Protected Data Reclamation For Decentralised Disruption-Forbearing In Wireless Sensor Network

Tejaswini B
Asst .Professor,
Alpha College Of Engineering,
Bangalore

Ashwini S
Asst .Professor,
Alpha College Of Engineering,
Bangalore

Shilpashree S
Asst .Professor,
Alpha College Of Engineering,
Bangalore

***Abstract:* Mobile nodes bear from periodic network connectivity and repeated partition. Disruption tolerant network (DTN) provides communication in most insecure, unreliable and stressed out environment. DTN is mostly used in wireless communication, where delay is considered to be high. At times the external storage node can be misused where the data is stored, and authorization will only be given to authorized mobile nodes which can access the necessary information quickly and efficiently. The information storage's attack is a severe attack that can be easily launched by a pair of external attackers in Wireless Sensor Networks. In this attack, an attacker sniffs packets or data at one point in the network by using wrong file name or wrong secret key for corresponding file. In this system, the system proposes novel attackers detection and positioning scheme based on mobile (Location Based Server) LBS, which can not only detect the existence of Storage Node attacks, but also accurately localize the attackers for the system to eliminate them out of the storage network.**

Among several applications military application needs additional protection and privacy. For most extent access control issues can be solved by Cipher text-policy characteristic-based encryption (CP-ABE .In CP-ABE scheme encryptor defines the attribute text set that the decryptor needs to possess in order to decrypt the cipher text. The paper proposes secure data retrieval for decentralised DTNs where multiple key authorities manage their attributes independently using CP-ABE and prevent attacker sniffs. The proposed scheme provides data confidentiality, collision resistance and gives backward and forward secrecy.

Keywords Access control, Cipher text-policy attribute-based encryption(CP-ABE), Disruption tolerant network (DTN), (Location Based Server) LBS.

I.INTRODUCTION

IN many wireless network scenarios, when wireless devices carried it may be temporarily disconnected by jamming, environmental factors, and mobility, especially when they operate in hostile environments. Disruption-tolerant network (DTN) technologies provide promising solutions that allow nodes to communicate with each other in these extreme networking environments. Many applications like the military applications require increased protection for confidential data including access control methods that are cryptographically enforced

Existing system, ABE comes in two flavours called key-policy ABE (KP-ABE) and cipher text-policy ABE (CP-ABE). In KP-ABE, the encryptor only gets to label a cipher text with a set of attributes. The key authority chooses a policy for each user that determines which cipher texts he can decrypt and issues the key to each user by embedding the policy into the user's key. However, the roles of the cipher texts and keys are reversed in CP-ABE. 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 encryptors 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.

II. LITERATURE SURVEY

This section briefly presents the related works of Attribute-Based Encryption and Decentralizing Attribute Based Encryption and on mobile nodes.

Brent Waters and Sahai describes "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data"[1], at times the confidential data needs to be stored in the third party storage and hence needs to be encrypted in order to keep the data secure. At a coarse-grained level (i.e., giving another party your private key) encrypting becomes a drawback as it can be shared in a grained level. So they developed a cryptosystem for fine-grained sharing of encrypted data that is called as Key-Policy Attribute-Based Encryption (KP-ABE). In this cryptosystem, set of attributes are labelled to cipher text and private keys are associated with access structures that control which cipher texts a user is able to decrypt.

Allison Lewko and Brent Waters describes "Decentralizing Attribute-Based Encryption (ABE) system"[2] .In this system, they describe the multi authority attribute based encryption in a party can simply act as an ABE authority by creating a public key and issuing private keys to different users that reflect their attributes and no necessary to become central authority for central co ordination. A end user can encrypt data by any Boolean formula over attributes issued from any chosen set of authorities and is not collision resistant.

Muhammad Mukarram Bin Tariq, Mostafa Ammar, Ellen Zegura in their paper "Message Ferry Route Design for Sparse Ad hoc Networks with Mobile Nodes"[3]describes that Message ferrying is a type of networking paradigm , a special node called a message ferry helps in the connectivity of a mobile ad hoc network where the nodes are sparsely deployed. The challenge faced by this network is end to end connectivity and delay. The problem is faced when the nodes move in a ad hoc network as it cannot be certain at a particular location, either the node has to be stationary or the node and the ferry node has to move pro-actively in prior in order to meet at particular location. Hence message ferry route design algorithm that was designed called Optimized Way-points, or OPWP that gave high performance and route between ferry and node.

P.Yang and M. Chuah published a paper on" Performance Evaluations of Data-Centric Information Retrieval Schemes for DTNs"[4], Disruption Tolerant Network (DTN) technologies are designed to enable communications in environments where there is frequent network partioning. The design issues are (a) how data should be replicated and stored at multiple nodes and routed back to issuing node (b) how a query is disseminated in sparsely connected networks,

III. PROPOSED SYSTEM

In this section, a multi authority CP-ABE scheme for secure data retrieval in decentralized DTNs is proposed and also the system proposes novel attackers detection and positioning scheme based on mobile (Location Based Server) LBS, which can not only detect the existence of Storage Node attacks, but also accurately localize the attackers for the system to eliminate them out of the storage network.

Each local authority issues secure 2PC protocol with the central authority. Each attribute key of a user can be updated individually and immediately. Thus, the scalability and security can be enhanced in the proposed scheme. System provides data confidentiality, collusion-resistence and enables backward and forward secrecy.

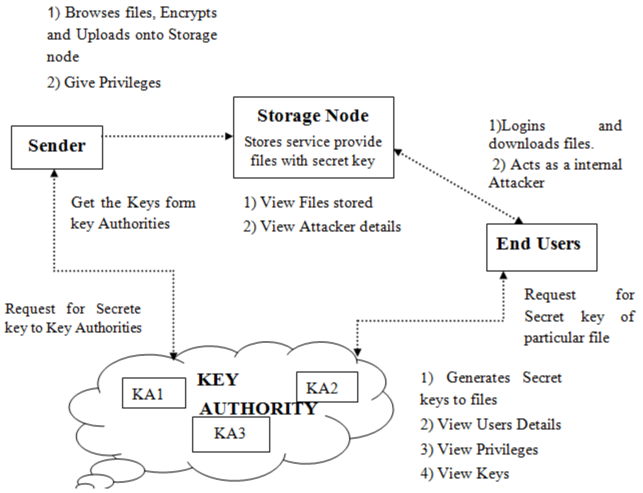
1) Browses files, Encrypts and Uploads onto Storage node
2) Give Privileges
Sender
Storage Node
Stores service provide files with secret key
1)Logins and downloads files.
2) Acts as a internal Attacker
Get the Keys form key Authorities
1) View Files stored
2) View Attacker details
End Users
Request for Secrete key to Key Authorities
Request for Secret key of particular file
KEY AUTHORITY
KA1
KA2
KA3
1) Generates Secret keys to files
2) View Users Details
3) View Privileges
4) View Keys

Fig.1. Architecture diagram of proposed system

Fig.1 shows the architecture and it consists of the following elements

1) Sender/transmitter: this entity has the confidential data which needs to be transmitted to the other end. Initially he needs to register himself to send the data. Functions like browsing, encrypting using the attribute, uploading the files to storage node is done here. Sender requests for the secret key from the key authority.

2) Key Authorities: it consists of a central key authority and many local key authorities. They generate the secrete key to the encrypted files, they can view the user details and keys from which key authority, the keys have been generated, also can view privilege given to the user to download the permission or not.

3) Storage node: this can be mobile or static. It stores the file sent by the sender along with the secret key, to keep it secure in the node. Viewing of the file stored and attackers details can be got in this entity.

4) User/receiver: This is a mobile node who wants to access the data stored at the storage node. The user needs to give the set of attributes satisfying the access policy of the encrypted data defined by the sender, hence he is considered authorised and he can decrypt the data by giving the set of attributes, else he is considered as unauthorized or an attacker.

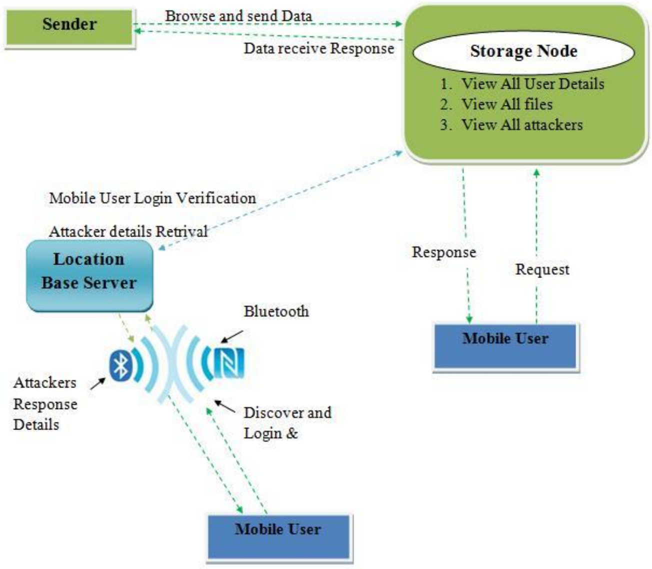

Fig.2. Architecture diagram of proposed system of the mobile part.

In order to find the attacker details in the mobile phone, the mobile phone consists of three logical parts which are involved in the data exchange. The first hardware component is the insecure communication unit of the device responsible for the Bluetooth, Location Base Server (LBS) or Mobile Device for communication with the external machine. The mobile user can connect with the LBS Server via Bluetooth device to communicate with the mobile. The user will find the Bluetooth server name and then login into mobile to view all current attackers in the Storage Node which is Delay Tolerant networks.

IV.EVALUATION RESULTS

The evaluation results in the below diagram shows the upload Delay time and the download delay time. The upload delay decreases eventually as the files get uploaded.

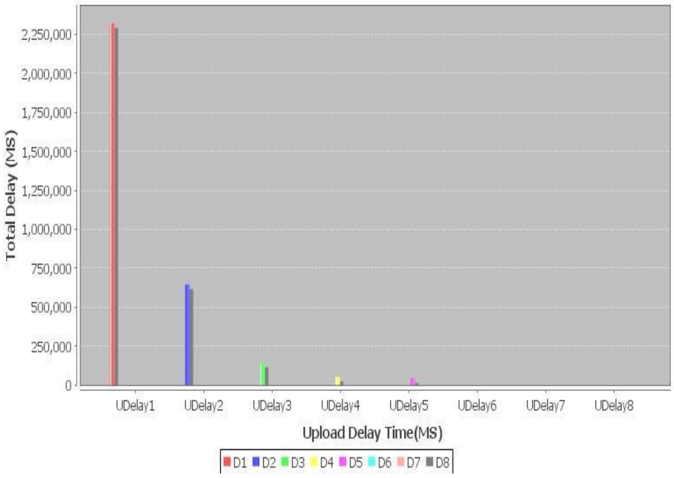

Fig.3. Upload delay time of the system.

The below diagram shows the delay in the download time.The
Download delay might be because of the location, file size, and wireless connections and it depends from one file to another.

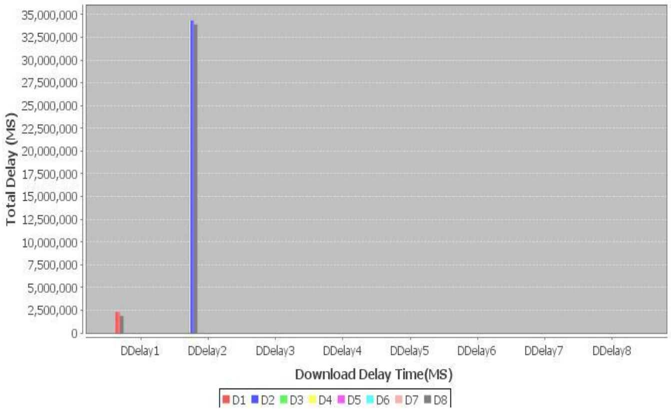

Fig 4. Download delay time of the system.

V. CONCLUSION

DTN technologies are becoming promising solutions in many critical 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 secures data retrieval issues. This also proposes a security concept to extend the present Storage network for message-based communication to detect and prevent the external attackers. It enables three interesting communication features, The asynchronous transfer provides a communication service even in areas without direct network coverage (the handset can carry the message into mobile coverage). The trust relationship between the external machine and the mobile phone is of a kind, that every user can become a potential node in this relay network.

REFERENCES

[1] Vipul Goyal Omkant Pandeyy Amit Sahaiz Brent Waters “Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data” .

[2] Allison Lewko and Brent Waters, “Decentralizing Attribute-Based Encryption (ABE) system”.

[3] 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, pp. 37–48.

[4] M. Chuah and P. Yang, “Performance evaluation of content-based information retrieval schemes for DTNs,” in Proc. IEEE MILCOM, 2007, pp. 1–7.

[5] 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.

[6] 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, pp. 29–42.

[7] Erman Ayday, Student Member, IEEE, and Faramarz Fekri, Senior Member, IEEE “An Iterative Algorithm for Trust Management and Adversary Detection for Delay-Tolerant Networks” IEEE trans. On mobile computing , vol. 11, no. 9, sep 2012

[8] A.A. Pirzada, C. McDonald, and A. Datta, “Performance Comparison of Trust-Based Reactive Routing Protocols,” IEEE Trans. Mobile Computing, vol. 5, no. 6, pp. 695-710, June 2006.

[9] Globecom 2012 - Communication and Information System Security Symposium A Security Metric for VANET Content Delivery Ikecukwu K. Azogu, Michael T. Ferreira, Hong Liu, Department of Electrical and Computer Engineering University of Massachusetts Dartmouth 285 Old Westport Road. N. Dartmouth, USA