www.ijiarec.com

ISSN: 2348-2079

MAR-2015

International Journal of Intellectual Advancements and Research in Engineering Computations

AN EFFICIENT AND SECURE MALICIOUS MODE DETECTION IN MILITARY NETWORKS USING REVOCATION SCHEME

*S. Anubama

ABSTRACT

Mobile nodes in military environments such as a battlefield or a hostile region 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. Cipher text-policy attribute-based encryption (CP-ABE) 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. An efficient and secure data retrieval method using CP-ABE has been proposed 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, the fine-grained key revocation can be done for each attribute group.

Index terms: Disruption-tolerant network (DTN), Cipher text-policy attribute-based encryption (CP-ABE)

INTRODUCTION

A disruption-tolerant network (DTN) is a network designed so that temporary or intermittent communications problems, limitations and anomalies have the least possible adverse impact. A disruption-tolerant network (DTN) is a network designed so that temporary or intermittent communications problems, limitations and anomalies have the least possible adverse impact. There are several aspects to the effective design of a DTN, including:

- The use of fault-tolerant methods and technologies.
- The quality of graceful degradation under adverse conditions or extreme traffic loads.
- The ability to prevent or quickly recover from electronic attacks.
- Ability to function with minimal latency even when routes are ill-defined or unreliable.

Fault-tolerant systems are designed so that if a component fails or a network route becomes unusable, a backup component, procedure or route can immediately take its place without loss of service. At the software level, an interface allows the administrator to continuously monitor network traffic at multiple points and locate problems immediately. In hardware, fault tolerance is achieved by component and subsystem redundancy.

Author for Correspondence:
*PG Scholar, Final year M. E (CSE), Ranganathan Engineering College, Coimbatore, Tamilnadu, India. Email: anubama.b.tech@gmail.com.

Graceful degradation has always been important in large networks. One of the original motivations for the development of the Internet by the Advanced Research Projects Agency (ARPA) of the U.S. government was the desire for a large-scale communications network that could resist massive physical as well as electronic attacks including global nuclear war. In graceful degradation, a network or system continues working to some extent even when a large portion of it has been destroyed or rendered inoperative.

Electronic attacks on networks can take the form of viruses, worms, Trojans, spyware and other destructive programs or code. Other common schemes include denial of service attacks and malicious transmission of bulk e-mail or spam with the intent of overwhelming network servers. In some instances, malicious hackers commits acts of identity theft against individual subscribers or groups of subscribers in an attempt to discourage network use. In a DTN, such attacks may not be entirely preventable but their effects are minimized and problems are quickly resolved when they occur. Servers can be provided with antivirus software and individual computers in the system can be protected by programs that detect and remove spyware.

As networks evolve and their usage levels vary, routes can change, sometimes within seconds. This can cause temporary propagation delays and unacceptable latency. In some cases, data transmission is blocked altogether. Internet users may notice this as periods during which some Web sites take a long time to download or do not appear at all. In a DTN, the frequency of events of this sort is kept to a minimum.

A disruption-tolerant network (DTN) is a network architecture that reduces intermittent communication issues by addressing technical problems in heterogeneous networks that lack continuous connectivity. DTN defines a series of contiguous network data bundles that enable applications. This architecture serves as a network overlay that bases new naming on endpoint identifiers.

Access control is the selective restriction of access to a place or other resource. The act of accessing may mean consuming, entering, or using. Permission to access a resource is called authorization.

Locks and login credentials are two analogous mechanisms of access control. When a credential is presented to a reader, the reader sends the credential's information, usually a number, to a control panel, a highly reliable processor. The control panel compares the credential's number to an access control list, grants or denies the presented request, and sends a transaction log to a database. When access is denied based on the access control list, the door remains locked. If there is a match between the credential and the access control list, the control panel operates a relay that in turn unlocks the door. The control panel also ignores a door open signal to prevent an alarm. Often the reader provides feedback, such as a flashing red LED for an access denied and a flashing green LED for an access granted.

The above description illustrates a single factor transaction. Credentials can be passed around, thus subverting the access control list. For example, Alice has access rights to the server room, but Bob does not. Alice either gives Bob her credential, or Bob takes it; he now has access to the server room. To prevent this, two-factor authentication can be used. In a two factor transaction, the presented credential and a second factor are needed for access to be granted; another factor can be a PIN, a second credential, operator intervention, or a biometric input.

There are three types (factors) of authenticating information:

- something the user knows, e.g. a password, pass-phrase or PIN
- something the user has, such as smart card or a key fob
- something the user is, such as fingerprint, verified by biometric measurement

The concept of attribute-based encryption was first proposed in a landmark work by Amit Sahai and Brent Waters and later by Vipul Goyal, Omkant Pandey, Amit Sahai and Brent Waters. It is a type of public-key encryption in which the secret key of a

user and the cipher text are dependent upon attributes (e.g. the country he lives, or the kind of subscription he has). In such a system, the decryption of a cipher text is possible only if the set of attributes of the user key matches the attributes of the cipher text.

A crucial security feature of Attribute-Based Encryption is collusion-resistance: An adversary that holds multiple keys should only be able to access data if at least one individual key grants access.

Attribute-based encryption (ABE) can be used for log encryption. Instead of encrypting each part of a log with the keys of all recipients, it is possible to encrypt the log only with attributes which match recipients' attributes. This primitive can also be used for broadcast encryption in order to decrease the number of keys used.

Secure Data Recovery Services is a privately held company with corporate headquarters in California, which provides data recovery services. Secure Data Recovery Services was the first data recovery company to achieve SSAE 16 Type II certification. The SSAE 16 Type II Certification is an updated version of the SAS 70 standards, which the company had also previously held. SSAE 16 reports (also known as "SOC 1" reports) retain the original purpose of SAS 70 by providing a means of reporting on the system of internal control particularly as it relates to internal control over financial reporting (ICFR).

SYSTEM ANALYSIS

The terms analysis and synthesis come from Greek where they mean respectively "to take apart" and "to put together". These terms are used in scientific disciplines from mathematics and logic to economics and psychology to denote similar investigative procedures. Analysis is defined as the procedure by which we break down an intellectual or substantial whole into parts. Synthesis is defined as the procedure by which we combine separate elements or components in order to form a coherent whole.

Systems analysis researchers apply methodology to the analysis of systems involved to form an overall picture. System analysis is used in every field where there is a work of developing something. Analysis can also be defined as a series of components that perform organic function together. An example of system analysis can be system engineering. Systems engineering is an interdisciplinary field of engineering that focuses on how complex engineering projects should be designed and managed.

EXISTING SYSTEM

The Concept of attribute based encryption is a promising approach that fulfills the requirements for secure data retrieval in DTNs. The concept of attribute-based encryption was first proposed in a landmark work by Amit Sahai and Brent Waters and later by Vipul Goyal, Omkant Pandey, Amit Sahai and Brent Waters.It is a type of public-key encryption in which the secret key of a user and the cipher text are dependent upon attributes (e.g. the country he lives, or the kind of subscription he has). In such a system, the decryption of a cipher text is possible only if the set of attributes of the user key matches the attributes of the cipher text.

A crucial security feature of Attribute-Based Encryption is collusion-resistance: An adversary that holds multiple keys should only be able to access data if at least one individual key grants access.

Attribute-based encryption (ABE) can be used for log encryption. Instead of encrypting each part of a log with the keys of all recipients, it is possible to encrypt the log only with attributes which match recipients' attributes. This primitive can also be used for broadcast encryption in order to decrease the number of keys used.

DISADVANTAGES

- Several security and privacy challenges

Eg: Since some users may change their associated attributes at some point (Moving their region) or some privated keys might be compromised, key revokation is necessary in order to make systems secure.

NETWORK ARCHITECTURE

SYSTEM DESCRIPTION AND ASSUMPTIONS

1) Key Authorities: They are key generation centers that generate public/secret parameters for CP-ABE. The key authorities consist of a central authority and

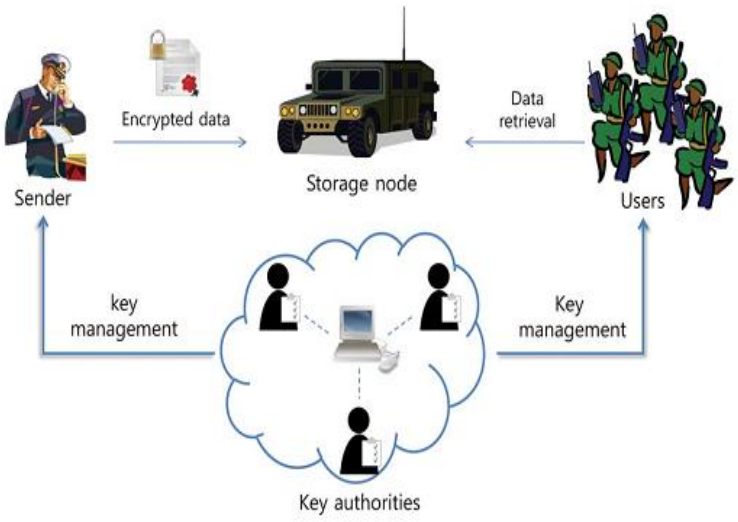
multiple local authorities. We assume that there are secure and reliable communication channels between a central authority and each local authority during the initial key setup and generation phase. Each local authority manages different attributes and issues corresponding attribute keys to users. They 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.

2) 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, and that is honest-but-curious.

3) 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' 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.

4) 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 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 cipher text 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; meanwhile, 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 arithmetic2PC protocol with master secret keys of their own independent key components to users during the key issuing phase. The 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. Thus, we take an assumption that the central authority does not collude with the local authorities (otherwise, they can guess the secret keys of every user by sharing their master secrets).

Fig System Architecture



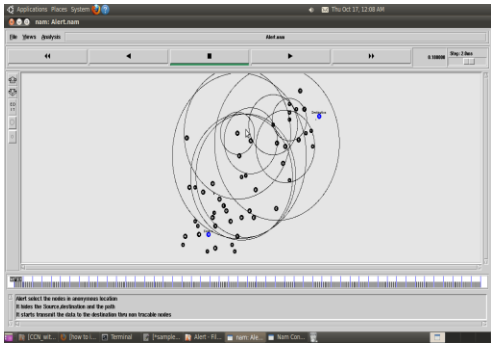
Threat Model and Security Requirements

1) Data confidentiality: Unauthorized users who do not have enough credentials satisfying the access policy should be deterred from accessing the plain data in the storage node. In addition, unauthorized access from the storage node or key authorities should be also prevented.

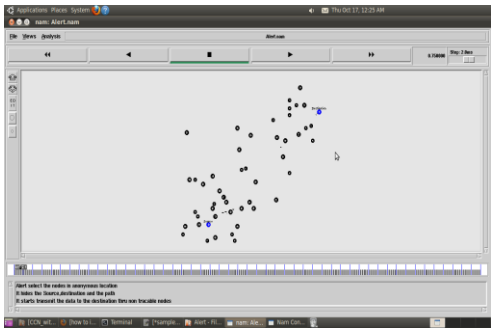
2) Collusion-resistance: If multiple users collude, they may be able to decrypt a cipher text by combining their attributes even if each of the users cannot decrypt the cipher text. For example, suppose there exist a user with attributes {"Battalion 1", "Region 1"} and another user with attributes {"Battalion 2", "Region 2"}. They may succeed in decrypting a cipher text encrypted under the access policy of ("Battalion 1" AND "Region 2"), even if each of them cannot decrypt it individually. We do not want these colluders to be able to decrypt the secret information by combining their attributes. We also consider collusion attack among curious local authorities to derive users' keys.

3) Backward and forward Secrecy: In the context of ABE, backward secrecy means that any user who comes to hold an attribute (that satisfies the access policy) should be prevented from accessing the plaintext of the previous data exchanged before he holds the attribute. On the other hand, forward secrecy means that any user who drops an attribute should be prevented from accessing the plaintext of the subsequent data exchanged after he drops the attribute, unless the other valid attributes that he is holding satisfy the access policy.

COLLUSION-RESISTANCE:



If multiple users collude, they may be able to decrypt a cipher text by combining their attributes even if each of the users cannot decrypt the cipher text alone. For example, suppose there exist a user with attributes {"Battalion 1", "Region 1"} and another user with attributes {"Battalion 2", "Region 2"}. They may succeed in decrypting a cipher text encrypted under the access policy of ("Battalion 1" AND "Region 2"), even if each of them cannot decrypt it individually. We do not want these colluders to be able to decrypt the secret information by combining their attributes. We also consider collusion attack among curious local authorities to derive users' keys.



BACKWARD AND FORWARD SECRECY

In the context of ABE, backward secrecy means that any user who comes to hold an attribute (that satisfies the access policy) should be prevented from accessing the plaintext of the previous data exchanged before he holds the attribute. On the other hand, forward secrecy means that any user who drops an attribute should be prevented from accessing the plaintext of the subsequent data exchanged after he drops the attribute, un- less the other valid attributes that he is holding satisfy the access policy. A multi authority CP-ABE scheme for secure data retrieval in decentralized DTNs. Each local authority issues partial personalized and attribute key components to a user by performing secure 2PC protocol with the central authority. Each attribute key of a user can be updated individually and immediately. Thus, the scalability and security can be enhanced in the proposed scheme.

CONCLUSION

DTN technologies are becoming successful solutions in military applications that allow wireless devices to communicate with each other and access the confidential information reliably by exploiting

external storage nodes. CP-ABE is a scalable cryptographic solution to the access control and secures data retrieval issues. An efficient and secure data retrieval method using CP-ABE is proposed 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 com- promised or not fully trusted. In addition, the fine-grained key revocation can be done for each attribute group. We demon-strata how to apply the proposed mechanism to securely and efficiently manage the confidential data distributed in the disruption-tolerant military network.

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. ACMMobiHoc, 2006, pp. 37–48.

[4]. S. Roy and. Chuah, "Secure data retrieval based on cipher text policy attribute-based encryption (CP-ABE) system for the DTNs," Lehigh's 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.

[7]. L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker, "Mediatedciphertext-policy attribute-based encryption and its application," in Proc. WISA, 2009, LNCS 5932, pp. 309–323.

[8]. 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,

[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]. A. Lewko and B. Waters, "Decentralizing attribute-based encryption,"Cryptology reprint Archive: Rep. 2010/351, 2010.