Countering Eavesdropper in Wsn by Traffic Decorrelation Techniques

[1]BITLA ALEKYA

PG Scholar, Department of CSE, Vaagdevi College of Engineering, Autonomous, Bollikunta, Warangal Telangana, Mail id:alekyabitla@gmail.com

[2]CHILUKOORI RAVINDER

Associate Professor Department of CSE, Vaagdevi College of Engineering, Autonomous, Bollikunta, Warangal Telangana, Mail id:rchilukoori@yahoo.com

ABSTRACT

Recently, a number of extended proxy re-encryption (PRE), e.g. Conditional (PRP), identity-based (PRP) and PRE (BPRE) have been proposed for flexible applications. By incorporating CPRE, IPRE and BPRE, this paper proposes a versatile primitive called conditional diffusion based on PRE identity (CIBPRE) and formalizes its semantic security. CIBPRE allows a sender to encrypt a message to multiple recipients by specifying the identities of those recipients, and the sender can delegate a re-encryption key to a proxy so that it can convert the original encrypted text into a new one at a time. new set of recipients. . In addition, the re-encryption key can be associated with a condition such that only the corresponding encrypted texts can be re-encrypted, which allows the original sender to apply access control to its remote encrypted texts in a fine manner. We offer an efficient CIBPRE system with provable security. In the instantiated schema, the initial encrypted text, the re-encrypted encrypted text and the re-encryption key are all of a constant size, and the parameters for generating a re-encryption key are independent of the original receivers of any initial encrypted text. . Finally, we show an application of our CIBPRE to secure an advantageous cloud messaging system compared to existing secure messaging systems based on the Pretty Good Privacy protocol or identity-based encryption

1 INTRODUCTION

PROXY re-encryption (PRE) [1] provides a secure and flexible method for a sender to store and share data. A user can encrypt his file with his own public key, and then store the encrypted text in an honest but curious server. When the recipient is decided, the sender may delegate a re-encryption key associated with the receiver to the server as a proxy. Then, the proxy re-encrypts the original encrypted text to the intended recipient. Finally, the recipient can decrypt the resulting encrypted text with his private key. The security of PRE generally ensures that (1) neither the server /proxy nor the unintended recipients can learn useful information about the (re) encrypted file, and (2) before receiving the re-encryption key, the proxy does not can not re-encrypt the initial encrypted text in a meaningful way. Efforts have been made to equip PRE with versatile capabilities. The early ERP has been proposed in the traditional framework of PKI which involves complicated certificate management [2]. To overcome this problem, several identity-based PRE (IPRE) schemas have been proposed so that the recognizable identities of the receivers can serve as public keys. Instead of picking up and verifying recipients' certificates, the sender and agent simply need to know who the recipients are, which is more practical in practice.

PRE and IPRE allow a single receiver. If there are more receivers, the system must call PRE or IPRE multiple times. To solve this problem, the diffusion concept PRE (BPRE) has been proposed [9]. BPRE works in the same way as PRE and IPRE but is more versatile. On the other hand, BPRE allows a sender to generate an initial ciphertext to a set of receivers instead of a single receiver. In addition, the sender can delegate a re-encryption key associated with another set of receivers so that the proxy can re-encrypt it. The PRE schemes above only allow the re-encryption procedure to be executed in an all or nothing manner. The proxy can re-encrypt all initial encrypted texts or none of them. This rough control over encrypted texts to be re-encrypted can limit the application of PRE systems. To fill this gap, a refined concept called PRE (ERCP) conditional has been proposed. In ERCP systems, a sender can apply fine-end encryption control over its initial encrypted texts. The sender achieves this by associating a condition with a re-encryption key. Only ciphers that meet the specified condition can be re-encrypted by the proxy containing the corresponding encryption key.

A recent conditional proxy broadcast re-encryption scheme [14] allows senders to control the time to re-encrypt their initial encrypted text. When a sender generates _ P. Xu is with the Laboratory of Technology and Computer Services System, cluster and grid computing laboratory, School of Computer Science and Technology, Huazhong University of Science and Technology, Wuhan 430074, China, a key of rechiff-encrypting an initial ciphertext, the sender must take as input the original identities of the recipient of the initial ciphertext. In practice, this means that the sender must remember locally the identities of the receivers of all initial encrypted texts. This requirement makes this scheme constrained for memory-limited or mobile senders and effective only for special applications.

2. RELATED WORK

The first PRE scheme was proposed by Blaze, Bleumer and Strauss in [1]. Following this seminal work, a number of PRE schemes have been proposed in the traditional public key setting. These PRE schemes need certificates to prove the validity of public keys. A user has to verify the certificates before encrypting a plaintext. In order to avoid the overhead to verify public keys' certificates, several IPRE schemes have been presented by incorporating the idea of identity-based encryption [16]. The scheme in [3] is proven secure in the random oracle (RO) model in which a hash function is assumed fully random. In contrast, the scheme in [4] is proven secure in the standard model. The scheme in [5] is proven secure in a stronger security sense, i.e., in distinguishability against chosen-ciphertext attack in the standard model. The above PRE schemes only allow data sharing in a coarse-grained manner. That is, if the user delegates a reencryption key to the proxy, all ciphertexts can be reencrypted and then be accessible to the intended users; else none of the ciphertexts can be re-encrypted or accessed by others.

This issue is addressed in the recent CPRE schemes allowing finegrained data sharing. The schemes in are proven secure against chosen-ciphertext attack. The conditional identity-based PRE (CIPRE) schemes in combines the underlying ideas of CPRE and IPRE. Similarly, the two conditional broadcast PRE schemes in [9] combines the notions of CPRE and broadcast encryption, and are secure against chosen-plaintext attacks and chosen-ciphertext attacks, respectively. In addition to fine-grained data sharing, an extra advantage of these CBPRE schemes is that it allows one to share data with multiple users in a more efficient way. Several other optional properties have been achieved in recent PRE schemes.

The PRE schemes in are equipped with an extra property that the receiver of aciphertext is anonymous. The schemes in [26], [27] achievemulti-use bidirectional re-encryption. A ciphertext can be re-encrypted multiple times. Moreover, a re-encryption key realizes the bidirectional share between two users. Specifically, if Alice delegates a re-encryption key to a proxy for re-encrypting her ciphertexts to Bob. The re-encryption key can also enable to re-encrypt Bob’s ciphertexts to Alice. These two PRE schemes are provably secure under the chosen- ciphertext attack respectively in the random oracle and standard models. In contrast, the PRE scheme in [21] is multi-use unidirectional PRE schemes in which bidirectional re-encryption is forbidden. The work in [28] defines a general notion for PRE, which is called deterministic finite automata-based functional PRE (DFA-based FPRE), and proposes a concrete DFA-based FPRE system. The recent work in [29] proposes cloud-based revocable identity-based proxy re-encryption that supports user revocation and delegation of decryption rights.

3 THE PROPOSED CIBPRE SCHEME

Referring to the concept of CIBPRE, roughly speaking, both the initial CIBPRE ciphertext and the re-encrypted CIBPRE ciphertext are the IBBE ciphertexts. But it is different with an IBBE scheme that CIBPRE provides algorithms to transform an IBBE ciphertext (corresponding to an initial CIBPRE ciphertext) into another IBBE ciphertext (corresponding to an re-encrypted CIBPRE ciphertext). Moreover, the transformation is correct if it satisfies the consistencies defined by CIBPRE. Therefore, in order to construct a CIBPRE scheme, we refers to the D07 scheme which was reviewed . Compared with the D07 scheme, the proposed CIBPRE scheme associates a D07 IBBE ciphertext with a new part to generate an initial CIBPRE ciphertext. This new part will be used to realize the capability ”Conditional” of CIBPRE. In addition, it provides some new algorithms, which are respectively to generate a reencryption key, re-encrypt an initial CIBPRE ciphertext and decrypt a re- encrypted CIBPRE ciphertext. The decryption of an initial CIBPRE ciphertext is the same with the D07 scheme. The proposed CIBPRE scheme is as follows:_ SetupPRE_;NÞ: Given a security parameter _ 2 N and value N (the maximum number of receivers in each encryption), this algorithm probabilistically constructs

4 CONCLUSION

We tackled the problem of privacy of contextual information in WSN under a global indiscreet ear. We presented a general method of traffic analysis to collectively deal with packet interception times and eavesdropping locations in a merge center. The method is independent of the protection mechanism and can be used as a reference to evaluate different schemes. To mitigate global spying, we have proposed traffic normalization methods that regulate the sensor traffic patterns of a subset of sensors that form MCDS. We developed two algorithms for partitioning the WSN into MCDS and SS-MCDS and evaluated their performance via simulations. Compared to previous methods able to protect against global eavesdropping, we have shown that the limitation of fictitious traffic transmissions to MCDS nodes, reduces the overhead of communication due to the normalization of traffic. We have also proposed a flexible transmission coordination system that reduces the end-to-end delay for event notification.

REFERENCES

[1] M. Akhlaq and T. R. Sheltami. RTSP: An accurate and energyefficient protocol for clock synchronization in wsns. IEEE Transactions on Instrumentation and Measurement, 62(3):578–589, 2013.

[2] B. Alomair, A. Clark, J. Cuellar, and R. Poovendran. Toward a statistical framework for source anonymity in sensor networks. IEEE Transactions on Mobile Computing, 12(2):248–260, 2013.

[3] F. Armknecht, J. Girao, A. Matos, and R. Aguiar. Who said that? privacy at the link layer. In Proc. of the INFOCOM Conference, pages 2521–2525, 2007.

[4] K. Bicakci, H. Gultekin, B. Tavli, and I. Bagci. Maximizing lifetime of event-unobservable wireless sensor networks. Computer Standards & Interfaces, 33(4):401–410, 2011.

[5] G. Chinnu and N. Dhinakaran. Protecting location privacy in wireless sensor networks against a local

eavesdropper–a survey. International Journal of Computer Applications, 56(5):25–47, 2012.

[6] M. Conti, J. Willemsen, and B. Crispo. Providing source location privacy in wireless sensor networks: A survey. Communications Surveys Tutorials, 15(3):1238–1280, 2013.

[7] J. Deng, R. Han, and S. Mishra. Decorrelating wireless sensor network traffic to inhibit traffic analysis attacks. Pervasive and Mobile Computing, 2(2):159–186, 2006.

[8] M. Fruth. Probabilistic model checking of contention resolution in the IEEE 802.15.4 low-rate wireless personal area network protocol. In Proc. of the Symp. on Leveraging Applications of Formal Methods, Verification and Validation, pages 290–297, 2006.

[9] M. Garey and D. Johnson. Computers and Intractability, volume 174. Freeman, 1979.

[10] B. Greenstein, D. McCoy, J. Pang, T. Kohno, S. Seshan, and D. Wetherall. Improving wireless privacy with an identifier-free link layer protocol. In Proc. of the ACM Conference on Mobile Systems, Spplications, and Services, pages 40–53, 2008.

[11] J. Gross and J. Yellen. Handbook of Graph Theory. CRC, 2004.

[12] A. Jhumka, M. Leeke, and S. Shrestha. On the use of fake sources for source