An Efficient Secure Data Transmission Based on Randomized Scheme in DTN

Dhivya.G , Rajeswari.G

Abstract— Mobile nodes in wireless connection may be temporarily disconnected especially in extremely challenged environments due to unreliable and intermittent connectivity, lack of trust between nodes, and unknown network characteristics. Disruption-tolerant network (DTN) technologies are becoming successful solutions that allow nodes to communicate in these extreme networking environments also introduced supply nodes where data are stored such that only authorized mobile nodes can access the necessary information quickly and efficiently. Cipher-text policy attribute based encryption (CP-ABE) provides a scalable method of cipher data, such that the encryptor defines the attributes set that the decryptor needs to possess in order to decrypt the encoded text. In M-CP-ABE scheme provide secure communication of data extraction but periodically. Not Data ensure. If any problem of network cannot recover and cannot choose another path. To overcome this Random Walk Gossip (RWG) is a message dissemination protocol for intermittently connected networks. RWG is based on a store-and-forward mechanism.

Keywords— wireless connections, M-CPABE, Random walk gossip, Store& forward.

I. INTRODUCTION

A disruption-tolerant network (DTN) is a network designed so that temporary or intermittent transmission troubles, flaws and abnormalities have the least possible opposite crash. There are various features to the strong scheme of a DTN, incorporating: 1. the use of fault-tolerant methods and technologies. 2. The quality of graceful degradation under adverse conditions or extreme traffic loads. 3. The ability to prevent or quickly recover from electronic attacks. 4. Ability to function with minimal latency even when routes are ill-defined or unreliable.

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 supply nodes. Typically, when there is no end-to-end connection between a source and a target pair, the data from the origin node may need to wait in the intermediate nodes for a substantial amount of time until the connection would be eventually established.DTN introduced supply nodes where data are stored or replicated such that only authorized mobile nodes can access the necessary information quickly and efficiently. For example, in a disruption-tolerant military network, a commander may store confidential information at a supply node, which should be entered by the subscriber of "Corps 1" who is participating in "Region 2." In this case, it is a reasonable assumption that multiple key sway are likely to manage their own dynamic attributes for soldiers in their deployed regions or echelons, which could be frequently changed (e.g., the attribute representing the current location of moving soldiers). DTN architecture where multiple sway issue and manage their own attribute keys independently as a decentralized DTN [14].

Attribute based encryption is a vision of public key encryption that allows exploiters to encrypt and decrypt messages based on exploiter attributes (e.g., the attribute representing the current location of moving soldiers) [8], [12], [13]. In a typical execution, the length of the encrypted text is proportional to the number of attributes associated with it and the decryption time is proportional to the number of attributes used during decryption.

However, the problem of applying the ABE to DTNs introduces several security and secrecy challenges. Since some exploiters may change their associated attributes at some point (for example, motion in their area), or some unique keys might be compromised, key revocation (or update) for each attribute is necessary in order to make systems secure. However, this issue is even additional inconvenient, especially in ABE systems, since each trait is conceivably shared by multiple exploiters. This points that revocation of any attributes or any single exploiter in a trait group would affect the other exploiters in the group.

Another challenge is the key escrow problem. In CP-ABE, the key authorization generates private keys of exploiters by applying the sway's master secret keys to exploiters' associated set of traits. The last challenge is the coordination of attributes issued by different sway. For example, suppose that traits "role 1" and "region 1" are managed by the sway A, and "role 2" and "region 2" are managed by the sway 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 by different sway cannot be implemented.

II. RANDOM WALK GOSSIP

The Random Walk Gossip (RWG) is a message dissemination protocol for intermittently connected networks. RWG is based on a store-and-forward mechanism. This is controlled by a three-way packet for the purpose of path Discovers. They are Request to Forward (REQF), acknowledgement packet (ACK), OK to Forward (OKTF). Each packet header contains a bit vector called the informed

Dhivya.G, PG Scholar, Sree Sowdambika College Of Engineering, Anna University, India. (Email: divya.jillu3@gmail.com)
Rajeswari.G, Assistant professor, Sree Sowdambika College Of Engineering, Anna University . (Email: prajasri10@gmail.com)

vector at the time of message transfer. When a node receives the message it produces a hash of its own address and puts a ‘1’ in the bit vector buffer in the field corresponding to the hash. When a node realizes that a message is delivered to destination it sends a Be Silent (BS) packet to its vicinity and thus removes it from their ‘1’ stored in the buffer.

Algorithm 1 Random walk gossip

```
Copy all 1s from recently to visited and set recently to empty
Send message to a random neighbor with 0 in recently
When a message m is heard:
Update visited
Decide if forwarder
After log (n) hops, duplicate message and repeat
When M nodes have been reached (easily seen in visited): stop forwarding and propagate delete (m)
```

Algorithm 1 describes the basic behavior during thegossiping phase of the algorithm. The mechanism tochoose a random neighbor does not require neighborhoodknowledge. Instead the message is broadcasted to all 1-hopreachable nodes. Each receiver sets a timer and when thetimer expires a request-to-forward is sent. The node whosent the message will only give permission to one such forwardrequest.

III. RELATED WORK

There are two types of ABE are depending on which of private keys or cipher texts that access policies are associated with.In a key-policy attribute-based encryption (KP-ABE) system, cipher texts are labeled by the transmitter with a set of descriptive attributes, while exploiter's private key is issued by the trusted attribute sway captures a policy (also called the access structure) that specifies which type of cipher texts the key can decrypt. KP-ABE schemes are suitable for structured organizations with rules about who may read particular documents. Typical applications of KP-ABE include secure forensic analysis and target broadcast. For example, in a secure forensic analysis system, audit log entries could be annotated with attributes such as the name of the exploiter, the date and time of the exploiter action, and the type of data modified or accessed by the exploiter action. While a forensic analyst charged with some investigation would be issued a private key that associated with a particular access structure. The private key would only open audit log records whose attributes satisfied the access policy associated with the private key[8], [11].

In a cipher text-policy attribute-based encryption (CP-ABE) system, when a transmitter encrypts a message, they specify a specific access policy in terms of the access structure over attributes in the cipher text, stating what kind of receivers will be able to decrypt the cipher text. Exploiters possess sets of attributes and obtain corresponding secret attribute keys from the attribute sway. Such anexploiter can decrypt a cipher text if his/her attributes satisfy the access policy associated with the cipher text. Thus, CP-ABE mechanism is conceptually closer to traditional role-based access control method.

IV. DESIGN PRINCIPLES

In this section, we describe the RWG architecture and define the security model.

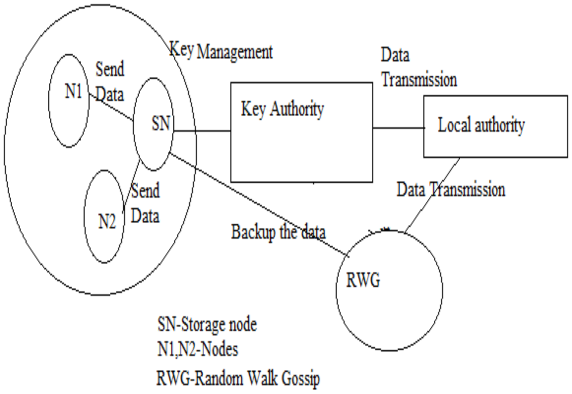

Fig.1. Architecture of secure data transmission in defense network

A. System Description and Assumptions

Fig. 1 shows the layout of the work process consist of the following entities

1) Storage Node: This entity which is used to Storedata from the other node. SN receives data with an encrypted format to provide security.

*2) Key Authority:*They are key generation centers that generate public/secret guidelines for CP-ABE. Let’s assume that there are secure and reliable transmission ducts between a central domination and each local domination during the preliminary key conformation and generation phase.

3) Local authority: Each local sway manages different attributes and issues corresponding attribute keys to exploiters. They grant different access entitlement to individual exploiters based on the exploiters’ attributes. That is, they will honestly perform the assigned tasks in the given order; however they would like to learn information of encrypted contents as much as possible.

*4) RWG:*The main purpose of RWG is used to retransmit the data when there is loss or disconnected. It receives backup from the SN while send information to the receiver.

Since the key authority is semi-trusted, they should be deterred from accessing plaintext of the data in the supply node; meanwhile, they should be still able to issue secret keys to exploiters. In order to realize this somewhat contradictory requirement, the central sway and the local sway engage in the arithmetic 2PC protocol with master keys of their own and issue independent key components to exploiters 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 exploiters individually.

B. Security Requirements

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

2) Collusion-resistance: If multiple exploiters collude, they may be able to decrypt a cipher text by combining their attributes even if each of the exploiters cannot decrypt the cipher text alone. For example, suppose there exist a exploiter with attributes {”Battalion 1”, “Region 1”} and another exploiter 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 a collusion attack among curious local sway to derive exploiters’ keys.

3) Backward and forward Secrecy: In the context of ABE, backward secrecy means that any exploiter 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 exploiter 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.

V. ANALYSIS

In this section, we first analyze and compare the efficiency of the proposed scheme to the previous multi-sway CP-ABE schemes in theoretical aspects. Then, the efficiency of the proposed scheme is demonstrated in the network simulation.

A. Simulation

Network Simulator NS2 is a primer providing materials for NS2 beginners, whether students, professors, or researchers for understanding the architecture of Network Simulator 2 (NS2) and for incorporating simulation modules into NS2. Here discussed the simulation architecture and the key components of NS2 including simulation-related objects, network objects, packet-related objects, and helper objects.

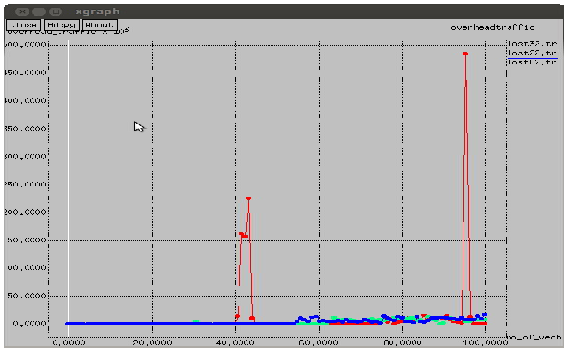

Fig.2. Number of nodes with overhead traffic comparison

The NS2 modules included within are nodes, links, Simple link objects, packets, agents, and applications. Further, the book covers three helper modules: timers, random number generators, and error models. Two appendices provide the details of scripting language Tcl, OTcl and AWK, as well object oriented programming used extensively in NS2.

Fig. 2 represents the number of nodes and how much traffic occur in existing (red), proposed (blue) & using RWG (green).

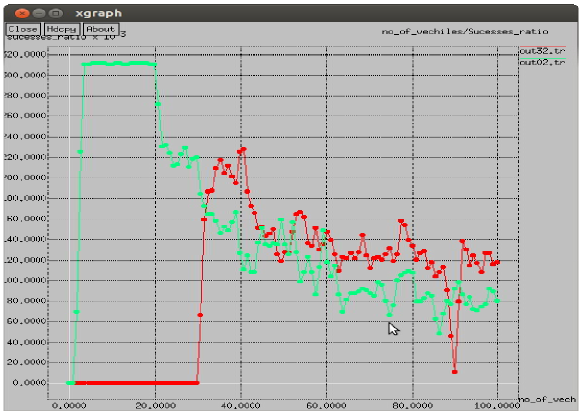

Fig.3. Number of nodes with how long message success

Fig. 3 shows the number of nodes and how long the message delivery success by comparing both proposed (green) and existing (red).

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 supply nodes. CP-ABE is a scalable cryptographic solution to the access control and secures data retrieval issues. In this paper, we proposed an efficient and secure data retrieval method using CP-ABE for decentralized DTNs where multiple key swaymanages 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 sway might be compromised or not fully trusted. In addition, the fine-grained key revocation can be done for each attribute group. We demonstrate how to apply the proposed mechanism to securely and efficiently manage the confidential data distributed in the disruption-tolerant defese network. RWG works well when compared to existing system. It works for store & forward mechanism.

REFERENCES

[1] Mikael Asplund, Simin Nadjm-Tehrani Linkoping University SE-581 83 Link□oping, Sweden,” Random Walk Gossip: A Manycast Algorithm forDisaster Area Networks”IEEE,2013

[2] Arathy Sankar , Rahul Jiwane ,” Back- Pressure Algorithm Using Shadow Queues in Communication Networks “Volume 4, Issue 10, October 2014

[3] Mrs. JAYASHREE,S. YADANNAVAR , ” Probabilistic Splitting Table helps in back pressure based packet by packet adoptive routing in communication network” VOL. 2, NO. 4, APRIL 2014, 137–141

[4] Nayana Hegde ,” Simulation of Wireless Sensor Network Security Model Using NS2” Vol. 4 Issue 1 May 2014

[5] *J. Burgess, B. Gallagher, D. Jensen, and B. N. Levine, “Maxprop: Routing for vehicle-based disruption tolerant networks,” 2006,*

[6] *M. Chuah and P. Yang, “Node density-based adaptive routing scheme for disruption tolerant networks,” 2006,.*

[7] *M. M. B. Tariq, M. Ammar, and E. Zequra, "Mesage ferry route design for sparse ad hoc networks with mobile nodes," in Proc. ACM MobiHoc, 2006,.*

[8] *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.*

[9] *M. Chuah and P. Yang, "Performance evaluation of content-based information retrieval schemes for DTNs, 2007*

[10] *M.Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, "Plutus: Scalable secure file sharing on untrusted storage," 2003*

[11] *L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker, "Mediated ciphertext-policy attribute-based encryption and its application," 2009.*

[12] *N. Chen, M. Gerla, D. Huang, and X. Hong, "Secure, selective group broadcast in vehicular networks using dynamic attribute based encryption," 2010*

[13] *D. Huang and M. Verma, "ASPE: Attribute-based secure policy enforcement in vehicular ad hoc networks," 2009*

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

[15] *A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Proc. Eurocrypt, 2005*

[16] *V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data,"2006*