Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 5.258

IJCSMC, Vol. 5, Issue. 5, May 2016, pg.100 – 104

A Survey on Security in Military Network for Data Retrieval

Suchita Ghugal[1], Mrunali Vaidya[2]
[1]M-Tech Student, Department of CSE, Ballarpur Institute of Technology(BIT), Gondwana University, Ganchiroli, Maharashtra, India
[2]Assistant Professor, Department of CSE, Ballarpur Institute of Technology(BIT), Gondwana University, Ganchiroli, Maharashtra, India
[1] suchitaghugal@gmail.com; [2] mrunalidhawas@gmail.com

ABSTRACT: In military environment the mobile nodes likely to suffer from many network connectivity problems. The DTN is best solution which allows mobile nodes to interact with each other in secure manner. Challenging problems in this scenario are the enforcement of authorization policies and secure data retrieval. The CP-ABE (ciphertext policy-attribute based encryption) is a guaranteeing cryptographic approach for access control issues. Hence if hacker hacks the message he cannot know which data has been transferred. In this paper we have discussed about disruption tolerant network and many more issues regarding to data retrieval.

Keywords:- DTN, CP-ABE, tolerant network.

1. INTRODUCTION

Nodes in military environments likely to suffer from challenging network connectivity problems. Disruption tolerant network (DTN) technologies are becoming successful solutions that allow wireless devices carried by soldiers to interact with one another and access the confidential information or command reliably by exploiting external storage nodes. Disruption tolerant network (DTN) technologies are becoming successful solutions that allows node to communicate with each other in such networking environments [1]-[3]. Usually, when there is no end to end connection between source and destination pair, then messages from the source node may need to wait for the intermediate nodes for a substantial amount of time until the connection would be

properly established. The concept of attribute based encryption (ABE) is a good approach that fulfills the requirements for secure data retrieval in DTNs. Especially, ciphertext-policy ABE (CP-ABE) provides a scalable way of encrypting data such that the encryptor defines the attribute set that the decryptor needs to possess in order to decrypt the ciphertext [4]. Hence, as per security policy different users try to decrypt data.

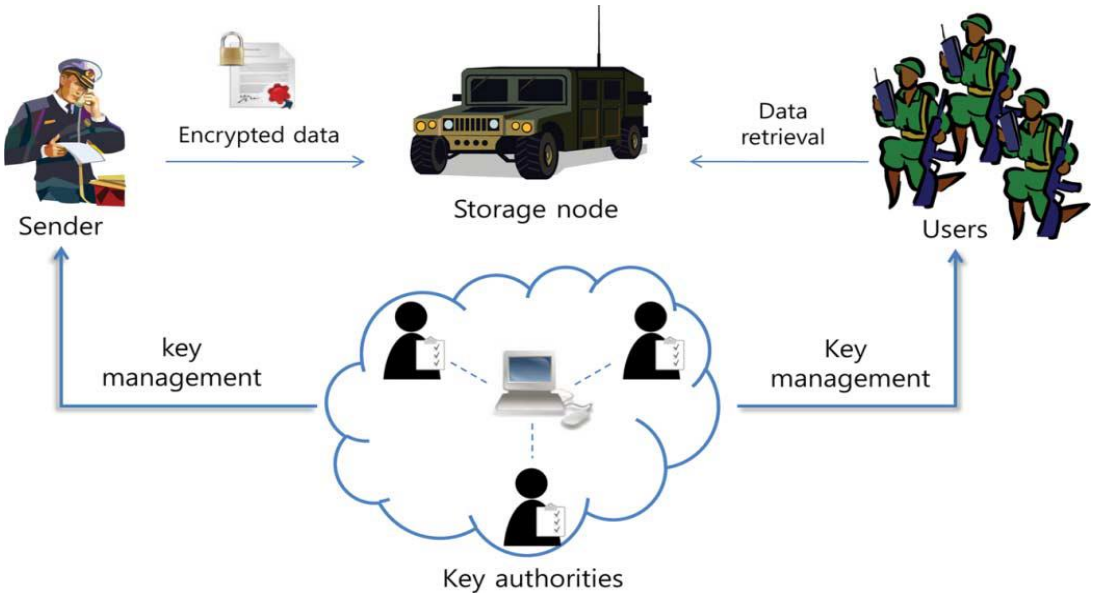

Fig. Architecture of DTN

2. EXISTING SYSTEM

In ABE the requirements for secure data retrieval in DTNs get fulfilled. ABE features a mechanism that enables an access control over encrypted data using access policies and attributes among private keys and cipher texts. CP-ABE provides a proper way of encrypting data such that the encryptor defines the attribute set that the decrypt or needs to possess in order to decrypt the cipher text [5]. According to different security policies users are allowed to decrypt different pieces of data.

2.1 Disadvantages of existing system:

1. For several security and privacy challenges in DTN ABE is used. Since some users may change their associated attributes at some point or some private keys might be compromised, key revocation for each attribute is necessary in order to make systems secure.
2. This issue is even more difficult, especially in ABE systems, since each attributes are shared by multiple users.

3. Another is key escrow problem. In CP-ABE, the key authority generates private keys of users by applying the authority's master secret keys to user associated set of attributes [6].
4. The coordination of attributes issued from different authorities. When many authorities manage and issue attribute keys to users independently with their own master secret keys, it is very hard to define fine-grained access policies over attributes issued from different authorities.

3. PROPOSED SYSTEM

In this paper, we propose an attribute-based secure data retrieval scheme using CP-ABE for decentralized DTNs [7]-[8]. The proposed scheme features the following achievements. Immediate attribute revocation enhances backward/ forward secrecy of confidential data by reducing security issues. Encryptors can define a fine-grained access policy using any single access structure under attributes issued from any chosen set of authorities. 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 secret keys. The 2PC protocol disallows the key authorities from obtaining any master secret key information of each other such that none of them could generate set of keys [9]-[10].

4. LITERATURE SURVEY

A multiauthority CP-ABE scheme is for secure data retrieval in decentralized DTNs. Each attribute key of a user can be updated individually and immediately. Thus, the scalability and security can be enhanced in the proposed scheme. DTN architectural design-related issues explored from the deep-space Inter-Planetary Networking (IPN) architecture, mother of all subsequent DTN architectural developments and extend to cover the most important recently emerging terrestrial DTN prototypes and their pertaining architectural enhancements.

4.1 The Inter-Planetary Networking (IPN):

DTN architectural designs and explorations dated ever since the first Inter-Planetary Internet (IPI) project started [11]. After thorough examination, researchers concluded that the astronomical mechanics of the solar system and the immutable characteristics of the outer space render end-to-end operation of standard Internet protocols in such environments infeasible. In an attempt to overcome this, they pictured the extraterrestrial world as the catholic network of ordinary Internets.

4.2 Delay / Disruption- Tolerant Networking:

The presented a thorough investigation of critical DTN protocol design-related issues and proposed the Delay-Tolerant Networking overlay architecture as a comprehensive solution to the DTN inter-operability problem. The majority of the studies performed by the DTNRG that followed addressed a few problems raised in Other issues such as error detection, custody transfers, congestion control, buffer management, addressing, fragmentation, naming and binding were left untouched by the DTNRG [12]-[13].

4.3 Content-Based Information Retrieval Scheme:

In this content-based information retrieval scheme they studied the scenario where the queries have multiple attributes [14]-[16]. In addition, we compare the effectiveness of using opportunistically encountered nodes or specially deployed index and storage points (ISPs) for storing replicated data items or indices of the data items.

4.4 Scalable Secure File Sharing:

Plutus: Scalable secure file sharing on untrusted storage explained the mechanisms in Plutus to reduce the number of cryptographic keys exchanged between users by using file groups, distinguish file read and write access, handle user revocation efficiently, and allow an untrusted server to authorize file writes [17]. We have built a prototype of Plutus on Open AFS. Measurements of this prototype show that Plutus achieves strong security with overhead comparable to systems that encrypt all network traffic.

4.5 Mediated CP-ABE:

In this they proposed a mediated Ciphertext-Policy Attribute-Based Encryption (mCP-ABE) which extends CP-ABE with instantaneous attribute revocation [18]. Furthermore, we demonstrate how to apply the proposed mCP-ABE scheme to securely manage Personal Health Records (PHRs).

4.6 Multiauthority Attribute Based Encryption:

In this they presented a Multi-Authority Attribute-Based Encryption (ABE) system [19]-[20]. In our system, any party can become an authority and there is no requirement for any global coordination other than the creation of an initial set of common reference parameters. A party can simply act as an ABE authority by creating a public key and issuing private keys to different users that reject their attributes. A user can encrypt data in terms of any Boolean formula over attributes issued from any chosen set of authorities. Finally, our system does not require any central authority.

5. CONCLUSION

In this survey we study various DTN technologies which are being used for secure data retrieval. In these techniques encrypted data can be kept confidential even if the storage server is untrusted; moreover, our methods are secure against many types of attacks.

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] S M. Chuah and P. Yang, "Node density- based adaptive routing scheme for disruption tolerant networks," in *Proc. IEEE MILCOM*, 2006, pp. 1–6.
[3] D 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 and M. Chuah, "Secure data retrieval based on ciphertext policy attribute-based encryption (CP-ABE) system for the DTNs," Lehigh CSE Tech. Rep., 2009.
[5] W. M. Chase and S. S. M. Chow, ―Improving privacy and security in multiauthority attribute-based encryption," in *Proc. ACM Conf. Comput. Commun. Security*, 2009, pp. 121–130.
[6] J. Bethencourt, A. Sahai, and B. Waters "Ciphertext-policy attribute based encryption," in *Proc. IEEE Symp. Security Privacy*, 2007, pp. 321–334.
[7] G A. Lewko and B. Waters, "Decentralizing attribute-based encryption," Cryptology ePrint Archive: Rep. 2010/351, 2010.
[8] 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
[9] D. Huang and M. Verma, "ASPE: Attribute-based secure policy enforcement in vehicular ad hoc networks," *Ad Hoc Netw.*, vol. 7, no. 8, pp. 1526–1535, 2009.
[10] 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.
[11] V. Cerf, S. Burleigh, A. Hooke, L. Torgerson, R. Durst, K. Scott, E. Travis and H. Weiss, "Interplanetary Internet (IPN): Architectural Definition," 2001.
[12] K. Fall, "A Delay-Tolerant Network Architecture for Challenged Internets," Intel Research Berkley, 2003.
[13] M. Loubser, "Delay Tolerant Networking for Sensor Networks," SICS Technical Report, ISSN 1100-3154, January 2006
[14] A. S. Pentland, R. Fletcher and A. Hasson, "DakNet: Rethinking Connectivity in Developing Nations," IEEE Computer, January 2004.
[15] M. J. Khabbaz, W. F. Fawaz and C. M. Assi, ‖Probabilistic Bundle Relaying Schemes In Two-Hop Vehicular Delay-Tolerant Networks,‖ IEEE Communications Letters, to appear, 2011.
[16] M. Chuah and P. Yang, ―Performance evaluation of content-based information retrieval schemes for DTNs,‖ in Proc. IEEE MILCOM, 2007
[17] 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.
[18] L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker, "Mediated ciphertext policy attribute-based encryption and its application," in Proc. WISA, 2009.
[19] Sribhashyam Sathvik and K.M.V Madan Kumar, ―A Strategic Review on Cipher Text Policy Attribute Based Encryption‖. 2650-2654, December 2014.
[20] M. Chase, ―Multi-authority attribute based encryption,‖ in *Proc. TCC*, 2007, LNCS 4329, pp. 515–534.

