Survey on Secure Data Retrieval Techniques for Military Networks

Roshni Khodke
Student, Sinhgad Institute of Technology,
Lonavala,
Pune, Maharashtra

V.N. Dhawas
Professor, Sinhgad Institute of Technology,
Lonavala,
Pune, Maharashtra

ABSTRACT
Wireless sensor network is having shared nature due to this security is one of the crucial feature for the network users. In commercial environment the whole thing depends on the other resource to transmit the data securely and retain the data as well in the regular medium. Transfer of data are done through intermediate node, hence data may loss due to the unauthorized persons. Mobile nodes in military environments like in battlefield region are likely to suffer from discontinuous network connectivity and frequent partitions. To solve this issue Disruption-tolerant network (DTN) is a technology which allows the node to communicate with each other access confidential information in secure manner. Most of the challenging issues in this scenario are the enforcement of authorization policies and the policies update for secure data retrieval. This paper is motivated by need of data retrieval in wireless network in secure manner. In existing system an attacker can attack the single key authority and can steal all the keys which threaten the system from security perspective. So in proposed system building multiple key authorities from where individual keys should be drawn. For efficient key generation and distribution point of view using ECC algorithm which can be more robust and secure. This algorithm is also time and energy aware.

Keywords
Wireless network, DTN, multiauthority, secure data retrieval.

1. INTRODUCTION
In the large commercial environment everything depends on the other sources to transmit the data securely and maintain the data as well in the regular medium. Wireless Network provides a sharing of data among various users by using wireless devices. So to do this we need to offer a secure communication among the network for data transfer to the whole user in the network. When there is no direct connection between a source and a destination pair, the data from the source node may need to wait in the intermediate nodes for a considerable amount of time until the connection would be established. After the connection is established, the data is transferred to the destination node. In most of military network scenarios, connections of wireless devices carried by soldiers may be detached by jamming, environmental factors, and mobility, particularly when they work in hostile environments. [1]

To allow all nodes to communicate with each other in these extreme networking environments, Disruption-tolerant network (DTN) is one of the successful solutions for transferring the data to each other. [1] Many of the military users use DTN technology for secure transfer of the data.

2. LITERATURE SURVEY
J. Bethencourt, A. Sahai, and B. Waters presented key revocation mechanisms in CP-ABE. This technique use to solve the problem of attribute revocation .Their solution to distribute a new key to valid users after the expiration. This scheme is secure against collusion attack. But there is problem of security degradation in terms of backward and forward secrecy. It is a considerable scenario that users such as soldiers may change their attributes frequently, if user join or leave the group. For e.g., position or location move when considering these as attributes. [2]

M. Chase and S. S. M. Chow presented distributed KP-ABE scheme that solves the key escrow problem in a multi authority system. In this approach, all (disjoint) attribute authorities are participating in the key generation protocol in a distributed way such that they cannot pool their data and link multiple attribute sets belonging to the same user. The advantage of this scheme is to enable more realistic deployment of attribute base access control. But One disadvantage of this fully distributed approach is the performance degradation. Since there is no centralized authority with master secret information, all attribute authorities should communicate with each other in the system to generate a user's secret key. [3]

S. Roy and M. Chuah presented decentralized CP-ABE schemes in the multi authority network environment. They achieved a combined access policy over the attributes issued from different authorities by simply encrypting data multiple times. The advantage of this scheme is flexible fine grained access policy. But the main disadvantages of this approach are efficiency and expressiveness of access policy. [4]

J. Burgess, B. Gallagher, D. Jensen, and B. N. Levine presented novel protocol called MaxProp for routing of DTN messages. MaxProp identifies the issue of scheduling packets for transmission to other peers and determining which packets should be deleted when buffers are low on space. Performance of the proposed protocol is better than the other protocols. Propose a DTN routing protocol, called MaxProp that performs significantly better than previous approaches. Proposed approach is depends upon prioritizing both the schedule of packets send to other peers and the schedule of packets to be dropped or deleted when buffers are low on space. [5]

M. Chuah and P. Yang presented in paper a plan of an information retrieval system for disruption tolerant networks (DTN). They demonstrated a content-based information retrieval system designed for DTNs. While designing author address three main issues such as first, how data should be replicated and stored at multiple nodes, second how a query should be disseminated in sparsely connected networks and third how a query response should is routed back to the

querying node. For query dissemination author used an L-hop Neighborhood Spraying (LNS) scheme and Prophet routing scheme or Highest Encounter First Routing (HEFR) scheme is used for message routing. Proposed approach achieved smaller query response time and hence achieve higher query success rate using the HEFR scheme. [6]

M. Kallahalla, Q.Wang, and K. Fu presented novel method called Plutus as cryptographic storage system to achieve secure file sharing in the presence of untrusted servers. Almost all requirements for server trust are removed and handles by single data owners as base for a secure storage system that can defend and share data at very large scales and across trust boundaries. Plutus features highly scalable key management while allowing individual users to retain direct control over who gets access to their files. Proposed approach is more secure and efficient. Plutus achieves strong security with overhead comparable to systems that encrypt all network traffic. [7]

R. Ostrovsky, A. Sahai, and B. Waters presented Attribute-Based Encryption (ABE) scheme that allows a user's private key to be expressed in terms of any access formula over attributes. Previous ABE schemes were limited to expressing only monotonic access structures. We provide a proof of security for our scheme based on the Decisional Bilinear Diffie-Hellman (BDH) assumption. Furthermore, the performance of our new scheme compares favorably with existing, less-expressive schemes. [8]

V. Goyal, O. Pandey, A. Sahai, and B. Waters proposed novel and efficient cryptosystem for fine-grained sharing of encrypted data that is Key-Policy Attribute-Based Encryption (KPABE). In proposed cryptosystem, ciphertexts are tag with sets of attributes and private keys are related with access structures that control which ciphertexts a user is able to decrypt. Proposed approach is applicable to sharing of audit-log information and broadcast encryption. It also supports delegation of private keys which subsumes Hierarchical Identity-Based Encryption (HIBE). [9]

L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker presented a system for realizing complex access control on encrypted data that we call Cipher-text Policy Attribute-Based Encryption. By using our techniques encrypted data can be kept confidential even if the storage server is untrusted; moreover, our methods are secure against collusion attacks. Previous Attribute-Based Encryption systems used attributes to describe the encrypted data and built policies into user's keys; while in our system attributes are used to describe a user's credentials, and a party encrypting data determines a policy for who can decrypt. Thus, our methods are conceptually closer to traditional access control methods such as Role-Based Access Control (RBAC). In addition, we provide an implementation of our system and give performance measurements. [10]

Table 1: Survey Table

Sr.no	System proposed	Advantage	Disadvantage
1	CP-ABE Method.[2]	Secure against collusion attack	Security degradation in term of backward & forward secrecy.
2	Distributed KP-ABE Method.[3]	It enables more realistic deployment of attribute based access control.	Performance degradation.
3	Decentralized CP-ABE Method.[4]	Flexible fine-grained access control.	Efficiency and expressiveness of access policy.
4	Maxprop: Routing Method. [5]	Propose a DTN routing protocol, called MaxProp that performs significantly better than previous approaches.	Load is increased.
5	Performance evaluation of content-based information retrieval Method. [6]	Proposed approach achieved smaller query response time and hence achieve higher query success rate.	The query load increases such that there is a buffer overflow of stored queries, Then the query success rate will drop.
6	Plutus: Novel Method .[7]	Proposed approach is more secure and efficient.	With overhead comparable to systems that encrypt all network traffic.
7	ABE Method.[8]	Performance better than existing system.	Less Expressive method.
8	KP-ABE Method.[9]	Efficient sharing of encrypted data.	Selectively shared only at a coarse-grained level.
9	mCP-ABE Method.[10]	Instantaneous attribute revocation.	No way to revoke an attribute before the expiration date.

3. ARCHITECTURAL VIEW

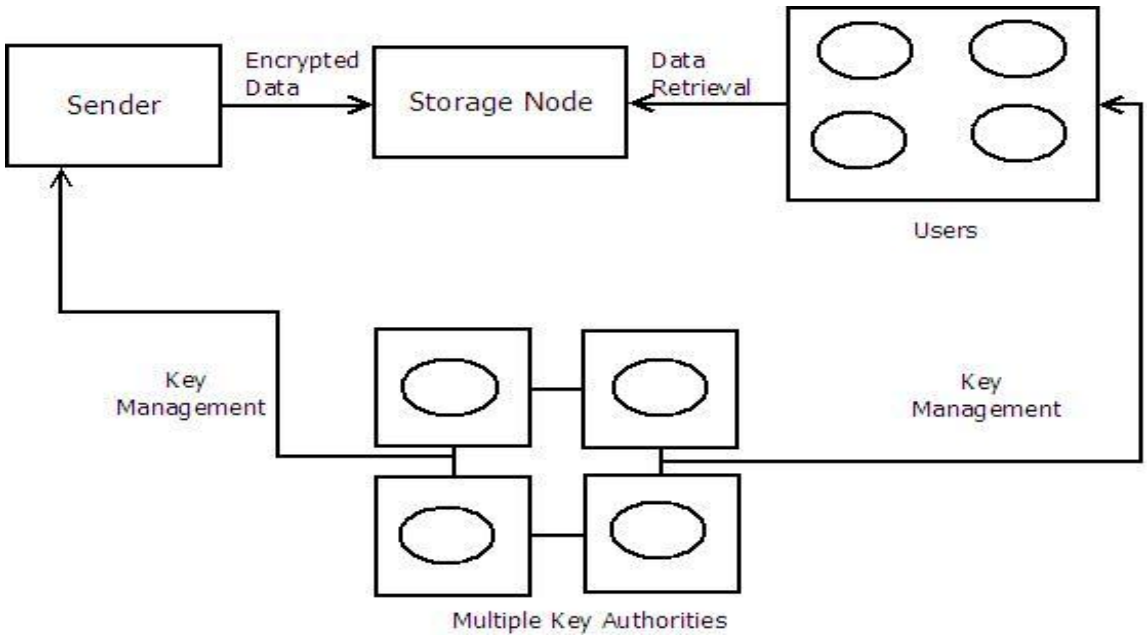

Fig 1: Architectural View

4. CONCLUSION AND FUTURE SCOPE

This paper presented an all-inclusive survey of we study a comprehensive overview of various algorithms of cryptographic method for DTN. The main features, the advantages and disadvantages of each are described. As per survey, strong needs to develop secure data retrieval in network system. In shared environment security is one of the essential factors. Mainly data transfer done using cryptographic method to provide better security.

In proposed system building multiple key authorities from where individual keys should be drawn. For efficient key generation and distribution point of view using ECC algorithm which can be more robust and secure. This algorithm is also time and energy aware. In future, improve the storage capacity by introducing multiple Data storages where each storage belongs to particular type of users.

5. ACKNOWLEDGEMENT

The authors would like to thank the researchers as well as publishers for making their resources available and teachers for their guidance. Also thankful to the reviewer for their valuable suggestions.

6. REFERENCES

[1] Junbeom Hur and Kyungtae Kang," Secure Data Retrieval for Decentralized Disruption-Tolerant Military Networks", IEEE, ACM,2014.

[2] J. Bethencourt, A. Sahai, and B. Waters,"Ciphertext-policy attribute based encryption," in Proc. IEEE Symp. Security Privacy, 2007,pp.321–334.

[3] M. Chase and S. S. M. Chow, "Improving privacy and security in multiauthority attribute-based encryption," in Proc. ACM Conf. Comput.Commun. Security, 2009, pp. 121–130.

[4] 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.

[5] J. Burgess, B. Gallagher, D. Jensen, and B. N. Levine, "Maxprop: Routing for vehicle-based disruption tolerant networks," in *Proc. IEEE INFOCOM*, 2006, pp. 1–11.

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

[7] 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.

[8] R. Ostrovsky, A. Sahai, and B. Waters,"Attribute-based encryption with non-monotonic access structures," in *Proc. ACM Conf. Comput. Commun. Security*, 2007, pp. 195–203.

[9] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proc. ACM Conf. Comput. Commun. Security*, 2006, pp. 89–98.

[10] L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker,"Mediated ciphertext-policy attribute-based encryption and its application," in *Proc. WISA*, 2009, LNCS 5932, pp. 309–323.