무선 센서 네트워크를 위한 동상 암호체계 기반의 안전한 데이터 병합 기법[†]

뽀노마르추크 율리야[*O], 남영진[**], 서대화[*]
[*]경북학교 전자전기컴퓨터학부, [**]대구대학교 컴퓨터·IT 공학부
rus_flash@hotmail.com, yjnam@daegu.ac.kr, dwseo@ee.knu.ac.kr

Homomorphic Cryptoschemes based Secure Data Aggregation for Wireless Sensor Networks

Ponomarchuk Yulia[*O], Young Jin Nam[**], Dae-Wha Seo[*]
[*]Dept. of Electronics and Computer Science, Kyungpook National University
[**]School of Computer & Information Technology, Daegu University

1. Introduction

Wireless sensor networks (WSNs) are becoming more and more popular in different industrial, research, and commercial projects and are used for environment, building or traffic monitoring, object tracking, in battlefield management, etc. Commonly WSNs consist of a large number of simple and inexpensive sensor nodes that have constrained and unrechargeable power resources draining off very quickly during communication. In order to increase the lifetime of a WSN and reduce the amount of transmitted data, aggregation is recommended when some synopsis of data (the average, minimum or maximum, etc.) is required at a base station. The method consists in sequential condensing of the sensed values in accordance with application requirements; the values aren't reconstructed at the receiver.

At the same time, the application, running over a WSN may require high level of transmitted data security. This paper considers data privacy issues between sensors, aggregators and base stations. We try to protect data, even if an adversary compromises aggregator nodes and obtains all keying material. This goal may be achieved if sensor data are not decrypted while they are aggregated. Therefore, the aim is to provide end-to-end encryption of measurements, as they are aggregated via hop-by-hop transmission. This approach also reduces the required number of computations. Such an end-to-end privacy is provided by homomorphic cryptoschemes. We observe several of such schemes and analyze their capabilities in providing data confidentiality and integrity. None of the considered schemes can guarantee high level of security under active attacker model alone; therefore combinations of schemes are analyzed if they can satisfy the requirements.

2. Analysis of Existing Homomorphic Cryptoschemes and Proposed Scheme

In the paper we assume an active adversary model, implying that an attacker can eavesdrop messages, physically access the nodes and read all stored data, perform replay attacks, modify packets, and inject bogus information. Thus, an aggregator's compromise leads to possibility of performing malicious aggregation, while data confidentiality and integrity require end-to-end privacy. Therefore secure encryption scheme must allow aggregation without decryption. At the same time, cryptographic instruments should be as cheap (in terms of computational cycles and memory) as possible.

Special cryptographic methods for secure data aggregation have privacy homomorphism (PH) property and allow aggregation without ciphertexts' decryption. The paper considers symmetric Domingo-Ferrer's (DF) PH scheme [1] and key stream based PH cryptoscheme of Castelluccia, et al. (CMT) [2], and public key based schemes of Okamoto-Uchiyama (OU) [3] and Elliptic curve ElGamal (ECEG) [4]. All considered PH schemes except CMT are vulnerable to replay attacks. For DF scheme it is crucial to keep the key in secret, since it is common for the whole network. ECEG and OU systems are very secure against chosen plaintext attack or physical attacks on sensors. But they can not protect from malicious modification and aggregation. CMT scheme provides security from the majority of attacks, except malicious modification. However, it is not scalable, as the base station should know all keys of all aggregated messages to decrypt the received result. None of the known solutions can provide both data integrity and confidentiality. However, DF scheme can be recommended for large synchronous networks in presence of passive attacker because of small time delay. Public key cryptography, especially ECEG, seems to be the most suitable for WSNs deployed in untrusted environment, especially if it is combined with digital signature scheme or uses different public keys for different time periods.

The proposed approach consists of encryption of sensed data and computing the digital signature of an encrypted message to prevent from malicious modification. Certainly, it would be better if the signature also could be

[†]This research was supported by the Kyungpook National University BK21, MKE (Ministry of Knowledge Economy), Korea, under the ITRC (Information Technology Research Center) support program supervised by the IITA (Institute for Information Technology Advancement) (IITA-2008-C1090-0801-0045).

aggregated. Several digital signature schemes, recommended for WSN, are considered in the paper. Scheme of [5] has low communication cost, but it is vulnerable if both a parent and a child node in the hierarchy are compromised. Also, its drawbacks are that the data is transmitted as plaintext, and the aggregators are assumed only to aggregate and forward messages, they do not have sensors. The scheme can be improved by applying Merkle hash tree [6] that is the commitment to all the leaf nodes. The communication cost of the modified scheme is lower, as interactive proof is used instead of queries. Boneh et al. in [7] described a scheme (BGLS) that allows aggregation of signatures generated by distinct signers on different messages into one short signature based on elliptic curves and bilinear mappings. Their scheme operates in so-called Gap Diffie-Hellman group (GDH), which is a group where the Decision Diffie-Hellman problem (DDH) is easy, but the Computational Diffie-Hellman problem (CDH) is hard. The aggregated signature is of the same size as individual ones and aggregation can be performed incrementally and by anyone. Verification of the aggregated BGLS signature involves computing the product of all messages' hashes.

After analyzing performance of the possible combinations of the encryption and digital signature schemes, we conclude that the combination of ECEG and BGLS is the most favorable. Here, the signature can use the same elliptic curve as the encryption scheme does. As for security, ECEG provides data confidentiality and BGLS can protect data integrity. Although it is quite expensive computationally, the size of encrypted message is smaller than the other schemes produce. The recent research has demonstrated that generation of such a signature using hardware accelerators may require less than a second and the impact on the lifetime of a node is negligible [8]. We assume the combination can be implemented on sensor nodes with limited resources in memory, energy and CPU cycles.

3. Conclusions

Previous research [2, 4] draws attention to the fact that symmetric cryptography requires data decryption to perform its aggregation and then, again, the result must be encrypted with another key. This procedure is repeated by each aggregator node while data are transmitted towards a base station. Therefore, employing of symmetric cryptography under high level of security requirements would demand sophisticated key management scheme and quite accurate nodes' synchronization when keys are revoked and exchanged. Still such a scheme could not be considered as highly secure, since an attacker can compromise any node, obtain all stored information, and take an advantage of it. Therefore homomorphic encryption schemes were proposed. Although they also turned to be vulnerable, as the majority of them allow malicious modification, they can be strengthened by application of signature scheme. BGLS seems to be the most perspective one, since it is also based on public cryptography and takes advantage of aggregation.

Recommended for WSNs digital signature schemes also are not satisfying, because they assume that aggregators do not have sensors, they sign plaintext messages, and an attacker can forge signatures if he compromises both a parent and a child. The schemes of [5, 6] allow data aggregation, but verification needs all keys broadcasting and storing intermediate results at each aggregator. The only known scheme, which can be applied to data aggregation combined with end-to-end privacy, is BGLS [7]. Its size is small (160 bits) and it can be aggregated as well. We considered combinations of BGLS with recommended homomorphic cryptoschemes and found that the most secure option is its combination with Elliptic Curve ElGamal scheme.

Future research will be devoted to the consideration of the suitable hash function for the BGLS scheme and the design of simulation of a WSN, over which secure data aggregation is used. Further, the obtained results will be compared with the other approaches.

References

1. Domingo-Ferrer J. A provably Secure Additive and Multiplicative Privacy Homomorphism. In Proc. of the 5th International Conference on Information Security, LNCS vol. 2433, pp. 471-483, 2002.
2. Castelluccia C., Mykletun E., Tsudik G. Efficient Aggregation of Encrypted Data in Wireless Sensor Networks. In Proc. of the 2nd Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services (MobiQuitos 2005), pp. 109-117, 2005.
3. Mykletun E., Girao J., Westhoff D. Public Key Based Cryptoschemes for Data Concealment in Wireless Sensor Networks. In Proc. of IEEE International Conference on Communications (ICC '06), vol. 5, pp. 2288-2295, 2006.
4. Peter S., Piotrowski K., Langendoerfer P. On Concealed Data Aggregation for Wireless Sensor Networks. In Proc. of IEEE Consumer Communications and Networking Conference (IEEE CCNC 2007), pp. 192-196, 2007.
5. Hu L., Evans D. Secure Aggregation for Wireless Networks. In Proc. of the 2003 Symposium on Applications and the Internet Workshops, pp. 384-391, 2003.
6. Przydatek B., Song D., Perrig A. SIA: Secure Information Aggregation in Sensor Networks. In Proc. Of the 1st International Conference on Embedded Networked Sensor Systems, pp. 255-265, 2003.
7. Boneh D., Gentry C., Lynn B., and Shacham H. Aggregate and Verifiably Encrypted Signatures from Bilinear Maps. In Proc. of EUROCRYPT '2003, LNSC vol. 2656, pp. 416-432, 2003.
8. Peter S., Langendoerfer P., Piotrowski K. Public key cryptography empowered smart dust is affordable. In Special issue on Energy-Efficient Algorithm and Protocol Design in Sensor Networks, International Journal of Sensor Networks (IJSNET), vol. 4, No. 1/2, 2008.