Securing Various Sensor Data in Wireless Nodes Using Incremental Cryptography

Sangeetha T S[1], Dr. Sobhana N V[2]

[1]*Student, Master of Technology, Computer Science &Engg, RIT Engineering College Kottayam, Kerala, India*
[2]*Professor, Dept. of Computer Science & Engg, RIT Engineering College Kottayam, Kerala, India*

---***---

Abstract - *Wireless sensor networks (WSNs) are increasingly being used in smart homes, by the military, for disaster detection, and in other applications which require the monitoring of environments. Meanwhile, many WSNs are deployed outside buildings, and the nodes in these networks are vulnerable to attack. Attackers can also obtain their own commodity sensor nodes and induce the network to accept them as legitimate nodes, or they can claim multiple identities for an altered node. Once in control of a few nodes inside the network, the adversary can then mount a variety of attacks such as falsification of sensor data, extraction of private sensed information from sensor network readings, and denial of service. Sensed information stays within the sensor network and is accessible only to trusted parties is an essential step toward achieving privacy. Encryption using Incremental cryptography is a promising method to address this problem. The goal of incremental cryptography is to design cryptography algorithms with the property that having applied the algorithm to a document, it is possible to quickly update the result of the algorithm for a modified document, rather than having to re-compute it from scratch.*

Key Words: **Incremental Cryptography, Wireless Sensor Networks, Encryption, Security, Performance.**

1. INTRODUCTION

Basic cryptographic primitives such as encryption and signatures (private or public key) have received thorough theoretical treatment. In various works strong definitions of security have been proposed and achieved under general complexity assumptions. The main problem that remains and which to a large extent prevents more widespread use of strong cryptography is the inefficiency of existing schemes. In a traditional cryptography, computation performed on entire document. It is a time consuming process. The goal of incremental cryptography is to design cryptographic algorithms with the property that having applied the algorithm to a document, it is possible to quickly update the result of the algorithm for a modified document, rather than having to re-compute it from scratch. In settings where cryptographic algorithms such as encryption or signatures are frequently applied to changing documents, dramatic efficiency improvements can be achieved.

Incrementality is a new measure of efficiency which is relevant in a large number of different settings and provide a comprehensive treatment of incremental cryptography. There are many ways to achieve incrementality. For example, an incremental encryption scheme can be made by first encrypting a document, and then for every change made to the document, merely append to the encryption an encrypted description of how to change the document.

Incremental cryptography provides an approach for reducing the costs associated with ease- of-use, speed, and ease of integration of cryptographic methods into software products. The way incremental cryptography solves these issues is by embedding the actual primitives into the system, be it a file system, text editor, web browser, or one of many other systems in common use today. Furthermore, it can compute in the background while the object is being modified, instead of after (as with traditional cryptography), and takes only an amount of time proportional to the length of edits, which can help speed up the computation considerably. In order to have incremental cryptography succeed, we need schemes which allow for dynamically re-evaluating computations based on changes. With these tools, we can solve some of the problems associated with traditional cryptography.

Consider the use case scenario of sensor networks where data comes from the nodes whose data rates rapidly increase as sensor technology improves and as the number of sensors expands. A typical representative for this scenario is environmental sensor networks used for natural disaster prevention or weather forecasting. In these cases, all data that is collected from different sensors should be publicly available, with data integrity guaranteed by digital signatures from a trusted party. Thus, data hashing is unavoidable, and as the dataset is being updated, the hash value should be recomputed. Normally, the update of such datasets is done by appending new data or by changing a small part of the existing dataset. As the size of the dataset grows, (and can reach hundreds of terabytes), recalculating the hash value of the entire dataset can become notoriously demanding in terms of both time and energy. An incremental update, on the other hand, can reduce the recalculation of the hash value to the minimum, and only of the parts of the dataset that have changed, or have been appended. Wireless Sensor Networks (WSNs) provide several types of applications providing comfortable and smart-economic life. Energy saving minimizing the rare sources of energy, noise and atmospheric monitoring reducing the pollution, and healthcare monitoring helping the health are examples of important applications in WSNs. And the sensor data updated in each and every second. So encryption and decryption is done each and every time using traditional cryptography. It is a time and energy consuming process. Using Incremental cryptography, updating of such datasets is done by changing a small part of the existing dataset.

2. LITERATURE REVIEW

Mihir Bellare, O. Goldreich and S. Goldwasser[1] proposed "Incremental Cryptography: The Case of Hashing and Signing". They initiate the investigation of a new kind of efficiency for cryptographic transformations. The idea is that having once applied the transformation to some document M, the time to update the result upon modification of M should be "proportional" to the "amount of modification" done to M. Thereby one obtains much faster cryptographic primitives for environments where closely related documents are undergoing the same cryptographic transformations. They provide some basic definitions enabling treatment of the new notion. We then exemplify our approach by suggesting incremental schemes for hashing and signing which are efficient according to our new measure.

Abdul Nasir Khan et. al.[2] proposed Incremental Cryptography for Security Schemes in Mobile Cloud computing environments. While using the cloud storage services on resource constraint mobile device, the mobile user needs to ensure the confidentiality of the critical data before uploading on the cloud storage. The resource limitation of mobile devices restricts mobile users for executing complex security operations using computational power of mobile devices. To make security schemes suitable for mobile devices, large volume of existing security schemes execute complex security operations remotely on cloud or trusted third party. Alternatively, few of the existing security schemes focus on the reduction of the computational complexity of the cryptographic algorithms. Keeping in view the resource limitation of mobile devices, it introduces an incremental cryptographic version of the existing security schemes, such as encryption-based scheme, coding based scheme, and sharing-based scheme, for improving the block(s) modification operations in term of resource utilization on mobile device. The experimental results show significant improvement in resource utilization on mobile device while performing block insertion, deletion, and modification operations as compared to the original version of the aforementioned schemes.

Mihir, Bellare et. al,[3] proposed incremental cryptography in the application of virus protection. One such setting is the use of authentication tags for virus protection. We consider documents that can be modified by powerful (and realistic) document modification operations such as insertion and deletion of character-strings (or equivalently cut and paste of text). We provide efficient incremental signature and message authentication schemes supporting the above document modification operations. They meet a strong notion of tamper-proof security which is appropriate for the virus protection setting. We initiate a study of incremental encryption, providing definitions as well as solutions. Finally, raise the novel issue of "privacy" of incremental authentication schemes.

Peng Xu et. al,[4] proposed a Lightweight Searchable Public-Key Encryption for Cloud- Assisted Wireless Sensor Networks. The industrial Internet of Things is flourishing, which is unprecedentedly driven by the rapid development of wireless sensor networks (WSNs) with the assistance of cloud computing. The new wave of technology will give rise to new risks to cyber security, particularly the data confidentiality in cloud-assisted WSNs (CWSNs). Searchable public-key encryption (SPE) is a promising method to address this problem. In theory, it allows sensors to upload public key cipher texts to the cloud, and the owner of these sensors can securely delegate a keyword search to the cloud and retrieve the intended data while maintaining data confidentiality. However, all existing and semantically secure SPE schemes have expensive costs in terms of generating cipher texts and searching key- words. Hence, this paper proposes a lightweight SPE (LSPE) scheme with semantic security for CWSNs. LSPE reduces a large number of the computation-intensive operations that are adopted in previous works; thus, LSPE has search performance close to that of some practical searchable symmetric encryption schemes. In addition, LSPE saves considerable time and energy costs of sensors for generating cipher texts. Finally, we experimentally test LSPE and compare the results with some previous works to quantitatively demonstrate the above advantages.

Subodha Charles et. al,[5] proposed incremental Cryptography to Secure Network-on-Chip. Network-on-chip (NoC) has become the standard communication fabric for on-chip components in modern System-on-chip (SoC) designs. Since NoC has visibility to all communications in the SoC, it has been one of the primary targets for security attacks. While packet encryption can provide secure communication, it can introduce unacceptable energy and performance overhead due to the resource- constrained nature of SoC designs. In this paper, we propose a lightweight encryption scheme that is implemented on the network interface. Our approach improves the performance of encryption without compromising security using incremental cryptography, which exploits the unique NoC traffic characteristics. Experimental results demonstrate that our proposed approach significantly reduces the encryption time compared to traditional approaches with negligible.

Wassim Itani et. al,[6] proposed the design and implementation of an integrity enforcement protocol for detecting malicious modification on electronic healthcare records (EHRs) stored and processed in the cloud. The proposed protocol leverages incremental cryptography premises and trusted computing building blocks to support secure integrity data structures that protect the medical records while: (1) complying with the specifications of regulatory policies and recommendations, (2) highly reducing the mobile client energy consumption, (3) considerably enhancing the performance of the applied cryptographic mechanisms on the mobile client as well as on the cloud servers, and (4) efficiently supporting dynamic data operations on the EHRs.

Junquan Wang et. al,[7] proposed Lattice-based Incremental Signature Scheme for the Authenticated Data Update in Fog Computing. he proposed scheme is provable secure in the standard model whose security is based on the hardness of the shortest integer solution (SIS) problem. There are several characters of the proposed scheme that are suitable for the application in fog computing. Such as, most of the time-consuming computing operations in the proposed scheme can be finished by the parallel computing. As a result, the computing speed of the proposed scheme can be improved efficiently. On the other hand, compared with a known lattice-based incremental digital signature, both the public key size and the signature length are shorter. Then the store resource and the bandwidth of the fog device can be saved efficiently when it is used in fog computing. Furthermore, a simulated experiment is given to check the functions of the proposed scheme by Java language on PC. The result shows that the computing cost to update a signature is much less than that to resign a message. At the same time, the parallel computing and pre-computing can really efficiently improve the computing speed of the proposed scheme. Since the SIS problem is hard even on quantum computers, the proposed scheme also gives a post-quantum secure solution to authenticate the updated data in fog computing.

Mihir Bellare et. al,[8] proposed a new approach for authenticating messages. "XOR MACs" have several nice features, including parallelizability, incrementality, and provable security. This method uses any finite pseudorandom function (PRF). The finite PRF can be "instantiated" via DES (yielding an alternative to the CBC MAC), via the compression function of MD5 (yielding an alternative to various "keyed MD5" constructions), or in a variety of other ways. The proven security is quantitative, expressing the adversary's inability to forge in terms of her (presumed) inability to break the underlying finite PRF. This is backed by attacks showing the analysis is tight. Our proofs exploit linear algebraic techniques, and relate the security of a given XOR scheme to the probability that a certain associated matrix is of full rank. Analysis shows that XOR schemes are actually more secure than the CBC MAC, in a sense that we can make precise.

3. CONCLUSIONS

As was stated in the introduction, cryptography is not used much in real world applications even in situations where it is an ideal solution to the problem. This problem has been one that cryptographers have worked hard at solving, and in order to do so, several problem areas were identified. Incremental cryptography has been demonstrated to be very effective in reducing the user-apparent delays, as well as making cryptography more embedded within the applications. While it does nothing to solve other problems, it does provide a major step in the direction of a long-term solution to the problems of ease of use, perceived speed, and ease of integration.

REFERENCES

[1] Mihir Bellare, O. Goldreich and S.Goldwasser, "Incremental Cryptography: The Case of Hashing and Signing", Crypto., Mar. 1994.

[2] Abdul Nasir Khan, M.L. Mat Kiah and Samee U. Khan , "A Study of Incremental Cryptography for Security Schemes in Mobile Cloud Computing Environments ", IEEE Symp.on Wireless Technology and Applications.,Sep. 2013.

[3] Mihir Bellare, O. Goldreich and S.Goldwasser, "Incremental Cryptography and Appli- cation to Virus Protection", n Proc. ACM Symp. on the Theory of Computing., May 1995.

[4] Peng Xu ,Shuanghong He, Wei Wang , Willy Susilo, and Hai Jin ,"Lightweight Search- able Public-Key Encryption for Cloud-Assisted Wireless Sensor Networks ", IEEE Trans.Industrial informatics.,Aug. 2018.

[5] Subodha Charles and Prabhat Mishra , "Securing Network-on-Chip Using Incremental Cryptography", in Proc. IEEE Computer society Symp., Jul. 2020.

[6] Wassim Itani,Ayman Kayssi and Ali Chehab, "Efficient healthcare integrity assurance in the cloud with incremental cryptography and trusted computing", in ResearchGate, Jan. 2014

[7] Junquan Wang , Fenghe Wang, Shaoquan Shi,,Wenfeng Yang, "Lattice-based Incremental Signature Scheme for the Authenticated Data Update in Fog Computing", in IEEE Access, Jul. 2017.

[8] Mihir Bellare, Roch Guerin and Phillip Rogawa, "SXOR MACs: New Methods for Message Authentication Using Finite Pseudorandom Functions", in Crypto 95 Proceedings ,Feb. 2005.