A Proposed System on Disruption-Tolerant Military Networks for Secure Data Retrieval

[1]Pratiksha Khodade, [2]Vaishnavi Dhongade, [3]Sapana Bhandare, [4]Priyanka Agavane, [5]Prof. Shital Salve

[1,2,3,4] Department of Computer Engineering,
[1,2,3,4] MES College Of Engineering, Pune, India

***Abstract*— In Military environments such as a battlefield the way of communication is the main and most critical part. As in battlefield every small thing which needs to convey towards soldier were should not be leaked. Also Mobile nodes in military environments such as a battlefield or a hostile region are likely to suffer from intermittent network connectivity and frequent partitions. 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 reliably by exploiting external storage nodes. Some of the most critical part of this is data retrieval. Ciphertext-policy attribute-based encryption (CP-ABE) is a one of the best cryptographic solution to the access control issues. In this paper, they took the survey of such type of technologies as well as system which are similar and based on such technology.**

***Index Terms*— Access control, attribute-based encryption (ABE), disruption-tolerant network (DTN), multiauthority, secure data retrieval.**

I. INTRODUCTION

Disturbance Tolerant Networking is a systems administration structural engineering that is intended to give correspondences in the most temperamental and focused on situations, where the system would ordinarily be liable to continuous and enduring interruptions and high piece blunder rates that could seriously debase ordinary interchanges. It is a trial convention created by the Delay and Disruption Tolerant Networking Research Group, which works under the Internet Research Task Force.

A Different Approach to TCP/IP

DTN works utilizing diverse sort of methodology than TCP/IP for bundle conveyance that is stronger to disturbance than TCP/IP. DTN depends on another test convention called the Bundle Protocol (RFC 5050). The Bundle Protocol (BP) sits at the application layer of some number of constituent webs, framing a store-and-forward overlay system. BP works as an overlay convention that connections together various subnets, (for example, Ethernet-based LANs) into a solitary system.

Store-And-Forward

The fundamental thought behind DTN system is that endpoints aren't generally consistently joined. So as to encourage information exchange, DTN utilizes a store-and-forward methodology crosswise over switches that is more disturbance tolerant than TCP/IP. On the other hand, the DTN methodology doesn't as a matter of course imply that all DTN switches on a system would require substantial capacity limit keeping in mind the end goal to keep up end-to-end information trustworthiness

DTN utilizes a mutual structure calculation that briefly interfaces information specialized gadgets. DTN administrations are like email, yet DTN incorporates upgraded directing, naming and security capacities.

Viable DTN configuration relies on upon the accompanying elements:
1] Fault-tolerant routines and advances
2] Electronic assault recuperation
3] Degradation quality from overwhelming activity loads
4] Minimal dormancy because of temperamental switches

DTN hubs upgrade system way choice by means of a naming sentence structure that backings an expansive scope of tending to traditions for enhanced interoperability. These hubs use system stockpiling to oversee, store, and forward operations over various ways and more periods. Security additionally shields the framework from unapproved use.

In many military system situations, associations of remote gadgets conveyed by fighters may be incidentally detached by sticking, natural components, and portability, particularly when they work in threatening situations. Disturbance tolerant system (DTN) innovations are getting to be fruitful arrangements that permit hubs to correspond with one another in these great systems administration situations. Normally, when there is no limit to-end association between a source and a destination match, the messages from the source hub may need to sit tight in the middle of the road hubs for a generous measure of time until the association would be in the eventually established.

In this paper, a survey has been taken on different techniques and system which are based on DTN.

II. RELATED WORK

In [2] they explains that satellite interchanges are described by long defers, parcel misfortunes, and at times irregular network what's more, connection disturbances. The TCP/IP stack is insufficient against these hindrances and even devoted arrangements, such as execution upgrading intermediaries (PEPs), can barely handle the most difficult situations, and make similarity issues with current security conventions. An option arrangement emerges from the postponement and interruption tolerant systems administration (DTN) building design, which indicates an overlay convention, called pack convention (BP), on top of either transport conventions (TCP, UDP, and so on.), or of lower layer conventions (Bluetooth, Ethernet, and so on.). The DTN building design gives long haul data capacity on middle of the road hubs, suitable for adapting to disturbed connections, long postpones, and discontinuous availability. By separating the end-to-end way into various DTN jumps, as it were that really amplifies the TCP-part idea misused in most PEPs, DTN permits the utilization of specific conventions on the satellite (or space) joins. This paper talks about the prospects for utilization of DTN in future satellite networks. They present a wide DTN review; to make the peruser acquainted with the attributes that separate DTN from normal TCP/IP systems administration, analyze the DTN and PEP architectures and stacks, as a preparatory venture for the resulting DTN execution evaluation did in down to earth LEO/GEO satellite situations. DTN security is considered next, looking at the favorable circumstances over present satellite architectures, the dangers confronted in satellite situations, furthermore open issues. At last, the connection in the middle of DTN and nature of administration (QoS) is researched, by concentrating on QoS architectures and QoS devices and by talking about the condition of the craft of DTN exploration action in demonstrating, steering, and blockage control.

As per [1] versatile hubs in military situations, for example, a front line or an antagonistic district are liable to experience the ill effects of discontinuous system availability and regular allotments. Interruption tolerant system (DTN) innovations are getting to be fruitful arrangements that permit remote gadgets conveyed by fighters to impart with one another and access the secret data or order dependably by misusing outer capacity hubs. A portion of the most difficult issues in this situation are the implementation of approval arrangements and the strategies redesign for secure information recovery. Cipher text-strategy property based encryption (CP-ABE) is a promising cryptographic answer for the entrance control issues. On the other hand, the issue of applying CP-ABE in decentralized DTNs presents a few securities and protection challenges with respect to the quality repudiation, key escrow, and coordination of characteristics issued from diverse powers. In this paper, they propose a safe information recovery plan utilizing CP-ABE for decentralized DTNs where different key powers deal with their properties autonomously. They show how to apply the proposed instrument to safely and effectively deal with the classified information disseminated in the disturbance tolerant military system.

III. Proposed System

The ciphertext-policy ABE (CP-ABE) proposed in the system 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 ciphertext. Thus, different users are allowed to decrypt different pieces of data according to the security policy. In CP-ABE, the key authority generates private keys of users by applying the authority's master secret keys to users' associated set of attributes. Thus, the key authority can decrypt every ciphertext addressed to specific users by generating their attribute keys. If the key authority is compromised by adversaries when deployed in the hostile environments, this could be a potential threat to the data confidentiality or privacy especially when the data is highly sensitive. The key escrow is an inherent problem even in the multiple-authority systems as long as each key authority has the whole privilege to generate their own attribute keys with their own master secrets. Since such a key generation mechanism based on the single master secret is the basic method for most of the asymmetric encryption systems such as the attribute- based or identity-based encryption protocols, removing escrow in single or multiple-authority CP-ABE is a pivotal open problem. The following diagram in figure 1 shows the architecture diagram of the proposed system. In the following diagram a sender (Commander) wants to send a confidential message to the receiver (group of soldiers).

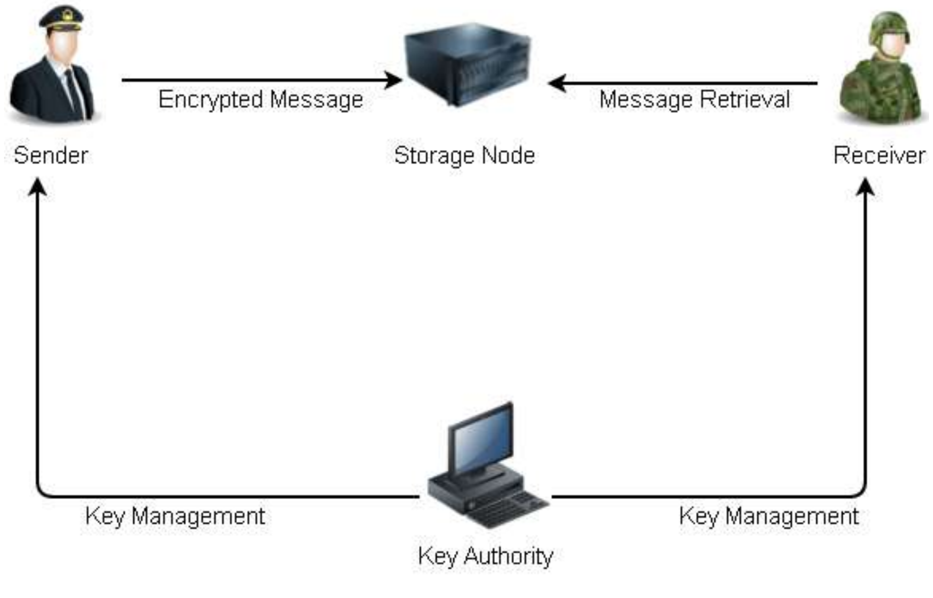

Figure 1. System Architecture

Following are the main modules in the proposed system architecture:

1. Key Authority.
2. Storage node.

3. Sender (Commander).
4. Receiver (Soldier).
5. CP-ABE Technique.

1. Key Authority: Key Authority is a key generation centre that generates public/secret parameters for CP-ABE technique. The key authority grant differential access rights to individual users based on the users' attributes. The key authority is assumed to be honest, that is, the authority will honestly execute the assigned tasks in the system.

2. Storage node: The storage node stores data received from senders and provide corresponding access to users. It may be mobile or static. The proposed system assumes the storage node to be semi-trusted.

3. Sender: Sender is a user of the system who has or wish to share confidential messages or data (For example: Commander). The confidential messages owned by the sender are store into the external data storage node for ease of sharing. The stored messages into external data storage node are also useful for delivery to users in the extreme networking environments. A sender is responsible for defining (attribute based) access policy and enforcing it on its own data by encrypting the data under the policy before storing it to the storage node.

4. Receiver: Receiver is a user of the system who wants to access the data stored at the storage node (For example: Soldier). The receiver side of the proposed system is a mobile node. If a receiver possesses a set of attributes satisfying the access policy of the encrypted data defined by the sender, and if all the attributes are matched, then the receiver will be able to decrypt the ciphertext and obtain the required message.

5. CP-ABE Method: In Ciphertext Policy Attribute based Encryption scheme, the encryptor can fix the policy, which can decrypt the encrypted message. The policy can be formed with the help of attributes. In CP-ABE, access policy is sent along with the ciphertext. A method is proposed in which the access policy need not be sent along with the ciphertext. Because of this the privacy of the encryptor is preserved. In CP-ABE technique used in the proposed system attributes are used to describe user's credentials. The user of the system who encrypts the message determines a policy in which user's are mentioned who can decrypt the message.

IV. Conclusion

DTN technologies are becoming successful solutions in secured applications that allow wireless devices to communicate with each other and access the confidential information reliably by exploiting external storage nodes. Also now a day's DTN is one the fastest growing technique for secured communication. Hence almost all of the security department like Defense, Army, and Military are using this technique for communication purpose.

References

[1] Junbeom Hur and Kyungtae Kang, "Secure Data Retrieval for Decentralized Disruption-Tolerant Military Networks", IEEE TRANSACTIONS ON NETWORKING Vol:22 No:1 Year 2014.

[2] Carlo Caini, Haitham Cruickshank, Stephen Farrell, and Mario Marchese, "Delay- and Disruption-Tolerant Networking (DTN): An Alternative Solution for Future SatelliteNetworking Applications".

[3] A. Balasubramanian, B. Levine, and A. Venkataramani, "BReplication routing in DTNs: A resource allocation approach", IEEE/ACM Trans. Netw., vol. 18, no. 2, pp. 596–609, Apr. 2010.

[4] X. Liang, Z. Cao, H. Lin, and D. Xing, "Provably secure and efficient bounded ciphertext policy attribute based encryption", Proc. ASIACCS, 2009.

[5] V.Goyal, A. Jain,O. Pandey, andA. Sahai, "Bounded ciphertext policy attribute-based encryption", Proc. ICALP, 2008.

[6] G. Loukas and G. Oke, "BProtection against denial of service attacks: A survey", 2010.

[7] S. S.M. Chow, "Removing escrow from identity-based encryption," Proc. PKC, 2009.

[8] Lindgren, A., Mascolo, C., Lonegan, M., and Mcconnell, B., "Seal2seal: A delay-tolerant protocol for contact logging in wildlife monitoring sensor networks", Proceedings of IEEE International Conference on Mobile Ad-hoc and Sensor Systems (MASS08) (Oct. 2008).

[9] J. Alonso, K. Fall, "A Linear Programming Formulation of Flows over Time with Piecewise Constant Capacity and Transit Times", Intel Research Technical Report IRB-TR-03-007, June 2003