Survey on Encryption Techniques in Delay and Disruption Tolerant Network

Akhil V.V[1], Jisha S.[2]

[1]P.G Scholar, Department of CSE, Mohandas College of Engineering and Technology, Anad, Nedumangad, Kerala, India
[2]Assistant Professor, Department of CSE, Mohandas College of Engineering and Technology, Anad, Nedumangad, Kerala, India

Abstract— *Delay and disruption tolerant network (DTN) is used for long area communication in computer network, where there is no direct connection between the sender and receiver and there was no internet facility. Delay tolerant network generally perform store and forward techniques as a result intermediate node can view the message, the possible solution is using encryption techniques to protect the message. Starting stages of DTN RSA, DES, 3DES encryption algorithms are used but now a day's attribute based encryption (ABE) techniques are used. Attribute based encryption technique can be classified in to two, key policy attribute based encryption (KPABE) and cipher policy attribute based encryption (CPABE). In this paper we perform a categorized survey on different encryption techniques presents in delay tolerant networks. This categorized survey is very helpful for researchers to propose modified encryption techniques. Finally the paper compares the performance and effectiveness of different encryption algorithms.*

Keywords— Delay and disruption tolerant network (DTN), attribute based encryption (ABE)

I. INTRODUCTION

Internet is a better medium to communicating different devices in world wide. For transferring of message from one device to other TCP/IP protocol place a major role. TCP/IP protocol works based on certain assumptions, they are

- End to end path between source and destination is exist.
- All the routers and end stations support TCP/IP protocol.
- End point based security mechanism is highly secure.
- Retransmission based on timely and stable form.

For some situation these criteria's may fail, for this purpose introduces a new technology called DTN. DTN is the better solution for following cases.

- If there is no end to end connection between source and destination
- Long propagation delay between the nodes.
- Asymmetric data rate and high error rate etc.

DTN uses store and forward techniques for achieving the above advantages. The store and forward technique specify that whole messages or a piece of messages are moved from a storage node to storage space of another node as shown in Fig 1. Internet routers use memory chips or internet buffers to store incoming packets. But these techniques have very few millisecond storage capacities. But DTN requires persistent storage because

- A communication link to the next hop may not be available for a long time.
- User within a communicating pair may send or receive data much faster or more reliably than the other node.
- A message, once transmitted, may need to be retransmitted if an error occurs

The store and forward technique uses new protocol called bundle protocol. The bundle protocol stores information as bundle and forward to adjacent node. The structure of the bundle protocol is shown in Fig. 1.

The bundle layer in DTN protocol helps to communicate application programs to same or different set of lower layer protocols under the condition that long network delays or disruption. The bundle protocol generally contains three things, they are

- Bundle header.
- Source applications user data.
- Optional bundle trailer.

Bundle header contains one or more DTN blocks inserted bundle agent. Source applications user data specifies how to store the data, how to process the data, how to handle the data and how to dispose the data. The optional bundle trailer consisting of zero or more DTN block inserted bundle agent.

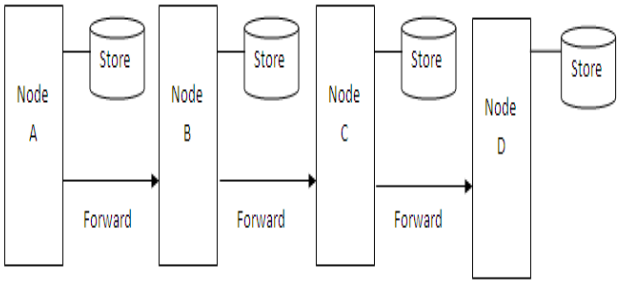

Fig. 1: Architecture of store and forward technique.

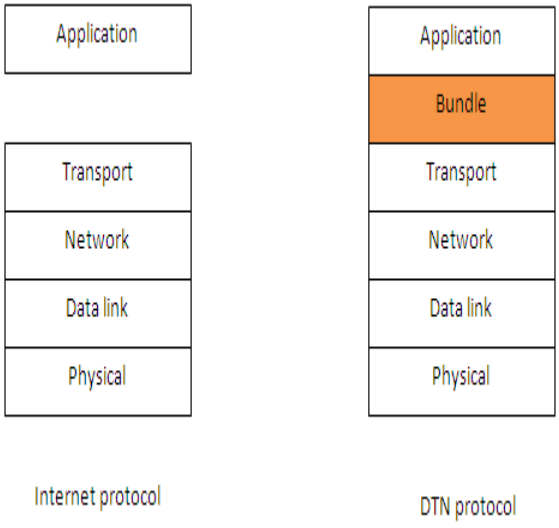

Fig. 2: Comparison of Internet protocol and DTN protocol.

Now a day's DTN has several applications, DTN is normally used in international space station communication, military and intelligence, commercial purpose like vehicle tracking, agriculture monitoring and underground mining, engineering and scientific research, environmental monitoring, public service and safety, and personal use.

The rest of the paper is organized as follows. Section II describes general attacks in DTN. General purpose encryptions techniques are described in section III. Section IV describes latest encryption techniques. In section V, we are performing a comparison of the discussed methods in section IV and section V concludes the paper.

II. GENERAL ATTACKS IN DTN

DTN faces some serious attacks in some situations; these attacks can be classified in to two. They are external attacks and internal attacks. External attacks cause congestion in routing and disturb node from providing routing information. But internal attacks access the network activities and destroy it with malicious attacks such as email attack, phishing attack etc. We can generally categorize attacks in communication network in to two. They are attacks on routing protocol and attacks on secret information. The second category is more serious than the first. [1]

Attacks on secret information occurred in three different types. They are attacks of content modification, worm attacks, and lack of cooperation in mobile nodes. The modification attacks modify the message and path and hence message is forwarded to malicious nodes in the network. As a result unauthorized users can access the information and send the bundles in bulk size and rate. To implement security some secret keys are provided for authentication and access policies. However with the help of this secret key plaintext is converted in to a cipher text. The cipher text sends from sender to receiver. The receiver can decrypt the cipher text with the help of this secret key. For this purpose key is also sending from sender to receiver. If an unauthorized person getting the key he can decrypt the message. So the other challenging attack is protection of these keys from a third party [2].

III. GENERAL PURPOSE ENCRYPTION TECHNIQUES

Generally used encryption techniques can be classified in to two types; they are symmetric key encryption and asymmetric key encryption techniques. For symmetric key encryption both encryption and decryption same keys are used. It is secure if both keys are the same. The message can be decrypted if the unauthorized person knows the key. The problem here is management of keys, transforming the keys securely i.e. not with the message. Keys are generated before the message because it is smaller than the message. Commonly used symmetric algorithms are DES [3], AES [4], and IDEA [3] etc.

In *asymmetric key encryption* technique a pair of key is used; one key for encrypting and other is for decrypting the message. Bob want to send a piece of information to Alice, Bob encrypting the message with the help of public key of Alice and Alice can decrypt the message using its own private key [5]. Hence the key management problem can be overcome. Commonly used asymmetric key algorithms are RSA [6], and ECC [7] etc. The Fig. 3 shows the general architecture of encryption technique

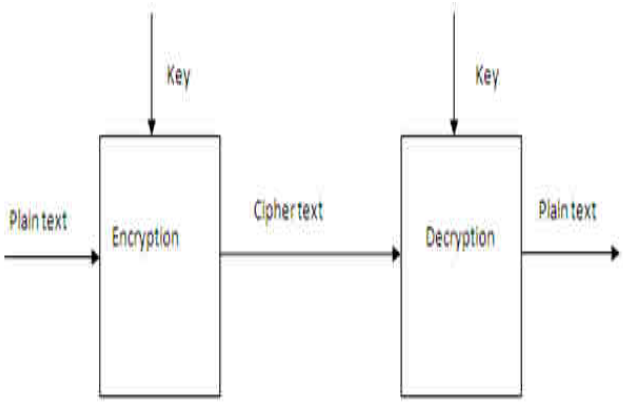

Fig. 3: General architecture of encryption technique.

IV. RECENT TREND IN ENCRYPTION TECHNIQUES

a. Attribute Based Encryption

The recent encryption techniques present in DTN field is *attribute based encryption*. Attribute based encryption is a type of public key encryption. In the case of attribute based encryption, secret key is used for performing encryption and cipher text depends on user attribute such as name, address, location, country etc. Decryption of the message is possible only when set of attributes of the key matches with attributes of cipher text. In this type of systems multiple keys should only be able to access data if at least one individual key grants access.

Attribute based encryption guaranty secure data transfer in DTN [5] [8]. The main problem occurs in this area is if some client modifies their key at some situation then handling the key is a challenging task. Attribute based encryption can be classified in to mainly two. They are *key policy attribute based encryption* (KPABE) and *cipher policy attributes based encryption* (CPABE).

KPABE is one of the secure data transfer mechanism. Here the sender generates a cipher text with a set of attributes or key provided by the key authority. Only the key authority decides a policy for each user that establishes which cipher texts he can decrypt and provide the key to each user. Using these keys receiver can decrypt it.

CPABE is another secure data transfer mechanism. The architecture of CPABE is depicted in Fig. 4. In CPABE the cipher text is encrypted with an access policy chosen by a sender, but a key is simply produced with admiration to an attributes set [5] [9]. CPABE is more suitable to DTNs than KPABE because it enables encryptions such as a leader to choose an access policy on attributes and to encrypt private data under the access structure via encrypting with the equivalent public keys or attributes. Cipher text policy attribute-based encryption (CP-ABE) is an assured cryptographic answer for the right to gain entry control issues. In the case of decentralized DTN CPABE is not that much suitable. Because handling *key escrow problem* [1], key updating problem [10] and handling light weight devices [11] [12] are very difficult. As a result some modifications are applied to CPABE. They are *Privacy Preserving Constant CPABE* (PPCCPABE), *a privacy-preserving decentralized CPABE* (PPDCPABE), *adaptable cipher text-policy attribute-based encryption* (ACPABE), *Cooperative Cipher text Policy* (CCPABE).

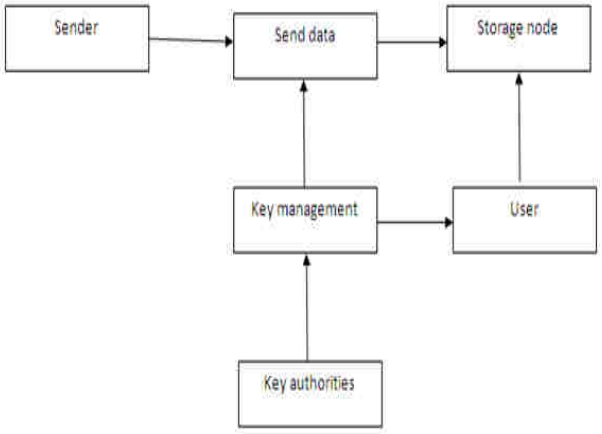

Fig. 4: Architecture of CPABE.

Zhibin Zhou et.al [13], propose a novel *Privacy Preserving Constant* CPABE (PPCPABE) construction, which enforces hidden access policies with wildcards and incurs constant-size conjunctive headers, regardless of the number of attributes. Each conjunctive cipher text header only requires 2 bilinear group elements, which are bounded by 100 bytes in total. The actual size of the bilinear group depends on the chosen parameters for the cryptosystem. Moreover, PPCPABE supports non-monotonic data access control policy. This technique significantly reduces the cipher text to a constant size with any given number of attributes. Furthermore, PPCPABE leverages a hidden policy construction such that the recipients' privacy is preserved efficiently. In the same paper, a *Constant Cipher text Policy Attribute Based Encryption* (PPCPABE) was proposed. Compared with existing CPABE constructions, PPCPABE significantly reduces the cipher text size from linear to constant and supports expressive access policies. Thus, PPCPABE can be used in many communication constrained environments. Based on PPCPABE, authors proposed an *Attribute Based Broadcast Encryption* (PPABBE) scheme that attains information theoretical minimal storage overhead. Thus, a storage restricted user can easily pre-install all required key materials to perform encryption and decryption. Through theoretical analysis

and simulation, they compared PPABBE with many existing BE solutions and they showed that PPABBE achieve better trade-offs between storage and communication overhead.

Jinguang Han et.al [14] proposes a *privacy-preserving* DCPABE (PPDCPABE) scheme where a central authority is not required and each local authority can work independently without any cooperation so that each authority can dynamically join or leave the system. Each communication party monitors a set of attributes and issues secret keys to users accordingly. To resist the collusion attacks, user's secret keys are tied to his Global identifier (GID). Especially, a user can obtain secret keys for his attributes from multiple authorities without knowing any information about his GID and attributes. Therefore, PPDCPABE scheme can provide stronger privacy protection compared to PPMAABE schemes where only the GID is protected. The advantage of this technique is to reduce the trust on the central authority and protect user's privacy; each authority can work independently without any collaboration to initial the system and issue secret keys to users. Furthermore, a user can obtain secret keys from multiple authorities without them knowing anything about his global identifier and attributes.

Junzuo Lai et.al [15] proposes *concrete adaptable CPABE* (ACPABE).They use *Key Gen*, Encrypt and Decrypt algorithms as in a traditional CPABE Scheme. Key gen algorithm takes inputs such as public parameter, master's secret key and set of attribute and produces the output a private key corresponding to the input. Encryption takes input message, access tree [15] and key generated by KeyGen algorithm to produce the output cipher text. The reverse operation performed in the decryption side. It takes public parameters, private key, and a cipher text associated with an access policy as input. If the attributes satisfies the access tree, then the algorithm will decrypt the cipher text and return a message. Adaptable CPABE scheme also includes two additional algorithms: *Trapdoor Gen* and *Policy Adaptive*. The authority runs the algorithm *Trapdoor Gen* to generate a trapdoor. Given the trapdoor, a proxy can transform a cipher text under an access policy into another cipher text of the same plaintext under any access policy using the algorithm Policy Adaptive. In this work, authors proposed yet another new variant of CPABE, namely adaptable CP-ABE. Authors introduce a semi-trusted party, called proxy, into the setting of CPABE. Given a trapdoor, the proxy is entitled to transform a cipher text under one access policy into cipher texts of the same plaintext under any other access policies. The proxy, however, learns nothing about the plaintext during the process of transformation. In this technique CPABE has many real world applications, such as handling policy changes in CPABE encryption of cloud data and outsourcing of CPABE encryption.

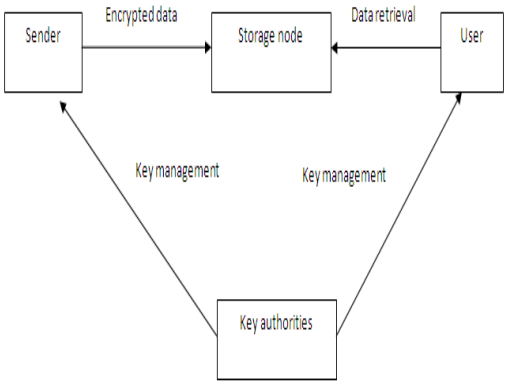

Fig. 5: Architecture of secure data retrieval in DTN network.

Cooperative Cipher text Policy Attribute-Based Encryption (CCPABE) technique proposed by Lyes Touati et.al [16] focus on the encryption algorithm and proposes a computation offloading scheme to reduce the induced overhead at resource-constrained objects. The main idea is to delegate the computation of exponentiation to other trusted neighbor devices called assistant nodes. When a resource-constrained device wants to encrypt a message, it looks for trusted unconstrained nodes in its neighborhood and it delegates to them the costly operations. Hence, the burden due to CP-ABE encryption primitive is displaced from resource-constrained devices to unconstrained ones. The advantage of this approach is that it exploits collaboration between heterogeneous nodes and accomplishes safe and efficient transmission. The Fig.5 shows the architecture of secure data retrieval in DTN network. It consist of following modules,

- *Sender* who wants to transfer a piece of information.
- *Key authorities* whom are key generation centers that generate the key for perform encryption operation.
- *Storage node* which stores data from the sender and pass to the corresponding users.
- *Users* a mobile node who want to access the data [10].

V. DISCUSSION

Symmetric algorithms and asymmetric algorithms are not suitable for DTN networks as a result attribute based

encryption techniques are introduced. Key policy attribute based encryption is one of the encryption techniques; here key authority maintains the task of key exchange between sender and receiver. As a result key escrow problems occur and sender has no control to the key generation and key distribution.

Another type of encryption technique used in DTN is cipher policy attributes based encryption. Here the sender has also got a contribution to key generation and receiver contributes attributes for key generation. But CPABE is not suitable for decentralized DTN and light weight devices; as a result some modification is performed on the CPABE. They are Privacy Preserving Constant CPABE (PPCCPABE), a privacy-preserving decentralized CPABE (PPDCPABE), adaptable cipher text-policy attribute-based encryption (ACPABE), Cooperative Cipher text Policy (CCPABE).

PPCPABE contains fixed size conjunctive headers which reduces cipher text in to a constant size with any number of attribute. We can simply say PPCPABE reduces cipher text size in to constant. PPCPABE is the better solution to avoid storage and communication overhead. PPDCPABE scheme central authority is not required each authority can work independently. PPDCPABE introduced GID to achieve and distribute information. The main attraction of this technique is reducing the trust on central authority and protects user privacy. In the case of ACPABE a proxy is created. The proxy transform message from one access policy to any other access policy. ACPABE has applications in the area of cloud data and outsourcing of CPABE encryption. CCPABE scheme node wants to transfer a message, it looks the neighbor nodes and calculates its cost of operation then only the message pass occurs. The main advantage of this technique is avoiding collaboration between heterogeneous nodes and provides safe and efficient transmission. The table I shows the most suitable DTN encryption technique for required DTN feature.

TABLE I
FEATURE WISE ENCRYPTION SOLUTION

Required Feature/ Network Type	**DTN Encryption Solution**
Storage and communication	PPCPABE
Protect users privacy in decentralized network	PPDCPABE
Bulk storage and handling bulk data	ACPABE
Safe and efficient transmission	CCPABE

VI. CONCLUSION

DTN technologies are becoming successful solution to transfer information between different wireless nodes without the presence of end to end connection and long propagation delay. Now a day's DTN contains several applications in the area of space agencies, military and intelligence, commercial purpose, public service and safety, environmental monitoring and engineering and scientific research etc. In the case of information transfer occur in DTN, there is a compulsory need for encryption, because it generally uses store and forward technique. As a result several nodes will get access to the critical information. In this paper we perform a survey on different encryption technique used in DTN networks. This survey shows that cipher policy attribute based encryption is the comparatively better technique. But some situations like decentralized DTN some modifications are required on base algorithms which guarantee better results.

REFERENCES

[1] Sonika Gandhi, A.N. Jaiswal,, "A Method for Detecting Attacks on Delay Tolerant Network," International Journal of Advanced Computational Engineering and Networking, Volume-2, Issue-6, June-2014.

[2] Sarawagya Singh, Elayaraja.K, "A survey of misbehaviors of node and routing attack in delay tolerant network," International Journal of Science, Engineering and Technology Research, Volume 4, Issue 2, February 2015.

[3] P. Eronen, Ed.Nokia, "DES and IDEA Cipher Suites for Transport Layer Security (TLS)," RFC 5469, February 2009.

[4] JH. Song, R. Poovendran, "The AES-CMAC Algorithm," RFC 4493, June 2006.

[5] Dhiren Kumar Dalai, P. Elumalaivasan, Sreejith V. P., "An analysis on attribute based encryption for secure data retrieval in DTNs," International Journal of Advance Research In Science And Engineering, Vol. No.4, Issue No.02, February 2015.

[6] J. Jonsson, B. Kaliski, "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1", RFC 3447, February 2003.

[7] S. Blake-Wilson, N. Bolyard, V. Gupta,"Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS)," RFC 4492,May 2006

[8] SuvarnaPatil,Geetha R. Chillerge, " Delay Tolerant Networks – Survey Paper," Int. Journal of

Engineering Research and Applications, Vol. 4, Issue 2(Version 2), February 2014.

[9] K. Kalaiselvi and B.Kabilarasan " Cipher Text-Policy Attribute based Encryption for Secure Data Retrieval in Disruption-Tolerant Military Networks," International Journal of Emerging Technology in Computer Science & Electronics,, volume 11 issue 3 –November 2014.

[10] Junbeom Hur and Kyungtae Kang, "Secure Data Retrieval for Decentralized Disruption-Tolerant Military Networks," IEEE Transactions on Networking vol:22 no:1 year 2014.

[11] Jianting Ning, Xiaolei Dong, Zhenfu Cao, Lifei Wei,and Xiaodong Lin, "White-Box Traceable Ciphertext-Policy Attribute-Based Encryption Supporting Flexible Attributes," IEEE Transactions on Information Forensics and Security, vol. 10, no. 6, June 2015.

[12] Fuchun Guo, Yi Mu, Willy Susilo, Duncan S. Wong, and Vijay Varadharajan, "CP-ABE With Constant-Size Keys for Lightweight Devices," IEEE transactions on information forensics and security, vol. 9, no. 5, May 2014.

[13] Zhibin Zhou and Dijiang Huang, "Efficient privacy-preserving Ciphertext-policy attribute based-encryption and broadcast encryption," IEEE Transactions on Computers, vol. 64, no. 1, January 2015.

[14] Jinguang Han, Willy Susilo, Yi Mu, Jianying Zhou,,and Man Ho Allen Au, "Improving Privacy and Security in Decentralized Ciphertext-Policy Attribute-Based Encryption," IEEE Transactions on Information Forensics and Security, vol. 10, no. 3, march 2015.

[15] Junzuo Lai, Robert H. Deng, Yanjiang Yang, and Jian Weng "Adaptable Ciphertext-Policy Attribute-Based Encryption," Springer International Publishing Switzerland 2014.

[16] Lyes Touati, Yacine Challal, Abdelmadjid Bouabdallah "C-CP-ABE: Cooperative Ciphertext Policy Attribute-Based Encryption for the Internet of Things," International Conference on Advanced Networking, Distributed Systems and Applications, 2014, B_ejaia, Algeria. pp.64-69, 2014.