Usage of CP-ABE with Vein Pattern Matching for the Secure Transmission of Data in Militarv Networks

Deepika M[1], S Kuzhalvaimozhi[2]

[1]*M.Tech, CNE, Dept . of ISE, National Institute of Engineering, Mysuru, Karnataka, India.*
[2]*Associate Professor, Dept of ISE, National Institute of Engineering, Mysuru, Karnataka, India.*

***

Abstract-*Disruption-Tolerant Network (DTN) technologies are becoming successful solutions in military environments such as a battle-field or a hostile region where mobile nodes suffer from frequent partitions and intermittent network connectivity. DTN's allow wireless devices carried by soldiers to communicate with each other and access the confidential information by exploiting external storage nodes. CP-ABE is a best approach to deal with several privacy challenges related to storing and sharing of secret information. In this paper we are going to make secure information retrieval with CP-ABE scheme. In addition to improve the security we introduced vein pattern matching concept.*

Key Words: Attribute-based encryption (ABE), Disruption-tolerant Network (DTN), secure data retrieval, Vein pattern matching.

1. INTRODUCTION

The Wireless devices carried by the soldiers in military environments are likely to suffer from end-to-end connectivity and frequent partitions. Disruption Tolerant networks are the one which gives solutions for the above problem by allowing these mobile nodes to communicate with each other. Introduction of storage node was done by Roy [6] and Chuah [3] in order to hold the data sent by the sender to the destination whenever there is no connection between them. Many military applications require increased protection of confidential data and therefore sometimes it is desirable to provide differentiated access services by defining data access policy over the user attributes. The concept of attribute-based encryption (ABE) [9] is a promising approach the fulfils the requirement of secure data retrieval in DTN's. Attribute-Based Encryption is the one where the encryption of the message is done with the help of the attributes defined over the users. Figure 1 shows the sample of key generation centre which are composed of one central authority and multiple local authorities. Each local authority manages different attributes and issues corresponding keys to users. Whenever the sender wants to send message to the destination, he sends the message along with attributes to the key generation centre for encryption. The Attribute-based Encryption is of two types where each of them has their own way of encrypting data.

In this type of encryption, the complete encryption task is done by the central authority and the corresponding local authority where the message is encrypted with the central authority's master secret. Then the encrypted message is sent back to the sender, and then he sends it to the destination.

Fig- 1: Key Generation Centre

The disadvantage here is, since the message is encrypted with the central authority's master secret, it can also be decrypted with the same, if suppose, the central authority is compromised illegally with some other local authority then the confidential message may be leaked. To solve this problem one can go with the cipher-text policy attribute based encryption.

B.Cipher-text Policy Attribute Based Encryption

In this type of encryption the esc-row free key issuing protocol is used. Here the key-issuing protocol generates and issues user secret keys by performing a secure 2PC (Two-party Computation) protocol among the key authorities with their own master secrets.

This avoids the key authority's from obtaining any master secret information of each other and therefore none of them can generate the whole set of user keys alone.

2. LITERATURE SURVEY

2.1 Maxprop: Routing for vehicle-based disruption tolerant networks

Communication networks are traditionally assumed to be connected. However, emerging wireless applications such as vehicular networks, pocket-switched networks, etc., coupled with volatile links, node mobility, and power outages, will require the network to operate despite frequent disconnections. To this end, opportunistic routing techniques have been proposed, where a node may store-and-carry a message for some time, until a new forwarding opportunity arises. Although a number of such algorithms exist, most focus on relatively homogeneous settings of nodes. However, in many envisioned applications, participating nodes might include handhelds, vehicles, sensors, etc. These various "classes" have diverse characteristics and mobility patterns, and will contribute quite differently to the routing process. In this paper, we address the problem of routing in intermittently connected wireless networks comprising multiple classes of nodes. We show that proposed solutions, which perform well in homogeneous scenarios, are not as competent in this setting. To this end, we propose a class of routing schemes that can identify the nodes of "highest utility" for routing, improving the delay and delivery ratio by four to five times. Additionally, we propose an analytical framework based on fluid models that can be used to analyze the performance of various opportunistic routing strategies, in heterogeneous settings [2].

2.2 Node density-based adaptive routing scheme

Traditional ad hoc routing protocols do not work in intermittently connected networks since end-to-end paths may not exist in such networks. Hence, routing mechanisms that can withstand disruptions need to he designed. A store-and-forward approach has been proposed for disruption tolerant networks. Recently, several approaches have been proposed for unicast routing in disruption-prone networks e.g. the 2-hop relay approach, delivery probability based routing, and message ferrying. In our earlier paper, we have evaluated a combined multihop and message ferrying approach in disruption tolerant networks. In that paper, we assume that a special node is designated to be a message ferry. A more flexible approach is to let regular nodes volunteer to be message ferries when network dynamics mandate the presence of such ferries to ensure communications. Thus, in this paper, we design a node-density based adaptive routing (NDBAR) scheme that allows regular nodes to volunteer to be message ferries when there are very few nodes around them to ensure the feasibility of continued communications. Our simulation results indicate that our NDBAR scheme can achieve the highest delivery ratio in very sparse networks that are prone to frequent disruptions [3].

2.3 Performance evaluation of content-based information retrieval schemes for DTNs

Mobile nodes in some challenging network scenarios suffer from intermittent connectivity and frequent partitions e.g. battlefield and disaster recovery scenarios. Disruption Tolerant Network (DTN) technologies are designed to enable nodes in such environments to communicate with one another. Several DTN routing schemes have been proposed. However, not much work has been done on providing information access in such challenging network scenarios. Existing client/server paradigm for information access will not be feasible in such scenarios since end-to-end path does not exist. Thus, in this paper, we explore how a content-based information retrieval system can be designed for DTNs. There are three important design issues, namely (a) how should data be replicated and stored at multiple nodes, (b) how should a query be disseminated in sparsely connected networks, (c) how should a query response be routed back to the querying node. We first describe two data caching schemes: (a) K-copy random caching, (b) K-copy intelligent caching. Then, we describe an L-hop Neighborhood Spraying (LNS) scheme for query dissemination. For message routing, we either use Prophet routing scheme or Highest Encounter First Routing (HEFR) scheme. We conduct extensive simulation studies to evaluate different combinations of these algorithms. Our results reveal that the scheme that performs the best is the one that uses the K-copy intelligent caching combined with the LNS query dissemination and HEFR scheme [4].

2.4 Ciphertext-policy attribute-based encryption

An Attribute-Based Encryption (ABE) is an encryption scheme, where users with some attributes can decrypt ciphertexts associated with these attributes. However, the length of the ciphertext depends on the number of attributes in previous ABE schemes. In this paper, we propose a new Ciphertext-Policy Attribute-Based Encryption (CP-ABE) with constant ciphertext length. Moreover, the number of pairing computations is also constant [5].

3. EXISTING SYSTEM

The military applications require increased protection of confidential data. So, in many cases it is desirable to provide differentiated access services where data access polices are defined over user attributes managed by key authority. To achieve this Attribute Based Encryption (ABE) is used.

Limitations of Existing Systems

However, applying ABE to DTNs introduces several security and privacy challenges [6].

1. Since some users may change their associated attributes at some point (for example, moving their region), or some private keys might be compromised, key revocation (or update) for each attribute is necessary in order to make systems secure.
2. Another challenge is the key escrow problem. In CP-ABE, the key authority generates private keys of users by applying the authority's master secret keys to users associated set of attributes.
3. The last challenge is the coordination of attributes issued from different authorities. When multiple

authorities manage and issue attributes keys to users independently with their own master secrets, it is very hard to define fine-grained access polices over attributes issued from different authorities.

4. PROPOSED SYSTEM

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 plain text 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. 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 [6].

Advantages of Proposed System

An attribute based secure data retrieval scheme using CP-ABE has been proposed for decentralized DTNs. The proposed scheme features the following achievements.

1. Immediate attribute revocation enhances backward/forward secrecy of confidential data by reducing the windows of vulnerability.
2. Encryptors can define a fine-grained access policy using any monotone access structure under attributes issued from any chosen set of authorities
3. 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.

5. SYSTEM ARCHITECTURE

The system architecture of disruption-tolerant military network shown in figure 1 comprised of the following system entities [6].

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.

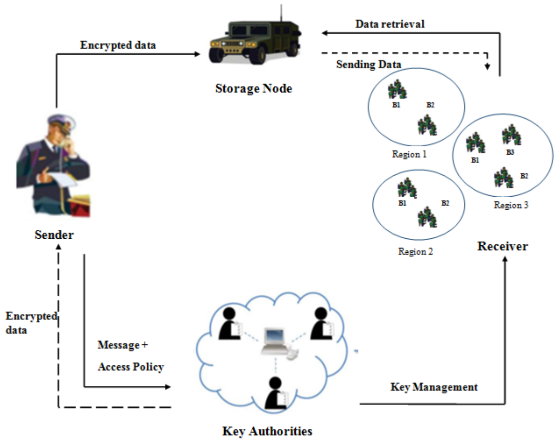

Fig-2: System Architecture

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 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. 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.
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 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 cipher text and obtain the data. In this paper we are going to implement one another module for increasing security of whole network i.e. face detection module.

5. *Vein Pattern Matching:* is a type of biometrics that can be used to identify individuals based on the vein patterns in the human figure or palm. It is to be used at the receiver end in order to make secure retrieval of information.

In this system, the usage of cipher-text policy attribute based encryption helps in defining fine-grained access policy over attributes issued from different authorities. As shown in figure 1, at the receiver side, the military environment is divided into regions say region 1, region 2, region 3..., where each region consists of some set of battalions (group of soldiers) battalion 1, battalion 2, battalion 3.... The two attributes considered here are Region and Battalion. For example, if the attributes defined over the information are "battalion 1" and "region 2", then the encrypted information is intended to the soldiers in region 2's battalion 1. But, here there is no way to securely transmit the information to the particular individual. The usage of vein pattern matching with this system helps in recognizing the individuals based on the vein patterns [8].

5.1 Working of vein Pattern matching

Vein matching is a biometric identification technique through the analysis of the patterns of blood vessels visible from the surface of the skin [7].

Working Steps:

1. Capture palm vein images.

   When a user's hand is placed on a scanner, a near-infrared light maps the location of the veins. The red blood cells present in the veins absorb the rays and show up on the map as black lines, whereas the remaining hand structure shows up as white as shown in the figure 2.

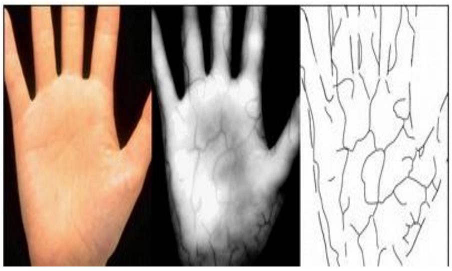

Figure 2: Capturing palm vein images

2. Maintenance of Template

The template is generated by the captured palm vein images in the previous step for authentication. Generated template should be managed by the user application.

3. Matching with the Template

   Whenever the user wants to learn the information, he needs to be authenticated first. With the help of scanner the palm/finger vein image is generated. Then the generated image is compared with the template that was stored. If they matched then that particular user gets the permission to access the information, if not, then the access to the information by that person is denied.

Advantages of vein pattern matching:

- *Accurate:* Rates for acceptance of false users or rejection of true users are among the lowest for biometric technologies, making finger vein authentication a reliable security solution. Unique vein patterns plus leading edge technology means high accuracy rates.
- *Secure:* As finger vein patterns are found internally within the body, forgery is extremely difficult.
- *Fast:* Vein pattern matching is completed within the blink of an eye, affording users a speedy authentication experience without the hassle and without the wait.
- *User-Friendly:* The vein patterns of each finger are unique, so each individual can register multiple fingers as "back-ups" for authentication purposes. Registration is possible even for sweaty, oily or dirty fingers.

6. CONCLUSION

Mobile nodes in military environments such as battlefield or a hostile region are likely to suffer from intermittent network connectivity and frequent partitions. Disruption Tolerant Network (DTN) Technologies are becoming successful solution. This paper proposes an efficient and secure data retrieval using CP-ABE for decentralized DTNs with the addition of brief idea of vein pattern matching to this system to increase the flexibility of the system in terms of privacy and security. In future, this paper can be enhanced by converting this technique into mobile application with which communication can be done more reliably.

REFERENCES

[1]. Junbeom Hur, Kyungtae Kang, "Secure Data Retrieval for Decentralized Disruption-Tolerant Military Networks," IEEE TRANSACTIONS ON NETWORKING VOL 22 NO:1 YEAR 2014 .

[2] J. Burgess, B. Gallagher, D. Jensen, and B. N. Levine, "Maxprop: Routing for vehicle-based disruption

tolerant networks," in Proc. IEEE INFOCOM, 2006, pp.

[3] M. Chuah and P. Yang, "Node density-based adaptive routing scheme for disruption tolerant networks" in Proc. IEEE MILCOM, 2006, pp. 1–6.

[4] M. Chuah and P. Yang, "Performance evaluation of content-based information retrieval schemes for DTNs" in Proc. IEEE MILCOM, 2007, pp. 17.

[5] Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in IEEE Symposium on Security and Privacy. , pp. 321–334, 2007.

[6] 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.

[7] Kamta Nath Mishra, Kanderp Narayan Mishra and Anupam Agrawal, "Veins Based Personal Identification Systems: A Review," Lehigh I.J. Intelligent Systems and Applications, 2016, 10, 68-85.

[8] Cpt. Fabio MULAZZANI, Lt.Col. Salvatore A. SARCIA, "Cyber Security on Military Deployed Networks: A Case Study on Real Information Leakage," 2011 3rd International Conference on Cyber Conflict C. Czosseck, E. Tyugu, T. Wingfield (Eds.) Tallinn, Estonia, 2011 © CCD COE Publications.

[9] 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.