Detection of Insider Attacks by Using Trust Value in Decentralized Disruption-Tolerant Military Networks

Afeefa T1, Afsar P2
1,2PG scholar, Department Of Computer Science and Engineering, MEA Engineering College, Perinthalmanna, INDIA

ABSTRACT

Disruption-tolerant network (DTN) technologies are becoming successful solutions that allow nodes to communicate with each other in these extreme networking environments. Some of the most challenging issues in this scenario are the enforcement of authorization policies and the policies update for secure data retrieval. The concept of attribute-based encryption (ABE) is a promising approach that fulfills the requirements for secure data retrieval in DTNs. So, in the existing system cipher text-policy attribute-based encryption (CP-ABE) is presented which 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. 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. So, a secure data retrieval scheme is presented using CP-ABE for decentralized DTNs where multiple key authorities manage their attributes independently. But the drawback is updating attributes is not so efficient and high complexity. So, in the proposed system a new technique is introduced which is called Efficient Trust management system (ETMS) for reducing complexity and improving the security. Also, the geographical routing is used to find the location of the nodes. In this method, each node evaluates other nodes in the same subtask group while each subtask group leader (SGL) evaluates other SGLs and nodes in its subtask group. The peer-to-peer trust evaluation is periodically updated based on either direct observations or indirect observations. An experimental result shows that the proposed ETMS method achieves high efficiency and security and less complexity.

General Terms-----Attribute-based encryption(ABE), disruption-tolerant network(DTN), multi-authority, secure data retrieval.

I. INTRODUCTION

Delay-tolerant networking (DTN) is an approach to computer network architecture that seeks to address the technical issues in heterogeneous networks that may lack perpetual network connectivity. It becoming prosperous solutions that sanction nodes to communicate with each other in these extreme networking environments. In many military network scenarios, connections of wireless contrivances carried by soldiers may be ephemerally disconnected by jamming, environmental factors, and mobility, especially when they operate in truculent environments. Typically, when there is no terminus-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 duration until the connection would be eventually established.

Many military applications require incremented auspice of confidential data including access control methods that are cryptographically enforced. The storage nodes are introduced in DTNs where data is stored or replicated such that only sanctioned mobile nodes can access the indispensable information expeditiously and efficiently. In many cases, it is desirable to provide differentiated access accommodations such that data access policies are defined over utilizer attributes or roles, which are managed by the key ascendant entities.

Attribute-based encryption (ABE) is a promising approach that fulfills the requisites for secure data retrieval in DTNs. ABE features a mechanism that enables an access control over encrypted data utilizing access policies and ascribed 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 sanctioned to decrypt different pieces of data per the security policy. However, the quandary of applying the ABE to DTNs introduces several security and privacy challenges. Since some users may transmute their associated attributes at some point, or some private keys might be compromised, key revocation for each attribute is indispensable 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 implicatively insinuates that revocation of any attribute or any single utilizer in an attribute group would affect the other users in the group. It
may result in bottleneck during rekeying procedure or security degradation due to the windows of susceptibility if the precedent attribute key is not updated immediately.

In the proposed system, 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. 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 the location information can be obtained.

II. BACKGROUND

Delay-tolerant Network: Delay-tolerant networking (DTN) is an approach to computer network architecture that seeks to address the technical issues in heterogeneous networks that may lack continuous network connectivity. Examples of such networks are those operating in mobile or extreme terrestrial environments, or planned networks in space.

Recently, the term disruption-tolerant networking has gained currency in the United States due to support from DARPA, which has funded many DTN projects. Disruption may occur because of the limits of wireless radio range, sparsity of mobile nodes, energy resources, attack, and noise.

![Figure 1. Delay-tolerant Network](image)

Abbreviated as DTN, 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. It is an experimental protocol developed by the Delay & Disruption Tolerant Networking Research Group, which operates under the Internet Research Task Force

III. RELATED WORK

Junbeom Hur and Kyungtae [1] propose an attribute-predicated secure data retrieval scheme utilizing CP-ABE for decentralized DTNs. The proposed scheme features the following achievements. First, immediate attribute revocation enhances rearward/forward secrecy of confidential data by reducing the windows of susceptibility. Second, encryptors can define a fine-grained access policy utilizing any monotone access structure under attributes issued from any culled set of ascendant entities. Third, the key escrow quandary is resolved by an escrow-free key issuing protocol that exploits the characteristic of the decentralized DTN architecture. The key issuing protocol engenders and issues user secret keys by performing a secure two-party computation (2PC) protocol among the key ascendant entities with their own master secrets. The 2PC protocol deters the key ascendant entities from obtaining any master secret information of each other such that none of them could engender the whole set of user keys alone. Thus, users are not required to plenarily trust the ascendant entities in order to bulwark their data to be shared. The data confidentiality and privacy can be cryptographically enforced against any curious key ascendant entities or data storage nodes in the proposed scheme.

Huang, Verma [2] proposed scheme for dynamic environment, where establishing trust among conveyances is arduous. Solution is predicated on attribute predicated encryption (ABE) to construct an attribute predicated security policy enforcement (ASPE) framework. ASPE considers sundry road situations as attributes. These attributes are utilized as encryption keys to secure the transmitted data. ASPE is flexible in that it can dynamically change encryption keys depending on the VANET situations. Concurrently, ASPE naturally incorporates data access control policies on the transmitted data. ASPE provides an integrated solution to involve data access control, key management, security policy enforcement, and secure group formation in highly dynamic vehicular communication environments. Its contributions are in three-fold: (i) ASPE provides an architectural solution that enforces policy control in highly dynamic communication environments. The policies defined are predicated on vehicles’ circumventing situations and can be modified to achieve different security and privacy goals for VANETs. (ii) It show how ASPE policies can be elongated to perform subgroup vehicular communications with minimum communication and computation overhead. (iii) Present an optimization of ABE for vehicular networks, which avail ASPE run more efficiently.

Roy, S., and M. Chuah [3] propose an access control scheme which is based on the Ciphertext Policy Attributed-Predicated Encryption (CP-ABE) approach. Here provides a flexible fine-grained access control such that the encrypted contents can only be accessed by sanctioned users. Two unique features provide are: (i) the incorporation of dynamic attributes whose value may change over time, and (ii) the revocation feature. Here postulate that the data object is encrypted utilizing a symmetric key which is later encrypted utilizing the CP-ABE approach. Furthermore, they additionally postulate that each utilizer can revoke any utilizer utilizing the negative attribute corresponding to that user’s identifier. It is postulated that any utilizer who revokes another utilizer notifies the central ascendency so that the central ascendency can compile a list of revoked users periodically.
and disseminate such information to the regional key servers. Luan Ibraimi, Milan Petkovic, and Svetla Nikov [4], application that elongates CP-ABE with instantaneous attribute revocation. Propose an incipient scheme for attribute revocation in CP-ABE called mediated Ciphertext-Policy Attribute-Predicated Encryption (mCP-ABE). The secret key is divided into two shares, one share for the mediator and the other for the users. To decrypt the data, the utilizer must contact the mediator to receive a decryption token. The mediator keeps an attribute revocation list (ARL) and relents to issue the decryption token for revoked attributes. Without the token, the user cannot decrypt the ciphertext, therefore the attribute is implicitly revoked. The technique of splitting the attribute components of the secret key into two shares, and the technique of utilizing an identifier Iu for each utilizer, avails us to achieve the following attribute revocations: i) revoking an attribute from a single utilizer without affecting other users, and ii) revoking an attribute from the system where all users are affected.

Bethencourt, Sahai, Waters [5] proposed the system such that a user's private key will be associated with an arbitrary number of attributes expressed as strings. On the other hand, when a party encrypts a message in the system, they designate an associated access structure over attributes. A utilizer will only be able to decrypt a cipher text if that utilizer's attributes pass through the cipher text's access structure. At a mathematical level, access structures in this system are described by a monotonic access tree”, where nodes of the access structure are composed of threshold gates and the leaves describe attributes. To note that AND gates can be constructed as n-of-n threshold gates and OR gates as 1-of-n threshold gates. Furthermore, handle more involute access controls such as numeric ranges by converting them to minute access trees. By using this method key revocation is difficult

IV. PROPOSED SYSTEM

In the proposed system, 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. Figure 2 shows the flowchart of proposed work.

### Table 1: Comparison Table

<table>
<thead>
<tr>
<th>Scheme</th>
<th>Authority</th>
<th>Expressiveness</th>
<th>Key Escrow</th>
<th>Revocation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure data retrieval for DIN [1]</td>
<td>Multiple</td>
<td>Any monotone access structure</td>
<td>No</td>
<td>Immediate attribute level revocation</td>
</tr>
</tbody>
</table>

4.1 Peer-to-peer trust evaluation:

It maintains two peer-to-peer level of trust: node level and SGL level trust. Each node evaluates other nodes in the same subtask group while each SGL evaluates other SGLs and nodes in its subtask group. The peer-to-peer trust evaluation is periodically updated based on either direct observation or indirect observation. When two nodes are neighbors within radio range, they evaluate each other based on direct observations via snooping or overhearing. Each node sends its trust evaluation results toward other nodes in the same subtask group to its SGL. The commander performs trust evaluation toward all SGLs (commander-to-SGL) in the system. A SGL is responsible for misbehaving node detection for nodes in its subtask group, while the commander is responsible for misbehaving SGL detection for all SGL nodes in the system.

4.2 Trust aggregation and trust formation

Use 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 $i$'s assessment toward node $j$ in trust property $X$ at time $t$. Below we describe how trust aggregation and trust propagation for peer-to-peer trust evaluation are conducted between two members in the same subtask group or two SGLs $T_{ij}^X(t)$. As illustrated in Figure 3 & 4, when a trustor node (node $i$) evaluates a trustee node (node $j$) at time $t$, it updates $T_{ij}^X(t)$ as follows:

$$T_{ij}^X(t) = (1-\alpha^X)T_{ij}^X(t-1) + \alpha^X T_{ij}^X(\text{direct}(t))$$

if $i$ and $j$ are 1-hop neighbours.

$$T_{ij}^X(t) = \text{avg}(1-\gamma^X)T_{ij}^X(t-1) + \gamma^X T_{ij}^X(\text{recommend}(t))$$

otherwise.

We use a design parameter $\alpha^X$ with $0 \leq \alpha^X \leq 1$ to weight these two contributions and to consider trust decay over time for trust property $X$. A larger $\alpha^X$ means that trust evaluation will rely more on direct observations. Parameter $\gamma^X$ is defined as follows:

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

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 the location information can be obtained.

V. RESULTS AND DISCUSSION

5.1 Description about network setup

In this section, the simulation results of communication cost and communication overhead is measured to compare the existing cipher text-policy attribute-based encryption method and the proposed Efficient Trust management system (ETMS).
Input parameters are,
Number of nodes

Number of nodes is defined as number of nodes is taken in the network setup.

5.2 Description of output parameter

Communication cost
The total communication cost includes the cipher text and rekeying messages for non-revoked users. It is measured in bits.

Communication overhead
Overhead is any combination of excess or indirect computation time, memory, bandwidth, or other resources that are required to attain a particular goal.

5.3 Comparison graphs

The communication cost is shown in this graph. In the X-axis number of nodes is taken. Y-axis communication cost is taken. In the existing cipher text-policy attribute-based encryption method is used and the proposed method Efficient Trust management system (ETMS) is used. This graph clearly shows that the number of nodes is increases the communication cost is increases in existing methods. But in the proposed method, the communication cost is decreases.

The overhead is shown in this graph. In the X-axis number of nodes is taken. Y-axis overhead is taken. In the existing cipher text-policy attribute-based encryption method is used and the proposed method Efficient Trust management system (ETMS) is used. This graph clearly shows that the overhead is increases in existing methods. But in the proposed method, the overhead is decreases.

VI. 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 tradeoff between the computational complexity and security. So, in the proposed system Efficient Trust management system (ETMS) is introduced using geographical 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.

VII. ACKNOWLEDGMENT

The author would like to express her sincere thanks to HOD, project guide and staff in Computer Science department, M E A Engineering College for many fruitful discussions and constructive suggestions during the preparation of this manuscript.

REFERENCES