Review Paper on Highly Secure Data Communication Between Two Decentralized Army Stations

Rasika S. Rangari , Prof. Anil N. Jaiswal

Abstract—**Disruption-tolerant network (DTN) technologies are becoming a successful solutions that allows wireless devices carried by a soldiers to communicate with each others and access the confidential information or a command reliably by exploiting storage nodes. Some of the challenging issues in the scenario are the enforcement of an authorization policy and the policies update for a secure data retrieval. Cipher text policy attribute based encryption is a promising cryptographic solution to access control issues. The problem of applying CPABE in decentralized DTN introduces a several security and a privacy challenges with a regard to the attribute revocation , key escrow , and the coordination of attributes issued from the different authorities. a secure data retrieval scheme using IDEA for decentralized DTNs where multiple key authorities manages their attributes independently. The demonstrate to apply a proposed mechanism to securely and efficiently manages the confidential data distributed in a disruption tolerant military network.**

Index Terms— An Access control, Attribute Based Encryption (ABE), Disruption Tolerant Network (DTN), multi authority and secure data retrieval.

I. INTRODUCTION

Mobile nodes in a military environments as a battlefield or a hostile regions are likely to be suffer from an intermittent networks connectivity and frequent partitions and Disruption tolerant network (DTN) technologies are becoming a successful solutions that allow a wireless devices carried by a soldiers to communicate with each other's and access the confidential information's or command reliably by exploiting the external storage nodes. The most challenging issues are an enforcement of authorization policy and the policies update for a secure data retrieval. Cipher text policy attribute based encryption is a promising cryptographic solution to access control issues.

Manuscript received Feb, 2013.

Rasika S. Rangari *, Department of Computer Science and Engineering, G.H Raisoni Institute of Engineering and Technology for Women, Nagpur, India.*

Prof. Anil N. Jaiswal,*, Department of Computer Science and Engineering, G.H Raisoni Institute of Engineering and Technology for Women, Nagpur, India.*

The problem of applying an CP-ABE in decentralized DTNs introduces a several security and a privacy challenges with regard to attribute revocation, key escrow, and a coordination of attributes issued from different authorities. a secure data retrieval schemes using a CP-ABE for a decentralized DTNs. where, a multiple key authorities manage their attributes independently. Demonstrate to appling the proposed mechanism to securely and efficiently manage a confidential data which is distributed in the disruption-tolerant military network.

II. PROBLEM DEFINATION

The military applications are requires to increased protection of a confidential data including access control methods. In many cases, it is a desirable to provide a differentiated access services that a Data access policies are defined over a user attributes or a roles, which are managed by the key authorities.

III. LITERATURE REVIEW

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.

A mobile nodes which contain in military environments such as a battlefield or a hostile regions are likely to a suffer from an intermittent networks connectivity and a frequent partitions. The Disruption tolerant network (DTN) technologies are becoming a successful solutions to that allows a wireless devices carried by a soldiers to communicate with each other's and an access the confidential information or a command reliably by exploiting external storage nodes. The most challenging issues for this scenario are the enforcement of authorization policy and the policies which are update for secure data retrieval.

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 a elementary sensors that detects the occurrences of particular events in a monitored area. The recent critical WSN applications are one can find a border surveillance applications. The first aim of the class of applications are to monitor the country border and a detect the presence of a intruders near to the border line. In this,

ISSN: 2278 – 1323

investigate a theoretically the effects of a natural factors on dynamic deployment schemes of a hierarchical WSN based solutions to providing two lines of a surveillance. Parameters such as wind effect, altitude and a velocity of the airplanes from which a sensors are thrown are put into a equation to optimize the coverage area and WSN connectivity. The mathematical models that evaluate a quality of connectivity and the coverage of the deployed network and allow a 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 MA 01854 USA 2008 IEEE.
Barrier coverage of a wireless sensor network aims at detecting intruders crossing a network. It provides a viable alternative for monitoring boundaries of battlefields, country borders, coastal lines, and The perimeters of critical infrastructures. Early studies on a barrier coverage typically is assume that sensors are deployed uniformly at random in a large area. while theoretically interesting, may be unrealistic in real applications. A more realistic approach in this paper. Considering that sensors are airdropped from an aircraft along its flying route.The wind, geographic terrain, and other factors are may cause a sensor to land in a locations deviating from its targeted landing point with a random offset. It is more realistic to assume that sensor nodes are distributed with a normal offset along the deployment line.

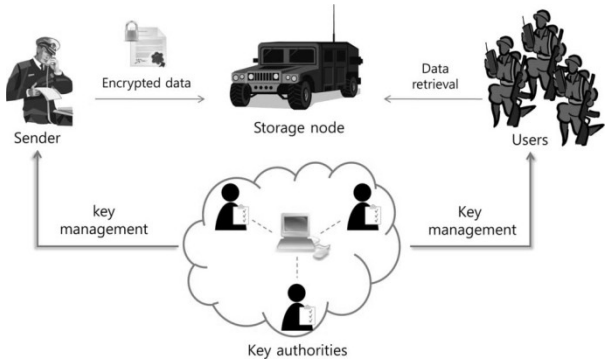

Fig 1. A System Flow

IV. PROPOSED METHOD

1) Key Authorities: They are the key generation centers that generate a public/secret parameters for a CP-ABE. The key authorities that consist of a central authority and a multiple local authorities. A secure and a reliable communication channels are between the central authority and each a local authority during an initial key setups and a generation phase. Each local authority manages a different attributes and issues corresponding to the attribute keys to users. They are grant differential access rights to a individual a users which based on a users attributes. The key authorities which are assumed to be an honest but curious. That is, they will be honestly execute the assigned tasks in a system. However, they would like to be learn information of an encrypted contents as much as possible.

2) Storage nodes: This is an entity that stores a data from senders and provide a corresponding access to the users. It may be a mobile or a static, Similar to the previous schemes. Assume the storage nodes to be a semi trusted, that is a honest but curious.

3) Sender: It is an entity which owns confidential messages or data and wishes to store them into a external data storage nodes for ease of sharing or for a reliable delivery to the users in the extremes networking environments. It is a responsible for a defining access a policy and that is enforcing it on its own data by encrypting the data under the policy before store to the storage node.

4) User: They are mobile nodes who want to access the data stored at storage node. If a user possesses a set of the attributes satisfying an access policy of the encrypt data defined by the sender and not a revoked in any of the attributes, then the user will be able to decrypt the IDEA ALGORTHIM and obtain the data. Since the key authorities are semi-trusted, they should be deterred from an accessing plaintext of the data in the storage nodes, they should be still able to issue the secret keys to users. In order to realize this somewhat contradictory requirement, the central authority and the local authorities engage to the arithmetic. 2PC protocol with a master secret keys of a their owns and issues the independent key components to users during the key issuing phase. 2PC protocol prevents them from knowing each other's master secrets, so that a none of them can be generate the whole set of a secret keys of users individually.

V. RELATED WORK

An attribute based a secure data which is a retrieval scheme using CP-ABE for a decentralized DTNs. The proposed scheme features are the following achievements. First, the immediate an attribute revocation enhances the backward/forward secrecy of a confidential data reducing by the windows of a vulnerability. Then Second, the encryptions can be defining a fine grain access policy using any of a monotone access structure under the attributes issued from any chosen set of the authorities. Third is the key escrow problem which resolved by an escrow-free key issuing a protocol that exploits the characteristic of a decentralized DTN architecture then The key issuing protocol that generates and a issues a user secret keys by performing a secure two-party computation (2PC) protocol among the key authorities with their own master secrets. 2PC protocols deters are the key authorities from obtaining an any master secret information's for each other's that no one of them could be generate the whole set of user keys are alone. Thus, a users are not required to fully trust to the authorities in order to a protect their data that to be shared. Data confidentiality and privacy that can be cryptographically enforced against a curious keys authorities or a data storage nodes in a proposed scheme.

IDEA ALGORTHIM

IDEA ALGORTHIM encrypts a 64 bit block of plaintext to a 64 bit block of cipher text. It uses a 128 bit key. The algorithm consists of a eight identical rounds and a half round final transformation. There are 216 possible a 16-bit blocks 0000000000000000, 1111111111111111 each operation with the set of a possible 16-bit blocks, which is an algebraic group.

ISSN: 2278 – 1323

Bitwise XOR is a 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 is not an element of the multiplicative group.

VI. CONCLUSION

The corresponding attribute group keys are updated and a delivered to valid attribute group members securely. In addition to all of the components which is encrypted with a secret key in a cipher text are reencrypted by the storage nodes with a random and cipher text components are corresponding to the attributes which are also reencrypted with the updated attribute group keys. If the user has stored the previous cipher text exchanged before user obtains the attribute keys and holding attributes satisfy the access policy, user cannot decrypt the pervious cipher text.

REFERENCES

[1] S. Roy and. Chuah, "Secure data retrieval based on cipher text policy attribute based encryption (CP-ABE) system for the DTNs," Lehigh CSE Tech. Rep., 2009.
[2] Anwar Saipulla Benyuan Liu Jie Wang,"Barrier Coverage with Airdropped Wireless Sensors Department of Computer Science, University of Massachusetts Lowell, MA 01854 USA IEEE 2008.
[3] M. Chuah and P. Yang, "Performance evaluation of content based information retrieval schemes for DTNs," in Proc. IEEE MILCOM, 2007, pp. 1–7.
[4] 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.
[5] M. Chuah and P. Yang, "Node density based adaptive routing scheme for disruption tolerant networks," in Proc. IEEE MILCOM, 2006, pp.1–6.
[6] 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.
[7] M 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.

ISSN: 2278 – 1323