International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

DTN Technologies Used for Secure Data Retrieval in Decentralized Military Networks

Dr. B R Prasad Babu[1], Kavyashree .G[2], T. Gayathri[3]

[1]Professor and Head, Department of Computer Science and Engineering, R & D center, SEACET, Bangalore-49, India

[2]M.Tech student, Department of CSE, SEACET, Bangalore-49, India

[3]Assistant Professor, Department of CSE, SEACET, Bangalore-49, India

Abstract: ***Development of mobile nodes in army environment such as war field or a confrontational region are likely to undergo irregularity in network connectivity and frequent partitions.DTN technologies are best solutions for wireless devices carried by armed force to imparting information with each other and access the secured information or command relied without exploiting external storage nodes. Some of the important issues in the scenario networks are the enforced by authorized policy and the policy that update the secure data retrieval. CP-ABE we are using cryptographic solution that access and control the issues. The main problem in this CP-ABE in decentralized DTNs have several security and privacy tasks with regard to the attribute revocation, backup, and information's of data that is in different networks solutions. A data that is retrieved during CP-ABE for decentralize DTNs .The proposed system that keeps the data securely.***

Keyword: Access control, Attribute-Based Encryption (ABE), Disruption-Tolerant Network (DTN), multi authority, secures data retrieval.

1. Introduction

According to army network scenarios, connections are carried by wireless equipments soldiers are sometimes cannot get connections by jammers, some environmental disturbances, and mobility, when they operate in battle-field. These technologies are becoming the best solutions for the mobile nodes that can communicate with each other in these extreme network stages. When there is no start to end connection between a sender and a receiver pair, the messages from the sender may wait in the intermediate nodes. Storage nodes in DTNs data are stored in such a way that the mobile nodes can access the data information quickly.

This applications will increase the protection and important data including control methods implemented.[1],[4],[5]. CP-ABE as a secured way of encrypting data such that as encryptor is defined in attribute that sets the data that is needs to possess in order to retrieves the secure text. Users may change the attributes at point (for example, moving their region), or the private key, key will generate each of it is necessary to make systems backup secure.

2. Literature Review

Literature review is in order to identify the background of the current information's which helps to find the existing system. So, the following information not only illustrates the background but also covers the problems that motivate to propose the solution and works. A variety of research has been done on power aware scheduling. Following section explores different references that discuss about several topics related to power aware scheduling .**Attribute Revocation:** first key revocation mechanisms in CP and KP. Their information are has more time and the keys will be sent to the users. The problem depredated the terms of the backward and forward secrecy that tells it is a considerable data's that users that's the soldiers may change their attributes frequently [4],[9].

R .Gullets also proposed attributes associated with a cipher text is exactly half of the universe size. **Key Escrow: *P***resented a distributed KP that solves the backup problem in a many authority system. This approach, all attribute authorities are participating in the keys that will distribute the way such that they cannot pull the data and link the users

3. Existing System

This Attribute-based encryption (ABE) fulfils the secure data retrieval in DTNs. ABE enables an access control over encrypted data which will the access control policies and attributes among keys and texts. When there is a policy ABE (CP-ABE) they are scalable by encrypting the data such that the sends the data defines the attribute set that the decrypt or 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.

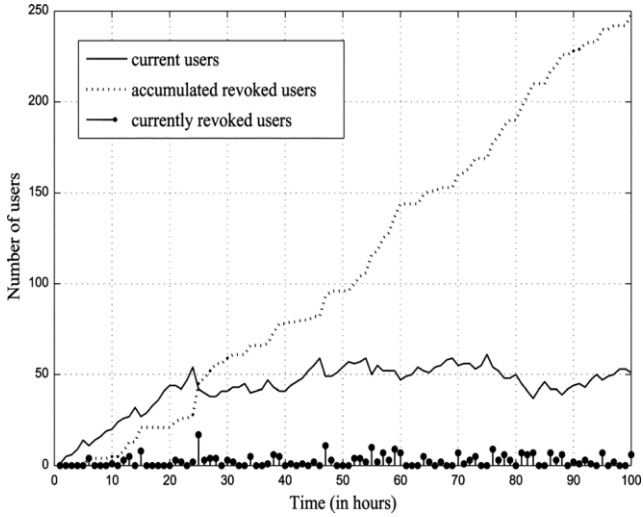

Figure 1: Number of users in an attribute group

4. Proposed System

An attribute-based secure data retrieval scheme using CP-ABE for decentralized DTNs [2][5]. They are three types: First, immediate attribute revocation will help the backward/forward data will be squired. Second, encryptors will find a fine-grained access policy authorities [2][3].Third, the key escrow problem is resolved by an escrow-free key using DTN architecture. [5][6][7].

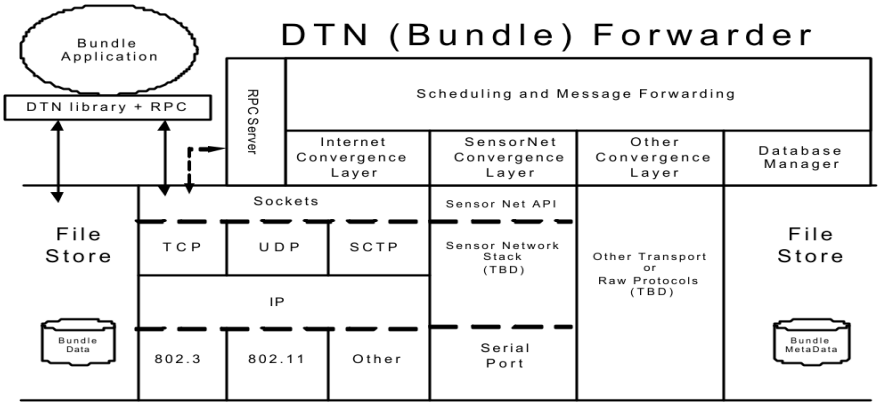

FIGURE 2. Structure of a DTN forwarder. Multiple *convergence layers*, one per protocol stack, provide a common interface to the message scheduler/forwarder.

The key problem faced by the protocol generates and issues user the secret keys by performing secure two-party computation protocol among the key authorities with their own master key[9][7].The 2PC protocol try the key authorities to obtain any master key information of each other so that none of them will generates the key. ADVANTAGES OF PROPOSED SYSTEM: **Data confidentiality, Collusion-resistance & Backward and forward Secrecy**

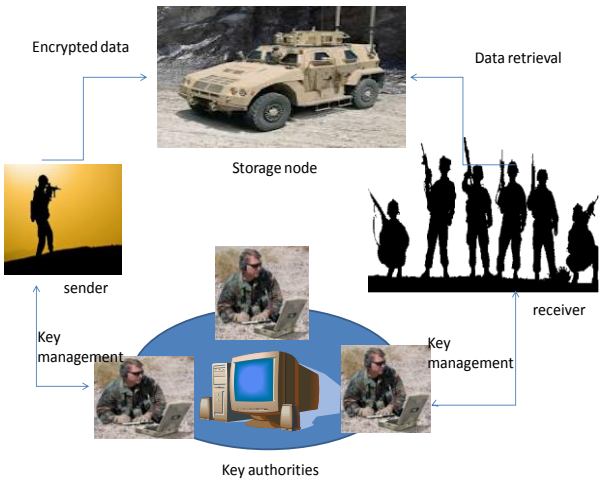

Figure 3: Architecture of secure data retrieval in a DTNs network.

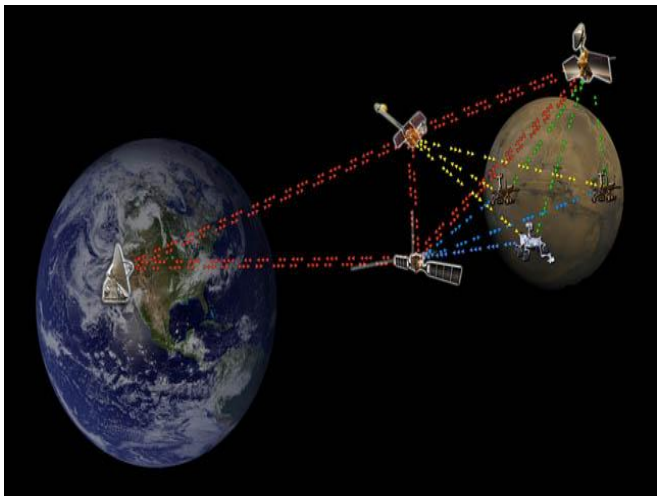

Figure 4: DTN used for Mars rover communication

5. Implementation

Analysis is the process of finding the best solution to the problem. System analysis is processed by learn about the existing problems, define objects and requirements and evaluates the solutions [7][9]. It is the way of thinking about the organization and the problem it involves, a set of technologies that helps in solving these problems.

Identification and design of the modules for implementing [8][10].

Feasibility Report: Depending on the results of the expanded to a more detailed feasibility study. By testing the system proposal according to its works, impact of the organization, ability to meet needs and effective use of the resources [6][7]. This determines the evaluate performance and cost effective of each proposed system. Select the best proposed system. Three key considerations involved in the feasibility analysis are:

- Economical Feasibility
- Technical Feasibility
- Social Feasibility

6. Conclusion

DTN technologies are successful solutions in army network applications that allow wireless devices to transmit the information is kept securely and then sends the information to all external storage nodes.

CP-ABE is a scalable cryptographic solution to the access control and secures data retrieval issues. 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 compromise or not fully trusted. We demonstrate how to apply the proposed mechanic securely and efficiently manage the confidential data distributed in the disruption tolerant army network.

References

[1] R. Swaminathan, Q. Wang, and K. Fu, "Plutus: Scalable secure file sharing on storage," 2006
[2] J. Burgess, B. Gallagher, D. Jensen, and B. N. Levine, " Routing for vehicle-based disruption networks," 1–11.2006
[3] M. Chuah and P. Yang, "Node density-based adaptive for disruption tolerant networks,"
[4] M. M. B. Tariq, "Mesage ferry route design for sparse ad hoc networks with mobile nodes," 2006
[5] M. Chuah and P. Yang, "Performance based on information retrieval schemes for DTNs," pp. 1–7.2007
[6] M. Petkovic, S. Nikova, P. Hartel, and W. Jonker, "Mediated CP-ABE and its application".2007
[7] M. Chuah, "Secure data retrieval based on (CP-ABE) system for the DTNs," Lehigh CSE Tech. Rep., 2009.
[8] A. Sahai, and B. Waters, "ABE with non-monotonic access structures," 2010
[9] J. Bethencourt, A. Sahai, and B. Waters, "Cipher text-policy encryption," 2010
[10] V.Goyal, A. Jain,O. Pandey, andA. Sahai, "Bounded CP-ABE," in *Proc. ICALP*, 2010, pp. 579–591.