Volume 3, Issue 12, December-2016, pp. 625-628 ISSN (O): 2349-7084

International Journal of Computer Engineering In Research Trends

Available online at: www.ijcert.org

Secure Data Communication Using IDEA for Decentralized Disruption-Tolerant Military Networks

[1] Atish Budhhe, [2] Prof. Hirendra R. Hajare

[1, 2] BIT Ballarpur Gondwana University

Email ID: [1] atishbuddhe30@gmail.com ,[2] hirendrahajare@gmail.com

Abstract— Nowadays Disruption tolerant network technologies are getting to be distinctly well known that permit wireless devices supported by soldiers to communicate with each other and access the confidential information or command consistently by abusing external storage nodes. The absolute 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 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 productively deal with the classified information conveyed in the distributed in the disruption-tolerant military network.

Index Terms— CP-ABE, Access control, attribute-based encryption (ABE), Dsruption-tolerant network (DTN), IDEA, multiauthority, secure data retrieval.

.

1. INTRODUCTION

A DTN is a network of smaller networks. It is an overlay on top of special-purpose networks, including the Internet.DTNs support interoperability of other networks by accommodating long disruptions and delays between and within those networks, and by translating between the communication protocols of those networks. In providing these functions, DTNs accommodate the mobility and limited power of evolving wireless communication devices.

DTNs were originally developed for interplanetary use, where the speed of light can seem slow and delay-tolerance is the greatest need. However, DTNs may have far more diverse applications on Earth, where disruption-tolerance is the greatest need. The potential Earth applications span a broad range of commercial, scientific, military, and public-service applications.

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 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.

2. LITERATURE SURVEY

1. Secure Data Retrieval for Decentralized Disruption-Tolerant Military Networks 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 () is a promising cryptographic solution to the access control issues. However, the problem of applying 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

2. Border Surveillance: A dynamic deployment scheme for WSN-based solutions Ramzi Bellazreg1, Noureddine Boudriga1, Khalifa Trimèche 2 and Sunshin An31 University of Carthage Tunisia, 2 Faculty of Science of tunis 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 planning and dimensioning of a border solution.

3. 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.

Fig 1. System Flow

3. PROPOSED SYSTEM

1) Key Authorities:

They are key generation centers that generate public/secret parameters for. The key authoritiesconsist 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 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 with master secret keys of their own and issue independent key components to users during the key issuing phase. It 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.

3.1 METHODLOGY:

We propose an attribute-based secure data retrieval scheme using 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 among the key authorities with their own master secrets. 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.

IDEA ALGORTHIM: IDEA encrypts a 64-bit block of plaintext to 64-bit block of ciphertext. It usesa 128-bit key. The algorithm consists of eight identical rounds and a "half" roundfinal Transformation. There are 216 possible 16-bit blocks: 0000000000000000, 1111111111111111, each operation with the set of possible 16-bit blocks is an algebraic group. Bitwise XOR is bitwise addition modulo 2, and addition modulo 216 is the usual group operation. Some spin must be put on the elements – the 16-bit blocks – to make sense of multiplication modulo 216 + 1, however. 0 (i.e., 0000000000000000) is not an element of the multiplicative group.

4. CONCLUSION

The consistent attribute group keys are reorganized and delivered to the effective attribute group members securely (including the user Furthermore, the majority of the components encoded with a secret key in the ciphertext are reencrypted by the storage node with a random, and the ciphertext components corresponding to the attributes are also reencrypted with the updated attribute group keys. Even if the user has stored the previous ciphertext exchanged before he obtains the attribute keys and the holding attributes satisfy the access policy, he cannot decrypt the permeable ciphertext.

5. REFERENCES

[1] J. Burgess, B. Gallagher, D. Jensen, and B. N. Levine, "Maxprop: outing 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 () 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.

 DOI:10.22362/ijcert/2016/v3/i12/xxxx