© 2017 IJSRST | Volume 3 | Issue 2 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X

National Conference on Advances in Engineering and Applied Science (NCAEAS)
16th February 2017
In association with
International Journal of Scientific Research in Science and Technology

Secure Data Key Retrieval for Decentralized Disruption Tolerant Military Networks

Prof. Devika Deshmukh, Aditi Zade, Dhanashri Jumade, Sharvari Katyayan,
Neha Thakare, Harshada Shende
Anjuman College of Engineering and Technology, Nagpur, Nagpur, Maharashtra, India

ABSTRACT

In the Disruption tolerant network technologies have successful solutions that has wireless devices carried by soldiers to communicate and access the confidential information reliably by external storage nodes. Some of the most challenging problem in this way the enforcement of authorization system and the policies are for secure data retrieval. The Ciphertext policy based encryption has a cryptographic solution to the access control problem. The problem of applying in decentralized has several security and privacy problem with regard to the attribute key, and supplies for the different authorities. The propose a secure data retrieval scheme using 3DES for decentralized where multiple key authorities manage their attributes independently. To demonstrate how to apply the proposed system to securely and which manage the confidential data distributed in the disruption military network.

Keywords: Triple Data Encryption Algorithm, Disruption-Tolerant Network, Multiauthority, Secure Data Retrieval.

I. INTRODUCTION

This nodes in military environments such as a battlefield in a region are likely to get from intermittent network connectivity and frequent partitions. Disruption based tolerant network technologies are becoming useful solutions that make wireless devices carried by soldiers to communicate amongst themselves and access the confidential data 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 based encryption is a promising cryptographic solution to the access control issues. However, the problem of applying 3DES in decentralized introduces several security and privacy challenges with apply to the attribute revocation, key , and coordination of attributes issued from different authorities., we propose a secure data retrieval scheme using 3DES for decentralized DTNs where multiple key authorities has their attributes. To apply the proposed mechanism securely and efficiently manage the confidential data distributed in the disruption military network.

II. METHODS AND MATERIAL

1. Existing

Military applications need increased protection of confidential data including access method It is desirable to provide differentiated access services Data access policies are defined over user roles, which are managed by the key authorities. Wireless Sensor Networks are based on elementary sensors that detect the occurrence of particular events in a monitored area. [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* Wireless Sensor Networks applications will find the border surveillance applications. The first aim of this applications is to monitor a country border and detect the presence of intruders in border line. [2] M. Chuah and P. Yang, “Node density-based adaptive routing scheme for disruption tolerant networks," in *Proc. IEEE MILCOM, 2006, pp.* 1–6. In this paper, the effects of natural factors on dynamic deployment scheme Wireless Sensor Networks based solution providing the surveillance. Parameters such as the wind effect, and velocity of the airplane from which the sensors are thrown are put to optimize the area coverage and Wireless Sensor Networks connectivity. [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. 3 09–323. Then, the propose models that evaluate the quality of connectivity and coverage of the deployed network and allow planning of a border solution. [9] D.HuangandM.Verma,"ASPE:Attrib ute-based secure policy enforcement in vehicular ad hoc networks," *Ad Hoc Netw.*, vol. 7 Integrity and authentication is necessary to check sensor nodes to detect modified, injected packets. With the safety critical applications require authentication, it is wise to use it even for the applications since otherwise the owner of the sensor network to get the wrong of the sensed thus making inappropriate decisions. However, authentication alone does not solve the problem of node takeovers Hence authentication system should be "collective" and aim at securing the entire network. [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.

Guidelines For Manuscript Preparation

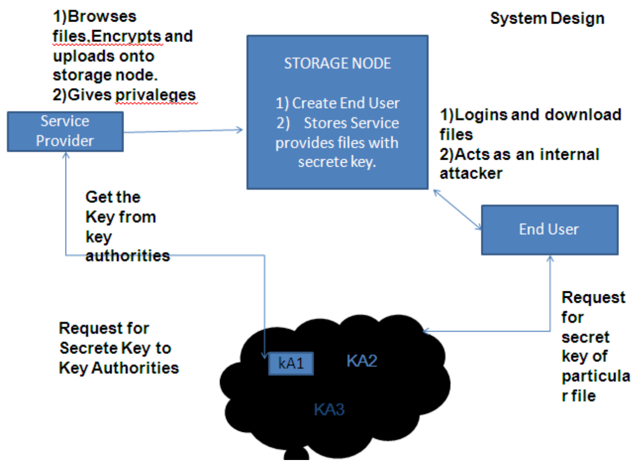

1)Browses files.Encrypts and uploads onto storage node.
2)Gives privaleges
System Design
STORAGE NODE
1) Create End User
2) Stores Service provides files with secrete key.
Service Provider
1)Logins and download files
2)Acts as an internal attacker
Get the Key from key authorities
End User
Request for Secrete Key to Key Authorities
kA1
KA2
KA3
Request for secret key of particula r file

Figure 1. Key generation

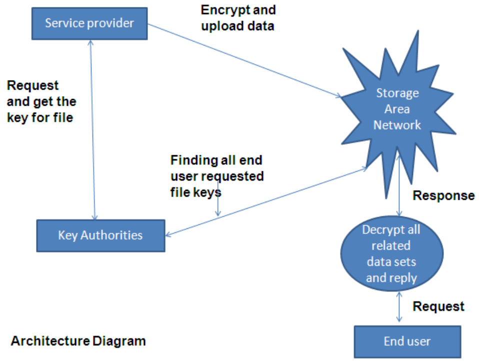


Figure 2. Data Encryption

Implementation of the project when the design is turned out into a working system. It can be considered to be the most important stage in achieving a successful new system and giving the user, confidence that the new system will work and be effective. The implementation involves careful planning, investigation of the existing system and it the implementation, designing of methods to get changeover and check of changeover methods.

2. Modules Description

A. Key Authorities

They are key generation that generate secret parameters for 3des. The key authorities consist of a central authority and number of local authorities. That there are secure and reliable communication channels between a central authority and each authority during the initial key and generation time . Each authority manages different attributes and issues corresponding attribute keys to users. They give differential rights to individual users based on the users attributes. The key authorities are assumed to be honest. That has honestly execute the assigned tasks in the system they would have information of encrypted contents as much as possible.

B. Storage Nodes

This is an entity values that stores data from senders and provide corresponding access to users. Similar to the previous schemes, we also assume the storage node to be semi trusted that is honest but curious .

C. Sender

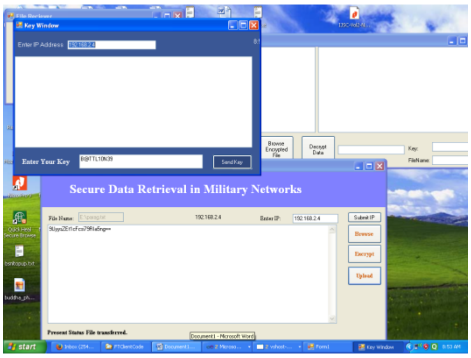
This is an entity who owns confidential data and wants to store them into the external data storage node for simplicity of sharing or for reliable delivery to users in the severe networking environments. A sender is responsible for defining access policy and implementing it on its own data by encrypting the data under the policy before storing it to the storage node.

D. User

This is a mobile node who want to access the data stored at the storage node. If user owns the set of attributes satisfying the access policy of the encrypted data defined by the sender, and is not invalidate in any of the attributes, then he will be able to decrypt the ciphertext and obtain the data. Cipher text method is one of the techniques for encrypting the data into some format which cannot be understood by anyone except the sender and the one who is the authorized user of data so even if the data gets leaked, because of mingle of words, it can't be understood by unauthorized users. In this cryptographic method, they are two steps, encryption and decryption. Sender of the node share the information from one to another in the network and share the message in the format of intermixed data with the help of private or public key which was called encryption. Another one is decryption where the receiver of the node decrypts the data or removes the intermixed words with the help of the private or public key. Then the message will show clearly to the receiver node.

3. DES with MD5 ALGORTHIM

3DES encrypts a 64-bit block of plaintext to 64-bit block of ciphertext. It uses a 128-bit key. The algorithm has of eight identical rounds and a half round final transformation. There are 216 possible 000000000000000, 111111111111111. Each operation with the set of possible 16-bit blocks is an algebraic group. 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.



Enter IP Address 192.168.2.4

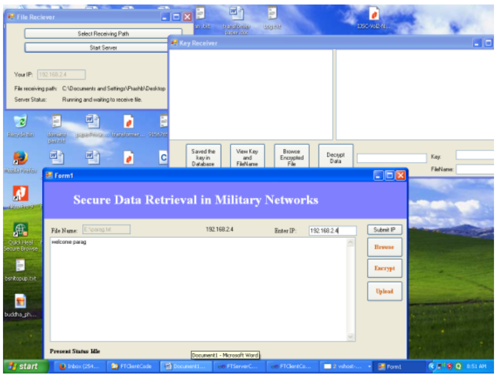
Enter Your Key B@TTL10N39

File Name: E:\parag.txt 192.168.2.4 Enter IP: 192.168.2.4

9UjyuZEt1cFcsi79RIa5ng==

Present Status File transferred.

Figure 3. User key Authorization



Your IP: 192.168.2.4

File receiving path: C:\Documents and Settings\Prashb\Desktop

Server Status: Running and waiting to receive file.

File Name: E:\parag.txt 192.168.2.4 Enter IP: 192.168.2.4

welcome parag

Present Status Idle

Figure 4. Secured Data retrieval system

Confidentiality: In order to protect data and communication exchanges between sensor nodes it is important to guarantee the secrecy of messages. In the sensor network case usually achieved by the use of symmetric cryptography or public key cryptography in general is considered too expensive. However, while encryption protect against all outside attacks, it does not protect against inside attacks, as an attacker can use recovered cryptographic key material to successfully eavesdrop, impersonate or participate in the secret communications of the network. While confidentiality guarantees the security of communications inside the network it does not prevent the misuse of information reaching the base station. Hence, confidentiality must also be coupled with the right control policies authorized users can have access to confidential information.

Integrity and Authentication: Integrity and authentication is necessary to enable sensor nodes to detect modified, injected, packets. While it is clear those safety-critical applications authentication, It is still wise to use it even for the rest of applications. Since the owner of the sensor network may get the wrong picture of the sensed world thus making inappropriate decisions. However, authentication alone does not solve the problem of node takeovers as compromised nodes can still authenticate themselves to the network. Hence authentication system should be “collective” and aim at securing the entire network.

III. CONCLUSION

The corresponding attribute group keys are updated and delivered to the justifiable assigned group members securely (including the user). In addition, all of the components encrypted 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 pervious ciphertext.

IV. 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. 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. 3 09–323.

[8]. N. Chen, M. Gerla, D. Huang, and X. Hon g, "Secure, selective group broadcast in vehicular networks us ing dynamic attribute based encryption," in Proc. Ad Hoc Netw. Worksho p, 2010, pp. 1–8.

[9]. D.HuangandM.Verma,"ASPE:Attrib ute-based secure policy enforcement in vehicular ad hoc net works," Ad Hoc Netw., vol. 7

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

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

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

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