud-based scheme for protecting source-location privacy against hotspot-locating attack in wireless sensor networks,” IEEE Trans. Parallel Distrib.Syst., vol. 23, no. 10, pp. 1805- 1818, 2012.

[7] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci, “A survey on sensor networks,” IEEE Commun.Mag., vol. 40, no. 8, pp. 102-114, 2002. [15] J. Yick, B. Mukherjee and D. Ghosal, “Analysis of a prediction-based mobility adaptive tracking algorithm,” in Proc. Broadband Networks, 2nd International Conference on, IEEE, pp. 753-760, 2005

[8] A. Mainwaring, J. Polastre, R. Szewczyk, D. Culler and J. Anderson, “Wireless Sensor Networks for Habitat Monitoring,” in Proc. WSNA’02, Atlanta, Georgia, September, 2002. [17] X. Lin, R. Lu, X. Shen, Y. Nemoto and N. Kato, “Sage: a strong privacy- preserving scheme against global eavesdropping for ehealth systems,” Selected Areas in Communications, IEEE Journal on, vol. 27, no. 4, pp. 365-378, 2009.

[9] R. Lu, X. Lin and X. Shen, (2013) “SPOC: A secure and privacy- preserving opportunistic computing framework for mobile-healthcare emergency,” Parallel and Distributed Systems, IEEE Transactions on, vol. 24, no. 3, pp. 614-624, 2013.

[10] N. Xu, S. Rangwala, K.K. Chintalapudi, D. Ganesan, A. Broad, R. Govindan and D. Estrin, “A Wireless Sensor Network for Structural Monitoring,” in Proc. ACM Conference on Embedded Networked Sensor Systems, Baltimore, MD, November, 2004.

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

[12] N. Pereira, R. Gomes, B. Andersson, and E. Tovar, “Efficient Aggregate Computations in Large-Scale Dense WSN,” in Proc. 15th IEEE Real- Time and Embedded Technology and Applications Symposium, RTAS, pp. 317-326, 2009.

[13] 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.

[14] A. Boldyreva, C. Gentry, A. O’Neill and D.H. Yum, “Ordered multisig- natures and identity-based sequential aggregate signatures, with applica- tions to secure routing”, in Proc. ACM Conference on Computer and Communications Security (CCS’2007), pp. 276-285, 2007.

[15] J.H. Ahn, M. Green and S. Hohenberger, “Synchronized aggregate signatures: new definitions, constructions and applications”, in Proc. ACM Computer and Communications Security (CCS’2010), pp. 473-484, 2010.