International Journal of Innovative Research in Advanced Engineering (IJIRAE) ISSN: 2349-2763
Issue 06, Volume 3 (June 2016) www.ijirae.com

COLLOBORATIVE APPROACH for SECURING DATA RETRIEVAL SCHEME BASED On TRIPPLE DES with MD5 for DECENTRALIZED DISRUPTION TOLERANT MILITARY NETWORK

Ruchi Rajkumar Bajpai
Department of Computer Science & Engineering,
Rajiv Gandhi College of Engineering,
Research &Technology, Chandrapur-442401

Prof. P.S. Kulkarni
Department of Information Technology,
Rajiv Gandhi College of Engineering
Research &Technology, Chandrapur-442401

Abstract— Disruption tolerant network 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 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 3DES with MD5 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.

Keywords — Access control, attribute-based encryption (ABE), disruption-tolerant network (DTN), triple data encryption standard (3DES), message digest algorithm (MD5)

I. INTRODUCTION

Mobile nodes in military environments such as a battlefield or hostile regions 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 CP-ABE in decentralized DTNs introduces several security and privacy challenges with regard to the attribute revocation, key escrow, and co-ordination of attributes issued from different authorities. We propose a secure data retrieval scheme using 3des with MD5 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.

II. PROBLEM DEFINATION

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

III. PROPOSED METHOD

To increase the security level this proposed scheme overcomes the limitation. The proposed enhanced scheme includes Triple DES and MD5.Triple DES (Variant of DES) strengthens the security of data transmission in military network. Reason behind for selecting triple DES rather than Double DES is that in double DES algorithm the key used for encryption and decryption is suspected to meet-in-middle attack. In addition to this MD5 to verify the integrity of the message. Use of message digest algorithm in combination of cryptographic algorithm provides strength in security of data transmitted in military network. Here we specify different modules of envision system.

I. KEY AUTHORITIES

There are key generation centres that generate public/secret parameters for 3des. The key authorities consist 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.

© 2014- 16, IJIRAE- All Rights Reserved

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.

II. 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

III. SENDER

This is an entity who owns confidential messages or data (e.g. a commander) and wishes to store them into the 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 (attribute based) access policy and enforcing it on its own data by encrypting the data under the policy before storing it to the storage node.

IV. 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 **3DES 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 central authority and the local authorities engage in the arithmetic 2PC protocol with master secret keys of their own and issue independent key components to users during the key issuing phase. 2PC protocol 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.

IV.METHODOLOGY

We propose an attribute-based secure data retrieval scheme using 3des with md5 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, encryptions 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 (2PC) protocol among the key authorities with their own master secrets. The 2PC protocol deters 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.

V. 3DES WITH MD5 ALGORITHM

3DES encrypts a 64-bit block of plaintext to 64-bit block of ciphertext. It uses a 128-bit key. The algorithm consists of eight identical rounds and a "half" round final 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.

- ***Sender Side Encryption Algorithm***
  1. *Take a file packet [N]*
  2. *Encrypt the plaintext blocks using single DES with E key K_1.*
  3. *Now decrypt the output of step 1 DP using single DES with key K_2.*
  4. *Finally, encrypt the output of step 2 using single DES with key K_3.*
  5. *The output of step 3 is the ciphertext. (CT)*
  6. *128 key by md5 (MD) KD*
  7. *CT= N K_3 (DP K_2(E K_1))*
  8. *Iblock= CT+KD*
  9. *Iblock is send to battalion receiver*

Triple DES as an encrypt process, it is possible to use a 3TDES (hardware) implementation for single DES by setting K_1, K_2, and K_3 to be the same value. This provides backwards compatibility with DES. Second variant of Triple DES (2TDES) is identical to 3TDES except that K_3 is replaced by K_1.

© 2014- 16, IJIRAE- All Rights Reserved

In other words, user encrypts plaintext blocks with key K_1, then decrypt with key K_2, and finally encrypt with K_1 again. Total I block Length is 192 bits Values returned by a hash function are called **message digest** or simply **hash values**.

- It is a 128-bit hash function.
- MD5 digests have been widely used in the software world to provide assurance about integrity of transferred file.

➢ ***Receiver Side Decryption Algorithm***

1. *Received Iblock= CT+KD*
2. *First and second secret keys or second and third secret keys are the same*
3. *Whichever key.*
4. *c = E3 (KD1 (K_1 (N))) = E3(N)*
5. *c = E3(KD3(K_2 (N))) = K_2 (N)*
6. *It is possible to use 3DES cipher with a secret 128 bit key.*
7. *In this case first and third secret keys are the same.*
8. *c = K 1(KD2(K1(N))*
9. *If key match data decryption*
10. *m = D1 (K_2(KD3(c)))*

I. Confidentiality

In order to protect sensed data and communication ex-changes between sensor nodes it is important to guarantee the secrecy of messages. In the sensor network case this is usually achieved by the use of symmetric cryptography as asymmetric or public key cryptography in general is considered too expensive. However, while encryption protects against outside attacks, it does not protect against inside attacks/node compromises, as an attacker can use recovered cryptographic key material to successfully eavesdrop, impersonate or participate in the secret communications of the network. Furthermore, 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 so that only authorized users can have access to confidential information.

II. Integrity and Authentication

Integrity and authentication is necessary to enable sensor nodes to detect modified, injected, or replayed packets. While it is clear that safety-critical applications require authentication, it is still wise to use it even for the rest of applications since otherwise 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 mechanisms should be “collective” and aim at securing the entire network. In particular, the following requirement must be supported by the key management scheme, in order to facilitate data aggregation and dissemination process:

I. DATA AGGREGATION

Data aggregation is possible only if intermediate nodes have access to encrypted data so that they can extract measurement values and apply to them aggregation functions. Therefore, nodes that send data packets toward the base station must encrypt them with keys available to the aggregator nodes.

II. DATA DISSEMINATION

Data dissemination implies broadcasting of a message from the aggregator to its group members. If an aggregator shares a different key (or set of keys) with each of the sensor within its group, then it will have to make multiple transmissions, encrypted each time with different key, in order to broadcast a message to all of the nodes. But transmission must be kept as low as possible because of their high energy consumption rate. First we focused on the establishment of trust relationship among wireless sensor nodes, and presented a key management protocol for sensor networks. The protocol includes support for establishing four types of keys per sensor node: individual keys shared with the base station, pair wise keys shared with individual neighbouring nodes, cluster keys shared with a set of neighbours, and a group key shared with all the nodes in the network. We showed how the keys can be distributed so that the protocol can support in network processing and efficient dissemination, while restricting the security impact of a node compromise to the immediate network neighbourhood of the compromised node. Applying the protocol makes it really hard for an adversary to disrupt the normal operation of the network.

© 2014- 16, IJIRAE- All Rights Reserved

VI. RESULT AND DISCUSSION

The results of the proposed scheme for cryptographic decentralized network are summarized in Table 1 which shows a summary of the topics and concepts considered for each approach. As it is shown in Table 1, most of the approaches discussed identify, classify, analyse, and list in below table. By analysing the scientific discipline algorithms, the subsequent results generated. The subsequent table characteristic precedes the insecure problems. Thus we have a tendency to be victimization the effective authentication decides to give stronger security for each network.

CHARACTERISTICS	EXISTING SCHEME	PROPOSED SCHEME
PLATFORM	Centralized network	De-Centralized network
KEYS USED	Same key is used for encryption and Decryption Purpose.	Authorization key used for encryption & decryption but additional authentication key is used
SCALABILITY	It is scalable algorithm due to varying the key size.	Symmetric and Asymmetric 64- bit key, 128-bit Symmetric key
SECURITY APPLIED TO	Both providers and client side	- Key distribution problem solved - Brute force attack problem is somehow solved because key size is increased
AUTHENTICATION TYPE	Key authentication used	Key authentication and network IP is used - use some advanced technique for encryption of file
SECURITY	Single encryption used	Use Triple DES (with 2- keys, MD5 hybrid encryption and authentication also used

In our project security is combination of more algorithm than base paper still requires less time to. In our project to enhance the security we use combination of algos'

- 3DES
- MD5

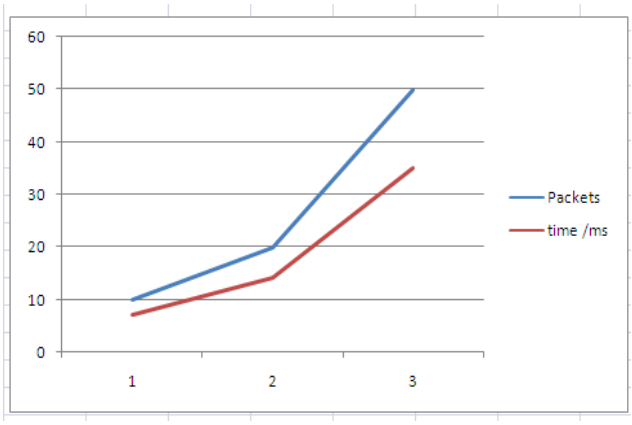

Fig. Packet Delivery Ratio

VII. CONCLUSION

The corresponding attribute group keys are updated and delivered to the valid attribute 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.

ACKNOWLEDGMENT

We would like to thanks Department of Computer Science & Engineering, RCERT Chandrapur for providing infrastructure and guidance to understand the security of Decentralized Disruption Tolerant Military Network..

© 2014- 16, IJIRAE- All Rights Reserved

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, "Message ferry route design for sparse ad hoc networks with mobile nodes," in Proc.ACMn Mobi Hoc, 2006, pp. 37–48.
[4]. S. Roy and M. Chuah, "Secure data retrieval based on cipher text policy attribute-based encryption (CP-ABE) system for the DTNs," LehighCSE Tech. Rep., 2009.
[5]. M. Chuah and P. Yang, "Performance evaluation of content-basedinformation 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.
[7]. L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker, "Mediated cipher text-policy attribute-based encryption and its application," in Proc. WISA, 2009, LNCS 5932, pp. 309–323.
[8]. Junbeom Hur and Kyungtae Kang, Member, IEEE, ACM "Secure Data Retrieval for Decentralized Disruption-Tolerant Military Networks"- IEEE/ACM TRANSACTIONS ON NETWORKING, VOL. 22, NO. 1, FEBRUARY 2014.
[9]. 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
[10]. 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.
[11]. A. Lewko and B. Waters, "Decentralizing attribute-based encryption," Cryptology ePrint Archive: Rep. 2010/351, 2010.
[12]. A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Proc. Eurocrypt, 2005, pp. 457–473.
[13]. 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.
[14]. J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute based encryption," in Proc. IEEE Symp. Security Privacy, 2007, pp. 321– 334
[15]. R. Ostrovsky, A. Sahai, and B. Waters, "Attribute-based encryption with non-monotonic access structures," in Proc. ACM Conf. Comput. Commun. Security, 2007, pp. 195–203.
[16]. S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute based data sharing with attribute revocation," in Proc. ASIACCS, 2010, pp.261–270
[17]. A. Boldyreva, V. Goyal, and V. Kumar, "Identity-based encryption with efficient revocation," in Proc. ACM Conf . Comput.Commune. Security, 2008 , pp. 417–426
[18]. M. Pirretti, P. Traynor, P. McDaniel, and B. Waters, "Secure attributebased systems," in Proc. ACM Conf. Comput. Commun.Security, 2006, pp. 99–112.
[19]. S. Rafaeli and D. Hutchison, "A survey of key management for secure group communication," Comput. Surv., vol. 35, no. 3,pp. 309–329, 2003.
[20]. S. Mittra, "Iolus: A framework for scalable secure multicasting," in Proc. ACM SIGCOMM, 1997, pp. 277–288.
[21]. P. Golle, J. Staddon, M. Gagne, and P. Rasmussen, "A content-driven access control system," in Proc. Symp. Identity Trust Internet, 2008, pp. 26–35
[22].L. Cheung and C. Newport, "Provably secure ciphertext policy ABE," in Proc. ACM Conf. Comput. Commun. Security, 2007,pp. 456–465

© 2014- 16, IJIRAE- All Rights Reserved