ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 10, October 2014

Advanced Data Access Scheme in Disruption Tolerant Network

S.Revathi [1], A.P.V.Raghavendra [2]

P.G. Scholar, Department of Computer Engineering, V.S.B Engineering College, Karur, Tamil Nadu, India[1]

Assistant Professor, Department of Computer Engineering, V.S.B Engineering College, Karur, Tamil Nadu, India[2]

ABSTRACT: Disruption- tolerant network (DTN) technologies are considered to be the successful solutions, allow nodes to communicate with each other in the extreme networking environments. Some of the most challenging issues in this scenario are the enforcement of authorization policies and the policy updating for secure data retrieval. The concept of attribute-based encryption (ABE) is a promising approach that full fills the requirements for secure data retrieval in DTN. The existing system involves cipher text-policy attribute-based encryption (CP-ABE) presentation, which provides a scalable way of encrypting data such that the encrypter defines the attribute set that the decrypted needs to process for decrypting the cipher text. However, the problem of applying CP-ABE in decentralized DTN results in several security and privacy challenges with regards to the attribute revocation, key escrow, and coordination of attributes issued from different authorities. So, a secure data retrieval scheme is needed for using CP-ABE for decentralized DTNs where multiple key authorities manage their attributes independently. But the main drawback is that the updating of attributes is not so efficient and high complexity. In order to overcome the above cited problems I am proposing a new technique "Efficient Trust management system (ETMS)", for reducing complexity and also to improve the security in DTN. In addition to that the geographical routing is also used for finding the location of the nodes. In this method, each node analyzes other neighbour nodes, which are located in the same subtask group. While each subtask group leader (SGL) identifies other SGLs and nodes in its subtask group and followed with the peer-to-peer trust evaluation is periodically updated based on either direct observations or indirect observations. The experimental results show that, the proposed ETMS method achieves high efficiency and security with less complexity.

KEYWORDS: Disruption Tolerant Network (DTN), Secure data retrieval, Trust Management, intrusion detection, Attribute Based Encryption

I.INTRODUCTION

In many military network environments, connections of wireless devices carried by soldiers may be temporarily disconnected by environmental factors, jamming and mobility, especially when they operate in terrestrial environments. Disruption- tolerant network (DTN) technologies are becoming successful solutions that allow nodes to communicate with each other in these extreme terrestrial environments. Typically, when there is no end-to-end connection between a source and a destination pair, the messages from the source node may need to wait in the intermediate nodes for a substantial amount of time until the connection would be eventually established.

II.BACKGROUND AND MOTIVATION

Disruption Tolerant Networking is a networking architecture that is designed to provide communications in the most unstable and stressed environments, where the network would normally be subject to frequent and long lasting disruptions and high bit error rates that could severely degrade normal communications. The storage nodes are introduced in DTNs where data is stored or replicated such that only authorized mobile nodes can access the necessary information quickly and efficiently. Many military applications require secure data exchange between mobile nodes including access control methods that are cryptographically enforced. 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. For example, in a disruption-tolerant military network, a commander may store confidential information at a storage node, which should be accessed by members of "Troop 1" who are participating in "Region 2." In this case, it is a reasonable assumption that multiple key authorities are likely to manage their own dynamic attributes for soldiers in their deployed regions or echelons, which could be frequently changed. To refer to this DTN

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 10, October 2014

architecture where multiple authorities issue and manage their own attribute keys independently as a decentralized DTN.

III.EXISTING SYSTEM

The concept of attribute-based encryption (ABE) full fills the requirements for secure data retrieval in DTNs. It provides an access control over encrypted data using access policies and attributes among private keys and cipher texts. Especially, cipher text-policy ABE (CP-ABE) provides a scalable way of encrypting data such that the encryptor defines the attribute set that the decryptor needs to possess in order to decrypt the cipher text. Thus, different users are allowed to decrypt different pieces of data per the security policy. However, the problem of applying the ABE to DTNs introduces several security and privacy challenges. Since some users may change their associated attributes at some point, or some private keys might be compromised, key revocation for each attribute is necessary in order to make systems secure. However, this issue is even more difficult, especially in ABE systems, since each attribute is conceivably shared by multiple users. This implies that revocation of any attribute or any single user in an attribute group would affect the other users in the group. For example, if a user joins or leaves an attribute group, the associated attribute key should be changed and redistributed to all the other members in the same group for backward or forward secrecy. It may result in bottleneck during re-keying procedure or security degradation due to the windows of vulnerability if the previous attribute key is not updated immediately.

In CP-ABE, authority's master secret key is used to generates private keys of users associated set of attributes. So, the key authority can decrypt every cipher text addressed to specific users by generating their attribute keys. If the key authority is compromised by adversaries when deployed in the hostile environments, this could be a potential threat to the data confidentiality or privacy especially when the data is highly sensitive. The key escrow is an inherent problem even in the multiple-authority systems as long as each key authority has the whole privilege to generate their own attribute keys with their own master secrets. Since such a key generation mechanism based on the single master secret is the basic method for most of the asymmetric encryption systems such as the attribute- based or identity-based encryption protocols, removing escrow in single or multiple-authority CP-ABE is a pivotal problem.

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 policies over attributes issued from different authorities. For example, suppose that attributes “role 1” and “region 1” are managed by the authority A, and “role 2” and “region 2” are managed by the authority B. Then, it is impossible to generate an access policy ((“role 1” OR “role 2”) AND (“region 1” or “region 2”)) in the previous schemes because the OR logic between attributes issued from different authorities cannot be implemented. This is due to the fact that the different authorities generate their own attribute keys using their own independent and individual master secret keys. Therefore, general access policies, such as “ -out-of- ” logic, cannot be expressed in the previous schemes, which is a very practical and commonly required access policy logic.

The Main Objective of Cp-ABE is:

- Immediate attribute revocation enhances backward/forward secrecy of confidential data by reducing the windows of vulnerability.
- Encryptor’s can define a fine-grained access policy using any monotone access structure under attributes issued from any chosen set of authorities.
- The key escrow problem is resolved by an escrow-free key issuing protocol that exploits the characteristic of the decentralized DTN architecture.

Drawbacks:

CP-ABE is used to generate a private key of user based on their attribute keys. Every time when a user enters or removes from certain group then immediate key revocation is done. Updating attribute is not so efficient for every changes and it produces high computation complexity and communication cost.

IV.PROPOSED SYSTEM

This Section focus on how to overcome the above drawback by using a new technique called ETMS. The motive is to make a secure data retrieval in DTN. it can be achieved by using Efficient Trust Management Scheme. In

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 10, October 2014

addition to this Geographical Routing Algorithm is introduced for finding the Neighbour nodes or users in the extreme Military Network

3.1 ETMS: In order to detect the misbehaving nodes with less computation, an innovative technique is introduced which called Efficient Trust management system (ETMS) and using geographical is routing to identify the location of the nodes in the network. This method can learn from past experiences and adapt to changing environment conditions to maximize application performance and enhance operation agility. The learning process and adaptive designs of trust management system are reflected in trust aggregation, trust propagation and trust formulation. For trust composition, aggregation and propagation, firstly explore novel social and QoS trust components and then devise trust aggregation and propagation protocols for peer-to-peer subjective trust evaluation of individual social and QoS trust components, and prove the accuracy by means of theoretical analysis with simulation validation. For trust formation, explore a new design concept of mission-dependent trust formation with the goal of application performance optimization, allowing trust being formed out of social and QoS trust properties. Dynamic trust management is achieved by first determining the best trust formation model given a set of model parameters specifying the environment conditions, and then at runtime this trust system learns and adapts to changing environment conditions by using the best trust formation model identified from static analysis. We use a misbehaving node detection application as an example for which we identify the best application-level drop-dead trust threshold below which a node is considered misbehaving, and that the minimum trust threshold can be adjusted in response to changing conditions to minimize the false alarm probability.

3.2 Geographical Routing: The geographical routing is also known as position-based routing or geometric routing is a technique to deliver a message to a node in a network over multiple hops by means of position information. Routing decisions are not based on network addresses and routing tables; instead, messages are routed towards a destination location. By using this routing algorithm the location information can be obtained.

V.IMPLEMENTATION

System Modules:

Secure Data retrieval is enhanced by using EMTS method and finding the location of users or nodes in DTN through Geographical Routing Algorithm. The system is divided into four major modules:

- CP-ABE Encryption & Decryption
- In Trust Evaluation system
- Location Tracking

1) CP-ABE Encryption & Decryption:

This module describes how the key generating authority generates key for user. Key revocation for forward and backward secrecy and also solving key escrow problems. For each every step we need to concentrate on master key and private key of users.

There are key generation centres that generate public parameters for CP-ABE. It may consist of one central authority and multiple local authorities. For secure communication key authority generate attribute keys to the user.

The next step is to encrypt the data to be stored in storage node securely. On receiving the request query from user the storage node respond to the user. Here sender can define the access policy under attributes. When user receives the cipher text from storage node, the user decrypts the cipher text with its secret key.

On other hand, when a user comes to drop a set of attributes that satisfy the access policy at some instance, the corresponding attribute group keys also updated and delivered to valid attribute group securely.

2) In Trust Evaluation system:

In this section, advocate that both social trust components such as connectivity, intimacy, honesty and unselfishness, and QoS trust components such as competence, reliability and delivery ratio be considered. Let X denote a trust component selected and let $T_{ij}^{X}(t)$ denote node i's assessment toward node j in trust property X at time t. When a trustor node (node i) evaluates a trustee node (node j) in the same level at time t, it updates $T_{ij}^{X}(t)$ as follows:

$$T_{ij}^{X}(t) = \begin{cases} (1-\alpha^{X})T_{ij}^{X}(t-\Delta t)+\alpha^{X}T_{i,j}^{X,direct}(t) & \text{if } i \wedge j \text{ are } 1-\text{hop neighbours;} \\ \text{avg}_{k \in N_i}\{(1-\gamma^{X})T_{ij}^{X}(t-\Delta t)+\gamma^{X}T_{kj}^{X,recom}(t)\} & \text{otherwise} \end{cases}$$

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 10, October 2014

If node *i* is a 1-hop neighbor of node *j* at time *t*, node *i* will use its direct observations $T_{ij}^{X,direct}(t)$ and past experiences $T_{ij}^{X}(t-\Delta t)$ where Δt is a trust update interval toward node j to update $T_{ij}^{X}(t)$. We use a design parameter α^X with $0 \le \alpha^X \le 1$ to weight these two contributions and to consider trust decay over time for trust property X. A larger α^X means that trust evaluation will rely more on direct observations. Here $T_{i,j}^{X,direct}(t)$ indicates node *i*'s trust value toward node *j* based on direct observations accumulated over the time period [0, t] possibly with a higher priority given to more recent interaction experiences. On the other hand, if node *i* is not a 1-hop neighbor of node *j*, node *i* will use its past experiences $T_{ij}^{X}(t-\Delta t)$ and recommendations $T_{kj}^{X,recomm}(t)'s$ where *k* is a recommender to update $T_{ij}^{X}(t)$. Here $T_{kj}^{X,recomm}(t)$ is the recommendation from node *k* toward node *j* in component *X* and can be just $T_{ij}^{X}(t)$. A parameter γ^X is used here to weigh these two contributions and to consider trust decay over time as follows:

$$\gamma^X = \frac{\beta^X T_{ik}(t)}{1+\beta^X T_{ik}(t)}$$

For ease of disposition, here we introduce another parameter $\beta^X \ge 0$ to specify the impact of "indirect recommendations" on $T_{ij}^{X}(t)$ such that the weight assigned to indirect recommendations is normalized to $\beta^X T_{ik}(t)$ relative to 1 assigned to past experiences. Essentially, the contribution of recommended trust increases proportionally as either $T_{ik}(t)$ or β^X increases. Here, $T_{ik}(t)$ is node *i*'s trust toward node *k* as a recommender. Furthermore, to enhance QoI trust propagation, node *i* will only use its 1-hop neighbors who are considered trustworthy as recommender's. The new trust value $T_{ij}^{X}(t)$ in this case would be the average of the combined trust values of past trust information and recommendations collected at time *t*.

A direct-observation trust term $T_{ij}^{X,direct}(t)$ computed by node *i* toward node *j* based on evidences observed by node *i*. For each trust property *X*, this work will develop and validate evidence-based trust aggregation protocols executed by node *i* such that $T_{ij}^{X,direct}(t)$ thus obtained is accurate against actual status of node *j* at time *t*. Below we describe trust aggregation protocols by which node *i* can collect evidences to assess $T_{ij}^{X,direct}(t)$ for the case in which *i* and *j* are 1-hop neighbors at time *t* for *X*=intimacy, honesty, unselfishness (social components) and competence (a QoS component) below.

Intimacy: This measures intimacy or closeness of node *i* toward node *j*. If there is a priori knowledge that node *i* is close to node *j*, e.g., deriving from a "friendship" matrix as input, then $T_{i,j}^{intimacy,direct}(t) = 1$. Otherwise node *i* can compute $T_{i,j}^{intimacy,direct}(t)$ by the ratio of the number of interactions it has with node *j* during $[t - d\Delta t, t]$ to the maximum number of interactions with any other node. Here *d* is the window size giving recent interaction experiences higher priority over ancient experiences.

Honesty: This refers to the belief of node *i* that node *j* is honest based on node *i*'s direct observations during $[t - d\Delta t, t]$. Node *i* estimate $T_{i,j}^{honesty,direct}$ by the ratio of the number of suspicious interaction experiences observed during $[t - d\Delta t, t]$ to a system honesty threshold to reduce false positives.

Unselfishness: This provides the belief of node *I* that node *j* is unselfishness based on direct observations during $[t - d\Delta t, t]$. Node *i* can estimate $T_{i,j}^{unselfishness,direct}(t)$ by the ratio of the number of cooperative interaction experiences to the total number of protocol interaction experiences.

Competence: This refers to the belief of node *i* that node *j*'s is competent at time *t*. Node *i* estimates $T_{i,j}^{competence,direct}(t)$ by the ratio of the number of positive packet transmission experiences to the total number of packet transmission experiences.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 10, October 2014

The difference between $T_{i,j}^{X,direct}(t)$ and $T_j^X(t)$ is the direct trust assessment error, $TE_{ij}^{X,direct}(t)$ defined as follows: $TE_{ij}^{X,direct}(t)=T_{ij}^{X,direct}(t) - T_j^X(t)$.$TE_{ij}^{X,direct}(t)$ Above is one source of trust inaccuracy. Based on the trust value the misbehaviour node is detected.

3) **Location Tracking:**

A simple scheme is presented for geographic forwarding that is similar to Cartesian routing. Each node determines its own geographic position using a mechanism such as GPS; positions consist of latitude and longitude. A node announces its presence, position, and velocity to its neighbors (other nodes within radio range) by broadcasting periodic HELLO packets. Each node maintains a table of its current neighbors' identities and geographic positions. The header of a packet destined for a particular node contains the destination's identity as well as its geographic position. When node needs to forward a packet toward location *P*, the node consults its neighbor table and chooses the neighbor closest to *P*. It then forwards the packet to that neighbor, which itself applies the same forwarding algorithm. The packet stops when it reaches the destination.

VI. RESULTS

The simulation studies involve the Disruption Tolerant Network. The proposed ETMS is implemented in NS2 Simulator. We perform secure data retrieval in proposed system by using Trust value and Threshold value of requesting node in military network. It helps in identifying the malicious nodes in DTN environment. From fig.1. Trust threshold value gets calculated for requesting node in DTN. Social trust and Qos trust is calculated in fig.2 by checking the unselfishness, honesty, intimacy and competence

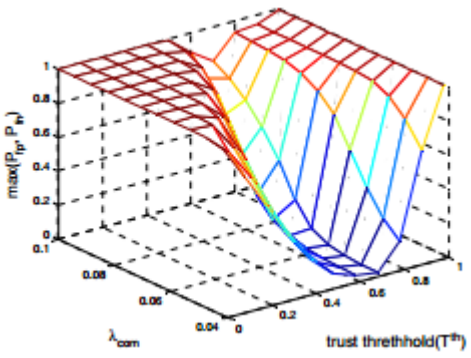

Fig.1. Analysing the trust threshold

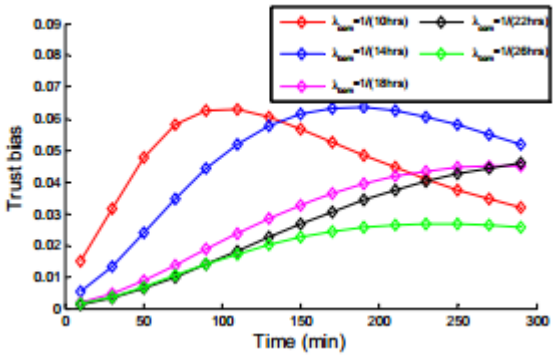

Fig.2. Calculating Trust Values

VII. 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 secure data retrieval issues. In the existing system, an efficient and secure data retrieval method using CP-ABE is used 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. But the drawback in this method is less trade off between the computational complexity and security. So, in the proposed system Efficient Trust management system (ETMS) is introduced using geographical is routing to identify the location of the nodes in the network. This method can learn from past experiences and adapt to changing environment conditions to maximize application performance and enhance operation agility.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 10, October 2014

REFERENCES

[1] Lei Yang ,A Reactive Geographic Routing Protocol for wireless sensor networks Rong Ding ; State Key Lab. of Software Dev. Environ., Beihang Univ., Beijing, China . Lei Yang
[2] A. Lewko and B. Waters, "Decentralizing attribute-based encryption," Cryptology ePrint Archive: Rep. 2010/351, 2010.
[3] Ing-Ray Chen," Dynamic Hierarchical Trust Management of Mobile Groups and Its Application to Misbehaving Node Detection" Dept. of Comput. Sci., Virginia Tech, Blacksburg, VA, USA; Jia Guo
[4] M. Chase, "Multi-authority attribute based encryption," in *Proc. TCC*, 2007, LNCS 4329, pp. 515–534.
[5] M. Chuah and P. Yang, "Node density-based adaptive routing scheme for disruption tolerant networks," in *Proc. IEEE MILCOM*, 2006, pp. 1–6.
[6] M. Chuah and P. Yang, "Performance evaluation of content-based information retrieval schemes for DTNs," in *Proc. IEEE MILCOM*, 2007, pp. 1–7.
[7] 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.
[8] 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.
[9] 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.