Efficient Authentication for Tiered Internet of Things Networks

Chi-Yuan Chen(✉)

Department of Computer Science and Information Engineering,
National Ilan University, Yilan, Taiwan
chiyuan.chen@ieee.org

Abstract. Tiered Internet of Things (IoT) and Wireless Sensor Networks (WSN) are popular for efficient resource management. In order to reduce the communication overhead for unnecessary sensed data and avoid obtaining a false result, we propose to use aggregate signature to deal with the authentication problem.

Keywords: Authentication · Internet of Things · Wireless Sensor Network

1 Introduction

The flat structure of networks is usually difficult for resource management. Thus, a middle tier as shown in the Fig. 1 is introduced to ease the management difficulty. Moreover, the sensors are cheap and therefore resource-limited [1]. It is impossible for sensors to keep all the sensed data in their local memory. They need to offload their sensed data for saving memory space. However, not all the sensed data are required by the network owner. Therefore, the simple solution that sensors simply send back to the network owner all the sensed data for each time period is also impractical. A middle tier for temporarily storing the sensed data collected from sensors is becoming necessary.

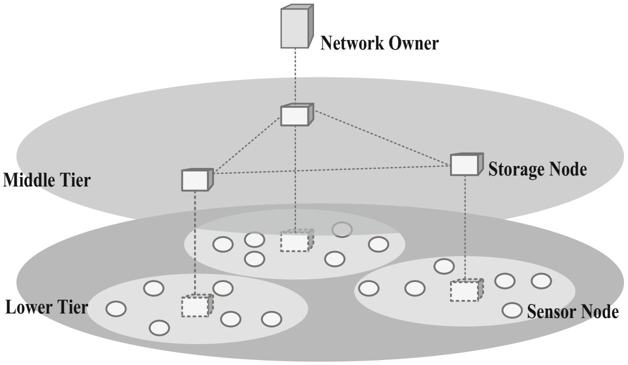

Fig. 1. Tiered Internet of Things (IoT) and Wireless Sensor Networks (WSN).

J.-H. Lee and S. Pack (Eds.): QShine 2016, LNICST 199, pp. 469–472, 2017.
DOI: 10.1007/978-3-319-60717-7_46

One can know from the above description that the only necessary requirement for the middle tier is the large storage space. Therefore, such a middle tier is also called *storage node*. The benefits of placing storage nodes in the network have been proven in [5].

The introduction of the storage node also redefines how the network owner acquires the sensed data. In particular, with the storage node, the network owner issues queries to the storage node to retrieve the part of sensed data it wants. The storage reports to the network owner the queried data. From the above statement, one can know that the benefit implied by the storage node is that the communication overhead for unnecessary sensed data between the storage node and network owner can be saved.

1.1 Security Risk

The placement of storage node also incurs new security challenge. Because sensors could be compromised, their compromises imply a large security risk, which means that all the sensed data and all the query results will be maliciously manipulated. In this paper, our concern is the authenticity of the query result. For example, in the presence of compromised sensors, the network owner issues a range query and then will obtain a false result.

A straightforward method to this problem is to attach a cryptographic hash to each individual sensed data. However, it also incurs a downside, which is that the communication overhead is also doubled. As the communication overhead is the main concern of the design of a network protocol, such method is unacceptable.

The existing methods conduct different approach to solve this problem. An encoding approach is used in [4]. Crosscheck is used in [6, 8]. Both these two also simply use conventional hash operation. In [3], a neighborhood chain, which is the hash of the consecutive sensed data, is used to guarantee the authenticity but still with the drawback of overwhelming communication burden. In [7], an aggregation tree is constructed before the network is deployed in order to aggregate the individual hashes. However, the method in [7] assumes too much information about the network topology.

1.2 Contribution

We propose to use aggregate signature [2] to deal with the authentication problem in tiered IoT and WSN. Though the use of aggregate signature involves complicated finite field arithmetic operations, the communication saving can be significant. Since the energy consumed by the communications is several orders larger than the energy consumed by the computation, we believe that our scheme can save a significant portion of energy and prolong the network lifetime.

2 Proposed Scheme

The aggregate signature involves a method for aggregating the traditional signatures. In particular, the use of traditional signature is to attach a signature to each individual data. However, in the bilinear setting, the aggregate signature is that each sensor also generates a signature for each individual data. However, to aggregate the signatures into one, each sensor performs multiplication operation on their generated signatures and the signatures sent from the neighboring sensors. Specifically, when a sensor has a tuple $\langle a, \sigma_a \rangle$, where a denotes the sensed data and σ_a is the corresponding signature, if it also receives a tuple $\langle b, \sigma_b \rangle$ from the neighboring, then it generally sends out the message $\langle a, b, \sigma_a \cdot \sigma_b \rangle$. The storage node in possession of the public keys and the claimed sensed data is therefore able to verify the legitimacy of the received signature $\sigma_a \cdot \sigma_b$ by the method in [2].

Despite the simplicity of the proposed scheme, it actually suggests the role change of which entity being needed to verify the legitimacy of the signature. In particular, in the traditional use of the signature, the storage node acts as only a relay that forwards the message from sensors to the network owner. However, in our proposed scheme, since the network owner no longer has the entire sensed data, it is unable to generate the corresponding hash so as to make sure whether the sensed data is authentic. It turns out that the storage node needs to check the legitimacy of received signatures regularly.

Thus, the whole picture of the proposed scheme is that, from ordinary sensor point of view, it generates and aggregates the signatures as mentioned above. From the storage node point of view, for each time period, it verifies the legitimacy of the received signature. Once at the end of the time period, the storage node does not report to the network owner that the signature is problematic, it implicitly implies that the received data is authentic. This gives an additional overhead on the storage node. However, as mentioned above, one can save more energy in our scheme than in existing schemes.

3 Performance Evaluation

The primary evaluation metric used in this paper is the communication overhead due to its important role in affecting the network lifetime. It is obvious that the communication overhead O^T_{comm} of the traditional method, which generates signatures for each individual data, can be computed as

$$O^T_{comm} = \sum\nolimits_{i=1}^{N} L(\ell_d n_d + \ell_s n_s), \tag{1}$$

where L is the average number of hops between sensors and storage node, N is the total number of sensors, ℓ_d is the number of bits for representing sensed data, n_d is the number of sensed data of each sensor, ℓ_s is the number of bits for representing signature, and n_s is the number of signature. The corresponding computation overhead O^T_{comp} is therefore:

$$O^T_{comp} = \ell_s O_{ts}, \tag{2}$$

where O_{ts} is the number of operations used in generating traditional signature.

On the other hand, the communication overhead O^A_{comm} of our proposed aggregate signature scheme, which generates and aggregates signatures, can be computed as

$$O^{A}_{comm} = \sum\nolimits_{i=1}^{N} L(\ell_d n_d + \ell_s), \tag{3}$$

where N is the total number of sensors, ℓ_d is the number of bits for representing sensed data, n_d is the number of sensed data of each sensor, and ℓ_s is the number of bits for representing signature. We particularly note that the n_s is equal to 1 in O^{A}_{comm} because all of the signatures is aggregated into one for each sensor. The corresponding computation overhead O^{A}_{comp} is therefore:

$$O^{A}_{comp} = \ell_s O_{as}, \tag{4}$$

where O_{as} is the number of operations used in generating aggregate signature. In essence, O_{as} can be approximately computed as

$$O_{as} = O_{ts} + O_m, \tag{5}$$

where O_m is the energy consumed by the multiplication operation.

4 Conclusion

In this paper, we utilize aggregate signature to reduce the authentication overhead in tiered IoT and WSN. We also provide a simple performance evaluation for our proposed approach. Though the use of aggregate signature involves a slightly computation overhead, the communication overhead can be reduced to prolong the network lifetime.

References

1. Chen, C.-Y., Chao, H.-C.: A survey of key distribution in wireless sensor networks. Secur. Commun. Netw. **7**(12), 2495–2508 (2014)
2. Boneh, D., Gentry, C., Lynn, B., Shacham, H.: Aggregate and veriably encrypted signatures from bilinear maps. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques (Eurocrypt) (2003)
3. Chen, F., Liu, A.X.: SafeQ: secure and efficient query processing in sensor networks. In: IEEE International Conference on Computer Communications (INFOCOM) (2010)
4. Sheng, B., Li, Q.: Verifiable privacy-preserving range query in twotiered sensor networks. In: IEEE International Conference on Computer Communications (INFOCOM) (2008)
5. Sheng, B., Li, Q., Mao, W.: Data storage placement in sensor networks. In: ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc) (2006)
6. Shi, J., Zhang, R., Zhang, Y.: Secure range queries in tiered sensor networks. In: IEEE International Conference on Computer Communications (INFOCOM) (2009)
7. Yu, C.-M., Tsou, Y.-T., Lu, C.-S., Kuo, S.-Y.: Practical and secure multidimensional query framework in tiered sensor networks. IEEE Trans. Inf. Forensics Secur. **6**(2), 241–255 (2011)
8. Zhang, R., Shi, J., Zhang, Y.: Secure multidimensional range queries in sensor networks. In: ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc) (2009)