A Cumulative study of DTN network for secure data transmission

Siddhesh Pande, Pankaj Sharma, Pritesh Soni, Aniket Shrimawale

(Department of Computer Engineering, SKN-SITS College of Engineering, Pune University, India)

ABSTRACT

For any country securing military strategies is most important aspect. Conventionally, interceptions and security risks for military communications are exceeded due to less secured data retrieval and less use of DTNs. Evaluating the present strategies nearer to this system we came aroundproducts like TASMUS and SBSP. In TASMUS Bulk Encryption Equipment provides secure data communication while SBSP established framework for bundle and delivery of bundle by adopting B-Cipher suite. They lacked in case where user changed their attributes which lead to compromisation of private keys and tamper detection is required to detect any kind of hostility. Key escrow is another major drawback. This paper puts forward an idea of sending text files with strong reverse circle cipher encryption technique and Time based unique key generation.

Keywords: Reverse circle cipher encryption, DTN, Key escrow, CP-ABE, Data tampering.

1. INTRODUCTION

Cipher text-Policy Attribute-Based Encryption (CP-ABE) is an identity based encryption. It makes use of one public key and a master private key. CP-ABE uses expressive rules for private key to decrypt cipher text. Private keys generated using this methodology makes is based on multiple attributes of user.

The proposed Reverse Circle Cipher exploits benefits of confusion and diffusion by using reversal transposition and circular substitution. This scheme uses an arbitrarily variable key length coupled with an arbitrary reversal factor.

Key generated in the system takes in multiple attributes from users. The attributes generated are changes with time as they are based on present state of the user like his geo-location, timestamp, etc. Multiple attributes to generate key makes it much harder for de-authenticated user to access data. A user can decrypt information only if its attributes are satisfied by the access policy.

Due to noise in communication and intruders, data communicated may get prone to unwanted changes called data tampering. Data tampering has zero tolerance in military where security is the key aspect of all strategies. System provides a way to detect tampering in the data communicated. Tampering detection in this system uses character ASCII identification and ASCII transposition.

The proposed system use provides a way to communicate data within Disruption Tolerant Network by encrypting data using reverse circle cipher. Users taking part in communication are provided authentication by providing them a key. Key generated in many present systems uses single attribute which is more prone to intrusion. Key generated in the present system will use multiple attributes from user. In this system key generation authority is a third party. It allows data to be sent to single user or a group of users. To generate key for a group of users attributes common to the members of group are used. All the key generation requests are only made to the Key Authority.

Key authority is also given the responsibility of updating key based on the current attributes of user. This helps in overcoming backward-forward secrecy. Earlier Backward-forward secrecy was an easy way to hack into network. Updating key on the basis of present attribute allows free mobility to users without affecting the data communication and its security. System provides security to tampered data by detecting data tampering.

This paper first goes through some past accomplishment in the given field in literature survey. Then it provides conclusion to the paper, moving on to references used for this paper.

2.LITERATURE SURVEY

DTN technologies are designed to enable nodes in environments like frequent partitions and intermittent connectivity which can be battlefield and disaster recovery scenarios.[5]Provides two unique specifications of CP-ABE scheme are:(1)The incorporation of attributes which are dynamic and changing the value over time. And (2)Revocation Feature.[5]also states that CP-ABE provides a flexible fine-grained access control such that the encrypted contents can only be accessed by authorized users,in which each user is corporate with set of attributes based on which the user's private key is generated.

[6]Provides idea of enhancement of the CP-ABE scheme with efficient revocation. The problem revocation in public key encryption scheme has been well studied [5]. Efficient revocation of certificates has been an active topic in the past several years [5]. CP-ABE can provide a perfect solution to an access control system by considering, efficient distributing, expressive access control and data confidentiality[6].After evaluation of [6]three aspects for designing CP-ABE are analyzed: First, system manager only associates user secret

ISSN: 2278 – 1323

keys with different sets of attributes instead of individual characteristics. The fuzzy identities therefore encumber the system revocation on one specified user; second, users' individuality are taken place by several common attributes, and thus revocation on attributes or attribute sets can not accurately exclude the users with misbehaviours; third, the system must be secure against collusion attack from revoked users even though they share some common attributes with non-revoked users. Hence we can say that in [6] we studied the feasible revocation
operations in CP-ABE scheme: single attribute revocation, attribute set revocation and unique identifier revocation.

Attribute Based Encryption (ABE) is a type of encryption which allows users to encrypt and decrypt message based on their attributes. This paper focuses on designing ABE schemes with algorithm of fast decryption. It also contributes an 'unbounded' key-policy ABE(KP-ABE) that requires constant number of pairing to decrypt any given message written in ciphertext. It further presents 'Key storage' and a generalized decryption algorithm that allows each user to independently tweak their settings for decryption in a spectrum ,from GPSW(i.e.short keys,slow decryption) to KP-ABE(ie. longer keys,fast decryption).

[7]states scheme for constructing a Ciphertext Policy Attribute based Encryption with hidden access policy and provide security under the Decisional Diffie-Hellman assumption. [7]contributed the work in which access policy can be expressed using AND, OR boolean operators, so that it is possible to express the access policy effectively. Each attribute ai in the access policy can take multiple values. The access policy can be represented by an n-ary tree, the leaf nodes represents the attribute present in the access policy, interior nodes represents the AND, OR operators. Each attribute in the leaf node can take multiple values. The value assigned for the leaf node by the secret sharing method will be distributed to these multiple values.it is not necessary to put all the attributes [7]in the access policy. [7]proposed an Attribute based encryption which preserves the privacy of the access policy, specified by the encryptor.

[8]Key escrow is major problem in network security. When third party (key authority) is hijacked it makes difficult to maintain security and integrity of data flowing through network. Identity-basedcryptography (IBC) is new tool introduced to secure ad hoc network. Trust authority (TA) is viewed as a key escrow it is property that every Identity Based Schemes (IBC) possessed. Key escrow in ad hoc network differs from that in other networks. New model is introduced where TA (Trust authority) uses spy nodes that acts as the network sniffer viewing and recording every communication and reporting back to the Trust Authority (TA). In this way key escrow is prevented by Trust Authority (TA).

[9]In 1998 new kind of cryptography concept was introduced called as proxy re-encryption. Proxy re-encryption is simple concept which uses the simple encryption. In states that, A's encrypted data with its own public key can be transformed by proxy to open the data under B's decryption key. In 2007 new concept was introduced in re-encryption which can re-encrypt the cipher text in CBE (certificate based encryption)and can be decrypted in identity based setting(IBE).As we are using IBE in re-encryption technique so there will be the key escrow problem. As a result key escrow problem is not avoidable in re-encryption from CBE to IBE.

3.CONCLUSION

All the respected studies in this paper clearly indicates many flaws in the existing systems. So to counter attack this, proposed system performs a detailed research on DTN, reverse circle cipher encryption, ABE, CP-ABE.

So the mentioned work of our ideaDTN technologies are becomingsuccessful solutions in military applications that allow wireless devices to communicatewith each other and access the confidential information reliably by exploiting external storage nodes. CP-ABE is a scalablecryptographic solution to the access control and secure data retrieval issues. We proposed a secure and efficient data retrieval method usingCP-ABE 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. In addition,thefine-grained key revocation can be done for each attribute group. We demonstrate how to apply the proposed mechanism to securely and efficiently manage the confidential data distributed in the disruption-tolerant military network.

4.REFERENCES

[1] "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data", Vipul Goyal, Omkant Pandey, Brent Waters, International Journal of network security, vol.15, July 2007.

[2] "Attribute-Based Encryption with Fast Decryption", Susan Hohenberger and Brent Waters, Theor.comp.sci.,422:15-38,2013.

[3]"Study of Various Cryptographic Algorithms", Mini Malhotra, Aman Singh,International Journal of Scientific Engineering and Research(IJSER), Vol. 1 issue 3, Nov. 2013.

[4] "Attribute-Based Encryption With Verifiable Outsourced Decryption", Junzuo LaiDeng, R.H.Chaowen Guan , Jian Weng, Information forensics and security, IEEE transaction, vol. 8 issue 8, July 2013.

ISSN: 2278 – 1323

[5] "Secure data retrieval based on ciphertext policy attribute based encryption system for DTNs", S. Roy, M. Chauh, Lehigh University, 2009.

[6] " Ciphertext policy attribute based encryption", Waters B., Sahai A., Bethencourt J., IEEE Symposium on security and privacy, pp. 321-334, 2007.

[7] " Ciphertext policy attribute based encryption with anonymous access policy", Cheung L., K. Kuppusami,17th ACM conference on communication security, 2011.

[8] " Limitations of key Escrow in Identity based Schemes in Ad-Hoc networks", Hoeper K., Guang Gong, Security and privacy for emerging areas in communication network, IEEE, pp 403-405, Sept. 2005.

[9] "How to solve Key escrow problem in proxy Re-encryption from CBE to IBE", Ke Niu, Xu An Wang, Minqing Zhang, 1st International workshop on Database technology and applications, IEEE, pp 95-98, April 2009.

[10] "Reverse Circle Cipher for personal and network security", Ebenezer R.H.P, Isaac, Joseph H.R. Isaac, J. Visumathi, IEEE symposium on computer and communication security, 2013.

[11] "Enforcing reverse circle cipher for Network security using Multirotational Technique", Sajjade Zeba S., Gupta Aruna K., International journal of Advanced Research in computer science and software engineering, Vol. 4 Issue 3, March 2014.

ISSN: 2278 – 1323