ISSN : 2348 - 9065 (Online)
ISSN : 2349 - 3143 (Print)
Vol. 3, Issue 1 Jan. - Mar. 2016
International Journal of Research in Electronics and Communication Technology (IJRECT 2016)

Secured Decentralized Confidential Data Distributed in The Disruption-Tolerant Military Network

[I]Aniruddha Singh Chauhan, [II]Prof. Nikita Umare
[I]ME 3rd Sem. WCC Student, Abha Gaikwad-Patil College of Engineering, Nagpur, Maharashtra, India
[II]Dept. of CSE/WCC, Abha Gaikwad-Patil College of Engineering, Nagpur, Maharashtra, India

Abstract
The confidential information or command reliably by exploiting external storage nodes. Some of the most challenging issues in this scenario are the enforcement of authorization policies and the policies update for secure data retrieval. Cipher text-policy attribute-based encryption is a promising cryptographic solution to the access control issues. However, the problem of applying CP-ABE in decentralized DTNs introduces several security and privacy challenges with regard to the attribute revocation, key escrow, and coordination of attributes issued from different authorities. we propose a secure data retrieval scheme using idea for decentralized DTNs where multiple key authorities manage their attributes independently. We demonstrate how to apply the proposed mechanism to securely and efficiently manage the confidential data distributed in the disruption-tolerant military network.

Keywords
Access Control, Attribute-Based Encryption (ABE), Disruption-Tolerant Network (DTN), Multiauthority, Secure

I. Introduction

Mobile nodes in military environments such as a battlefield or a hostile region are likely to suffer from intermittent network connectivity and frequent partitions. Disruption-tolerant network (DTN) technologies are becoming successful solutions that allow wireless devices carried by soldiers to communicate with each other and access the confidential information or command reliably by exploiting external storage nodes. Some of the most challenging issues in this scenario are the enforcement of authorization policies and the policies update for secure data retrieval. Ciphertext-policy attribute-based encryption (CP-ABE) is a promising cryptographic solution to the access control issues. However, the problem of applying CP-ABE in decentralized DTNs introduces several security and privacy challenges with regard to the attribute revocation, key escrow, and coordination of attributes issued from different authorities. We propose a secure data retrieval scheme using CP-ABE for decentralized DTNs where multiple key authorities manage their attributes independently. We demonstrate how to apply the proposed mechanism to securely and efficiently manage the confidential data distributed in the disruption-tolerant military network data sets in order to illustrate the advantages of using such an approach

II. Problem Defination

- Military applications require increased protection of confidential data including access control methods.
- In many cases, it is desirable to provide differentiated access services such that

Data access policies are defined over user attributes or roles, which are managed by the key authorities. It propose a D2C2 algorithm for visual pattern discovery by joint analysis of visual content and side information. A content collection is partitioned into subsets based on side information, and the unique and common visual patterns are discovered with multiple instance learning and clustering steps that analyzes across and within these subsets. Such patterns help to visualize the data content and generate vocabulary-based features for semantic classification. The proposed framework is rather general which can handle all types' offside information, and incorporate different common/unique pattern extraction algorithms. One future work is to improve the generation of common patterns by emphasizing the shared consistencies, instead of the current heuristic clustering. Another future work is toexplore other applications using the unique common patterns.and rms do not have to be defined. Do not use abbreviations in the title or heads unless they are unavoidable.

III. Literature Review

Secure Data Retrieval for Decentralized Disruption-Tolerant Military Networks [1] Junbeom Hur and Kyungtae Kang, IEEE/ ACM TRANSACTIONS ON NETWORKING, VOL. 22, NO. 1, FEBRUARY 2014. Mobile nodes in military environments such as a battlefield or a hostile region are likely to suffer from intermittent network connectivity and frequent partitions. Disruption-tolerant network (DTN) technologies are becoming successful solutions that allow wireless devices carried by soldiers to communicate with each other and access the confidential information or command reliably by exploiting external storage nodes. Some of the most challenging issues in this scenario are the enforcement of authorization policies and the policies update for secure data retrieval. Ciphertext-policy attribute-based encryption (CP-ABE) is a promising cryptographic solution to the access control issues. However, the problem of applying CP-ABE in decentralized DTNs introduces several security and privacy challenges with regard to the attribute revocation, key escrow, and coordination of attributes issued from different authorities.

Border Surveillance: [2] A dynamic deployment scheme for WSN-based solutions Ramzi Bellazreg1, Noureddine Boudriga1, Khalifa

Tunisia and 3Korea University ©2013 IEEE.

Wireless Sensor Networks (WSNs) are based on elementary sensors that detect the occurrence of particular events in a monitored area. Among the recent critical WSN applications one can find the border surveillance applications. The first aim of this class of applications is to monitor a country border and detect the presence of intruders near the border line. In this paper, we investigate theoretically the effects of natural factors on dynamic deployment scheme of a hierarchical WSN-based solution providing two lines of surveillance. Parameters such as the wind effect, the altitude and velocity of the airplane from which the sensors are thrown are put into equation to optimize the area coverage and WSN connectivity. Then, we propose mathematical models that evaluate the quality of connectivity and coverage of the deployed network and allow

ISSN : 2348 - 9065 (Online)
ISSN : 2349 - 3143 (Print)

planning and dimensioning of a border solution.
Barrier Coverage with Airdropped Wireless Sensors Anwar Saipulla Benyuan Liu Jie Wang Department of Computer Science University of Massachusetts Lowell Lowell, MA 01854 USA 2008 IEEE.
Barrier coverage of a wireless sensor network aims at detecting intruders crossing the network. It provides a viable alternative for monitoring boundaries of battlefields, country borders, coastal lines, and perimeters of critical infrastructures. Early studies on barrier coverage typically assume that sensors are deployed uniformly at random in a large area. This assumption, while theoretically interesting, may be unrealistic in real applications. We take a more realistic approach in this paper. In particular, we consider that sensors are airdropped from an aircraft along its flying route. We note that wind, geographic terrain, and other factors may cause a sensor to land in a location deviating from its targeted landing point with a random offset. Thus, it is more realistic to assume that sensor nodes are distributed with a normal offset along the deployment line.

IV. Motovation

We provide a multi authority CP-ABE scheme for secure data retrieval in decentralized DTNs. Each local authority issues partial personalized and attribute key components to a user by performing secure 2PC protocol with the central authority. Each attribute key of a user can be updated individually and immediately. Thus, the scalability and security can be enhanced in the proposed scheme. Since the first CP-ABE scheme proposed by Be then court et al. [13], dozens of CP-ABE schemes have been proposed [7], [21]–[23]. The subsequent CP-ABE schemes are mostly motivated by more rigorous security proof in the standard model. However, most of the schemes failed to achieve the expressiveness of the Bethencourt et al.'s scheme,
The main priority to resolve following issues in proposed Project as:

1. Key Escrow
2. Decentralized ABE Scheme
3. Central authority and local authority engage with MD5 Algo which prevents to know them each other master Secrets.
4. User should not revoked its attributes and satisfying access policies
5. Sender is responsible for enforcing access scheme

V. Proposed Method

1) Key Authorities: They are key generation centers that generate public/secret parameters for CP-ABE. The key authorities consist of a central authority and multiple local authorities. We assume that there are secure and reliable communication channels between a central authority and each local authority during the initial key setup and generation phase.
   Each local authority manages different attributes and issues corresponding attribute keys to users.
   They grant differential access rights to individual users based on the users' attributes. The key authorities are assumed to be honest-but-curious. That is, they will honestly execute the assigned tasks in the system, however they would like to learn information of encrypted contents as much as possible.
2) Storage node: This is an entity that stores data from senders and provide corresponding access to users. It may be mobile or static. Similar to the previous schemes, we also assume the storage node to be semi trusted that is honest-but-curious.
3) Sender: This is an entity who owns confidential messages or data (e.g., a commander) and wishes to store them intothe external data storage node for ease of sharing or for reliable delivery to users in the extreme networking environments. A sender is responsible for defining (attributebased) access policy and enforcing it on its own data by encrypting the data under the policy before storing it to the storage node.
4) User: This is a mobile node who wants to access the data stored at the storage node (e.g., a soldier). If a user possesses a set of attributes satisfying the access policy of the encrypted data defined by the sender, and is not revoked in any of the attributes, then he will be able to decrypt the IDEA ALGORTHIM and obtain the data. Since the key authorities are semi-trusted, they should be deterred from accessing plaintext of the data in the storage node; they should be still able to issue secret keys to users. In order to realize this somewhat contradictory requirement, the entral authority and the local authorities engage in the arithmetic 2PC protocol with master secret keys of their own and issue independent key components to users during the key issuing phase. 2PC protocol prevents them from knowing each other's master secrets so that none of them can generate the whole set of secret keys of users individually.

VI. Methodlogy

We propose an attribute-based secure data retrieval scheme using CP-ABE for decentralized DTNs. The proposed scheme features the following achievements. First, immediate attribute revocation enhances backward/forward secrecy of confidential data by reducing the windows of vulnerability. Second, encryptors can define a fine-grained access policy using any monotone access structure under attributes issued from any chosen set of authorities. Third, the key escrow problem is resolved by an escrow-free key issuing protocol that exploits the characteristic of the decentralized DTN architecture. The key issuing protocol generates and issues user secret keys by performing a secure two-party computation (2PC) protocol among the key authorities with their own master secrets. The 2PC protocol deters the key authorities from obtaining any master secret information of each other such that none of them could generate the whole set of user keys alone. Thus, users are not required to fully trust the authorities in order to protect their data to be shared. The data confidentiality and privacy can be cryptographically enforced against any curious key authorities or data storage nodes in the proposed scheme.

VII. Conculsion

Technologies are becoming successful solutions in military Applications that allow wireless devices to communicate with each other and access the confidential information reliably by exploiting external storage nodes. It is a scalable cryptographic solution to the access control and secure data retrieval issues. In this paper, we proposed an efficient and secure data retrieval method using this method for decentralized DTNs where multiple key authorities manage their attributes independently. The inherent key escrow problem is resolved such that the confidentiality of the stored data is guaranteed even under the hostile environment where key authorities might be compromised or not fully trusted.

References

[1] J. Burgess, B. Gallagher, D. Jensen, and B. N. Levine, "Maxprop: Routing for vehicle-based disruption tolerant

networks," in Proc. IEEE INFOCOM, 2006, pp. 1–11.

[2] M. Chuah and P. Yang, "Node density-based adaptive routing scheme for disruption tolerant networks," in Proc. IEEE MILCOM, 2006, pp. 1–6.

[3] M. M. B. Tariq, M. Ammar, and E. Zequra, "Mesage ferry route design for sparse ad hoc networks with mobile nodes," in Proc. ACM MobiHoc, 2006, pp. 37–48.

[4] S. Roy andM. Chuah, "Secure data retrieval based on ciphertext policy attribute-based encryption (CP-ABE) system for the DTNs," Lehigh CSE Tech. Rep., 2009.

[5] M. Chuah and P. Yang, "Performance evaluation of content-based information retrieval schemes for DTNs," in Proc. IEEE MILCOM, 2007, pp. 1–7.

[6] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, "Plutus: Scalable secure file sharing on untrusted storage," in Proc. Conf. File Storage Technol., 2003, pp. 29–42.

[7] L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker, "Mediated ciphertext-policy attribute-based encryption and its application,"in Proc. WISA, 2009, LNCS 5932, pp. 309–323.

[8] N. Chen, M. Gerla, D. Huang, and X. Hong, "Secure, selective group Broadcast in vehicular networks using dynamic attribute based encryption,"in Proc. Ad Hoc Netw. Workshop, 2010, pp. 1–8.

[9] D. Huang and M. Verma, "ASPE: Attribute-based secure policy enforcement n vehicular ad hoc networks," Ad Hoc Netw., vol. 7, no. 8, pp. 1526–1535, 2009.

[10] A. Lewko and B. Waters, "Decentralizing attribute-based encryption,"Cryptology ePrint Archive: Rep. 2010/351, 2010.

[11] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Proc.Eurocrypt, 2005, pp. 457–473.

[12] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proc. ACM Conf. Comput. Commun. Security, 2006, pp. 89–98.

[13] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attributebased encryption," in Proc. IEEE Symp. Security Privacy, 2007, pp. 321–334.

[14] R. Ostrovsky, A. Sahai, and B. Waters, "Attribute-based encryption with non-monotonic access structures," in Proc. ACM Conf. Comput. Commun. Security, 2007, pp. 195–203.

[15] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute based data sharing with attribute revocation," in Proc. ASIACCS, 2010, pp. 261–270.

Author's Profile

Pursuing M.E. in Wireless communication from Nagpur University .