Abstract
The current Internet service models is based on a few assumptions such as the existence of an end to end path between a source and destination pair, and low round-trip latency between any node pair. However, these assumptions do not hold in some emerging networks. Like battlefield ad-hoc Networks in which wireless devices carried by soldiers operate in hostile environments where jamming, environmental factors and mobility may cause temporary disconnections. To allow nodes to communicate with each other in these extreme networking environments, we proposed a new architecture called the Disruption Tolerant Network (DTN). In some application scenarios, there are some ‘storage nodes’ in the network where useful data is stored or replicated so that other regular mobile nodes can access the necessary information quickly and efficiently. A requirement in some security-critical applications is to design an access control system to protect the confidential data stored in the storage nodes or contents of the confidential messages routed through the network. Overcome this problem, in this project we propose a 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. The proposed scheme have attribute revocation enhances backward/forward secrecy of confidential data; the coordination of attributes issued from different authorities and avoid third party compromised with key authorities. The proposed scheme to securely and efficiently manage the confidential data distributed in the disruption- tolerant military network.

Keywords: Disruption Tolerant Network, 2PC

1. Introduction
In many military network scenarios, connections of wireless devices carried by soldiers may be temporarily disconnected by jamming, environmental factors, and mobility, especially when they operate in hostile environments. Disruption Tolerant Network (DTN) technologies are becoming successful solutions that allow nodes to communicate with each other in these extreme networking 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. In CP-ABE, the cipher text is encrypted with an access policy chosen by an encryptor, but a key is simply created with respect to an attributes set. CP-ABE is more appropriate to DTNs than KP-ABE because it
enables encrypers such as a commander to choose an access policy on attributes and to encrypt confidential data under the access structure via encrypting with the corresponding public keys or attributes.

DTN architecture may be referred as where multiple authorities issue and manage their own attribute keys independently as a decentralized DTN. There may be a packet loss due to transmission of many data and sometimes the attacker may leak the data when they compromise with third party. For this purpose we have one local authority and global authority, so now the data won’t be shared to others since each have only their part of key generation.

2. System Design

2.1 Existing System

An attribute-based secure data retrieval scheme using CP-ABE for decentralized DTNs. The proposed scheme features the following achievements. First, immediate attribute revocation enhances backward/forward secrecy of confidential data by reducing the windows of vulnerability. Second, encrypers can define a fine-grained access policy using any monotone access structure under attributes issued from any chosen set of authorities. Third, 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 2-Party Computation (2PC) protocol among the key authorities with their own master secrets. 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.

2.1.1 Advantages

2.1.1.1 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.

2.1.2 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 alone.

2.1.3 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.

2.2 System Architecture

In this section, we describe the DTN architecture and define the security model. First we are setting up two groups as 1 and 2.

2.2.1 Group Creation

It creates a new group and initializes the public key for that particular group. After the initialization if a new user joins the group it create the node else they leave their group if user time expires and key is invalidated for the user. After joining he group a private key is generated for the particular person. All these key and other details are stored in the database.

2.2.2 Node Join or Leave

After a user joins their group, if he wants to check any of the particular data attribute revocation is done. i.e. There are many departments in military network such as food department, health department etc. Hence each use can revoke particular attribute independently.
2.2.3 Fine Grained
Using fine grained access policy only valid use can view/update the data. Other third party cannot use any information.

2.2.4 Key Authority
In the existing system it was centralized DTN network using which it share the data only to particular area. If it's behind the reach of area the data will not be able to communicate. In the above architecture, Decentralized key is spitted into two ways one is local authority and global authority.

Each local authority manage different attribute and provide corresponding attribute key to the user. 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.

2.2.5 Database
This is an entity that stores data from senders and provide corresponding access to users. It may be mobile or static.

Finally the keys, revocation of attribute and are shared to the sender.

2.3 Proposed System
By using ns2 simulator, first we are identifying the root node. Once it is identified the flow starts from source node to destination node. For interacting with other node, intermediate node is used for sharing the data. At first stage getting key from both the group (i.e. from local and global authority) and also getting key from sender. Finally sends the data to the receiver. If it's passing through particular its wait for a while and then it transmit the data. It comes directly then it does not consider the particular node for transmission, hence communication will be within two nodes in both groups. Since there is a large gap between nodes intermediate node is assigned.

Now it establishes communication between each node. For decrypting the message it gets key from global authority and local authority. Here we proposed is when transmission rate increases data loss will be constant and there will be only minimal loss of data. Since only part of key is shared none can hack the data and misuse. Hence finally the total energy saved during transmission, power loss, and throughput is calculated. Even if number of transmission gets increases, the data will be secure.

The different types of node used are sender, receiver, intermediate node, global authority and local authority on each side. First the sender sends request to the receiver which in turn acknowledges the packet to the source node. Then it makes a connection between sender and local authority. The keys are shared between them. Foremost only a part of key is being transmitted by the local authority. Now connection setup is between global authorities, it gets the key from both part of the group and stores it for later use. Once it gets all its acknowledgment from local and global authority it forms a link between them and starts sharing their data.

2.3.1 Advantages of Proposed System
- During transmission of more packets, data loss will be constant.
- Energy power can be controlled.
- Data loss can be calculated manually.
- It provides security.
2.4.1 Module Description

2.4.1.1 Network Creation (Wireless Sensor Networks)
Creation of nodes in the wireless networks is the first module that is done using NS2 Software. In this module we deploy the nodes in the network and each node pass the information through the HELLO packets to its neighbor nodes and update the neighbor node id, location information in each node in order to find the route. It also create group. If you enter into the group first you have to send your id to group head.

- Composed of many small nodes deployed in an ad hoc fashion
- Most communication will be between nodes as peers, rather than to a single base station
- Nodes must self-configure
- Dedicated to a single application or a few collaborative applications
- Involves in-network processing to reduce traffic and thereby increase the life-time
- This implies that data will be processed as whole messages at a time in store-and-forward fashion
- Hence packet or fragment-level interleaving from multiple sources only delays overall latency
- Applications will have long idle periods and can tolerate some latency

2.4.1.2 Sink and Source Nodes
The sink is the point of contact for users of the sensor network. Each time the sink receives a question from a user, it first translates the question into multiple queries and then disseminates the queries to the corresponding mobile relay, which process the queries based on their data and return the query results to the sink. The sink unifies the query results from multiple storage nodes into the final answer and sends it back to the user.

The source nodes in our problem formulation serve as storage points which cache the data gathered by other nodes and periodically transmit to the sink, in response to user queries. Such network architecture is consistent with the design of storage centric sensor networks. Our problem formulation also considers the initial positions of nodes and the amount of data that needs to be transmitted from each storage node to the sink.

2.4.1.3 Key Authorities Computation
The key authorities consist of a global authority and multiple local authorities to achieve secure communication
in network environment. While doing encrypting operation, Local authorities are providing the half of the encryption key. The other half will be provided by the global authority in order to complete effective secure encryption. Even though the local authority compromised with the unauthorized external user, he cannot access the information which has been encrypted, since he is having only half of the encryption key. If a new user wants to join in that group then he should priorly know about his private key pairs and his own group's public key. While joining into the network, the node user should submit the public key to the respective group. Thus public key will be transmitted all over the group users. When leaving the group, the public key validity is permanently expired and new public key has been generated by the group manager and it will be circulated to all the existing group users. Hence the attribute revocation is successfully achieved.

2.4.1.4 Decentralization

Previously, the encrypted information can be transferred to only one receiving end group user at a time. But in this module, at the same time the encrypted information is being transferred to multiple receiving end group users. Such that co-ordination of attributes access is achieved. Due to this reduced time consumption, reliability, secured transmission of information and cost effective system is obtained.

Thus after getting the session key generated by the sender, the data which need to be sent will be encrypted using this temporary session key and it will be routed to the destination receiver user. Thus receiver will get the private key pair and using the private key pair, the data will be decrypted. Thus unauthorized user cannot able to enter in the group for tracking the key pairs for misleading purposes.

2.4.1.5 Encryption and Data Transmission

Thus after getting the session key generated by the sender, the data which need to be sent will be encrypted using this temporary session key and it will be routed to the destination receiver user. Thus receiver will get the private key pair and using the private key pair, the data will be decrypted. Thus unauthorized user cannot able to enter in the group for tracking the key pairs for misleading purposes.

3. Conclusion

Our project is not the unique one, but is an endeavor attempt to have a precise scenario of what the terms “A new trust management for secure communication using MANET is meant to be implemented as well on which we are working”. As stated before, our proposed system can enhance the security of military network and can avoid loss as more number of transmission increases. It perform better throughput and energy is consumed as compared to existing system. The provision of key is only part for each group. Hence third part cannot compromise with the authorities. Security is enhanced and even if more number of transmissions takes place the data loss will be constant. Our proposed scheme to securely and efficiently manage the confidential data distributed in the disruption-tolerant military network. In future it can be used in wireless and mobile network.

4. References

1. Roy S, Chuah M. Secure data retrieval based on Ciphertext Policy Attribute-Based Encryption (CP-ABE) system for the DTNs. Lehigh CSE Technical Report. 2009.
2. Lewko A, Waters B. Decentralizing attribute-based encryption. 2010. CryptologyePrint Archive: Report 2010/351.
3. Goyal V, Pandey O, Sahai A, Waters B. Attribute-based encryption for fine-grained access control of encrypted data. Proceedings ACM Conference on Computer and Communications Security; 2006. p. 89–98.
4. Lewko A, Waters B. Decentralizing attribute-based encryption. 2010. CryptologyePrint Archive: Rep. 2010/351.
5. Sahai A, Waters B. Fuzzy identity-based encryption. Proceedings of EUROCRYPT; 2005. p. 457–73.
6. Bethencourt J, Sahai A, Waters B. Ciphertext-policy attribute based encryption. Proceedings IEEE Symposium Security Privacy; 2007. p. 321–34.
7. Ostrovsky R, Sahai A, Waters B. Attribute-based encryption with no monotonic access structures. Proceedings
ACM Conference on Computer and Communications Security; 2007. p. 195–203.
8. Yu S, Wang C, Ren K, Lou W. Attribute based data sharing with attribute revocation. Proceedings ASIACCS; 2010. p. 261–70.
9. Boldyreva A, Goyal V, Kumar V. Identity-based encryption with efficient revocation. Proceedings ACM Conference on Computer and Communications Security; 2008. p. 417–26.
10. Pirretti M, Traynor P, McDaniel P, Waters B. Secure attribute based systems. Proceedings ACM Conference on Computer and Communications Security; 2006. p. 99–112.
11. Rafaeli S, Hutchison D. A survey of key management for secure group communication. Comput Surv. 2003; 35(3):309–29.
12. Mittra S. Iolus: A framework for scalable secure multicasting. Proceedings ACM SIGCOMM; 1997. p. 277–88.
13. Golle P, Staddon J, Gagne M, Rasmussen P. A content-driven access control system. Proceedings Symposium on Identity Trust Internet; 2008. p. 26–35.
14. Cheung L, Newport C. Provably secure cipher text policy ABE. Proceedings ACM Conference on Computer and Communications Security; 2007. p. 456–65.
15. Goyal V, Jain A, Pandey O, Sahai A. Bounded cipher text policy attribute-based encryption. Proceedings ICALP; 2008. p. 579–91.
16. Ibraimi I, Petkovic M, Nikova S, Hartel P, Jonker W. Mediated cipher text-policy attribute-based encryption and its application. Proceedings WISA LNCS. 2009; 5932:309–23.
17. Chen N, Gerla M, Huang D, Hong X. Secure, selective group broadcast in vehicular networks using dynamic attribute based encryption. Proceedings Ad Hoc Networking Workshop; 2010. p. 1–8.