ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 4, April 2015

A Survey Of Secure Data Transfer In Disruption Tolerant Military Network

E K Girisan[1], Shidha S[2]

Assistant Professor of Computer Science, Sree Narayana Guru College, Coimbatore, Tamil Nadu, India[1]

M.Phil. Scholar, Department of Computer Science, Sree Narayana Guru College, Coimbatore, Tamil Nadu, India[2]

Abstract: With this shared environment, security is one of the essential factors for the network users. Transfer of data are done through intermediate node, hence data may loss due to the unauthorized persons in the intermediate node. For this issue Disruption-tolerant network (DTN) is a technology which allows the node to communicate with each other in secure manner. DTN technology were used to transfer the data with the help of cryptographic method that provide a most security factor for the data, here the data were encrypted in some format, hence if hacker hack the data means they cannot know the message which they transmitted from the one to another node. For this issue this survey provides a various technology of transferring data with the secure manner.

Keywords: Wireless network, DTN, Military environment and secure transfer of data.

I. INTRODUCTION

Network provides a sharing of data among different users with the help of wireless devices. For this, a network must provide a secure communication among the network for data transfer to the entire user in the network. With the wireless network, transfer of data where done with the help of the intermediate node, here data may be lose because of unauthorized user in the network may hack the data. Disruption-tolerant network (DTN) is a technology which allows the node to communicate with each other in secure manner [1]. It is one of the successful solutions for transferring the data in network. Most of the military users use this technology for secure transfer of the data. In the large number of outgrowing commercial environment such as military each and everything based on the another sources to broadcast the data strongly and maintain the data as well in the regular medium. Usually, when there is no end-to-end communication among a source and a destination pair, the data from the source node may want to stay in the intermediate nodes for an extensive amount of time until the connection would be ultimately established. After the connection is ultimately established, the data is delivered to the destination node.

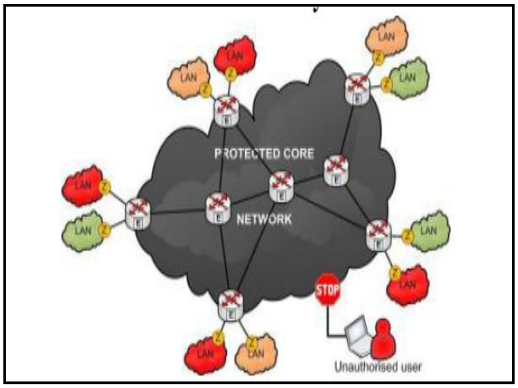

Fig: 1 Military Network

DTNs maintain interoperability of networks by cooperating a long disruptions and delays among those networks, and by communicating among the communications protocols of those networks. DTNs can accommodate many kinds of wireless technologies, including radio frequency (RF), ultra-wide band (UWB), free-space optical, and acoustic (sonar or ultrasonic) technologies [2]. Transportable nodes in military environments, for example, in an antagonistic area are horizontal to practice in endure of asymmetrical system network and numerous partitions. Disruption-tolerant network (DTN) modernisms are receiving to be productive results that authorize remote device conveyed by officers to speak with one another and admit the private data or secret data or beckon unvaryingly by neglecting outside capacity nodes or storage nodes. A DTN node can forward package between two or more other nodes in one of two situations they were Routing and Equivalent Forwarding. In DTNs, data where stored or pretend such that only authorized mobile nodes can entrée the required information rapidly and efficiently. In DTN, the multiple authorities' problem and to managing their own attribute keys independently as a decentralized DTN. In Military environment network have to provide a better secure manner of data transferring mechanism among the nodes [3, 4]. This survey shows the comprehensive study of many techniques for the sharing of data in the network.

II. LITERATURE REVIEW

This section deals with the many authors approaches of various technique and some approaches have a few benefited for sharing the data in network, but network have to provide better security also for the network users. The aim of this survey is to provide a comprehensive study of various researchers' approaches and their limitations. From the paper [5] author analyze the data sharing in the distributed system and their issues, to solve the issues they proposed the CP-ABE. They believe that Cipher text Policy attributes based encryption (CP-ABE) is becoming a guaranteed technique for solving the issues

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 4, April 2015

in data sharing. Users of distributed Data sharing want their data in safe and secure manner. Distributed data such as online social networking or cloud computing, user were demands in the security concerns of distributed data. The main issue in this sharing of data is access mechanism of unauthorized person. Here the owner of data can identify the admittance to their own strategy and user attribute pertain the data policy for release. Here the main downside is problem of key escrow, advantage is shipped. Capable to decrypt any message by producing a secret key, key generation center, addressed to an explicit user. Therefore, the author analyzes the special techniques to solve the encryption methods and attribute based data sharing.

From paper [6] the authors were analyze the DTN technologies are considered to be the successful solutions, which allow nodes to exchange with each other in the tremendous networking environments. Most challenging issues here are the insistent of authorization policies and the policy updating for protected data reclamation. For data sharing mechanism attribute-based encryption (ABE) is one of the promising approaches to full fill the necessities for secure data reclamation in DTN. Their existing paper work were engross in the cipher text-policy attribute-based encryption (CP-ABE) presentation, which present a scalable way of encrypting data such that the encrypter identifies the feature set that the decrypted wants to procedure for decrypting the cipher text. Hence, the difficulty of pertaining CP-ABE in decentralized DTN outcomes in numerous security and privacy confronts with observes to the characteristic retraction, key escrow, and synchronization of attributes issued from dissimilar authorities. Hence, a secure data reclamation method is desirable for using CP-ABE for decentralized DTNs where multiple key authorities direct their attributes separately. The drawback here is that the updating of fields is not so competent and high complexity.

P. Yang and M. Chuah et al [7] analyze several approaches for the distribution of data in the network, and they have been proposed for multicast routing in DTNs presumptuous the accessibility of dissimilar amounts of knowledge about network topology, etc. and they have propose a context-aware adaptive multicast routing (CAMR) approach to switch different network situation improved performance than the existing approach of multicast rescue schemes for DTNs. Their approach is to address the confronts of opportunistic association connectivity in DTNs.

The CAMR approach can accomplish the maximum message delivery ratio with comparable interruption routine especially when the nodes are very sparingly connected. They also execute compassion examination on the tunable limitation of our CAMR approach and estimate the delivery routine of CAMR in unlike scenarios e.g. special number of groups, different maximum node speeds. From paper [8] they proposed the approach of secure transmission of the data in the distributed network of regular transmission with the help of cipher text. Hence handling of cipher text scheme will provide guaranteed performance for the secure information sharing. In their system their approach switched to present a secure data release proposal with CP-ABE for decentralized DTNs, where multiple key authorities direct the key attributes autonomously. Their proposed approach show how proficiently and securely manages the private data in distributed network architecture.

John Burgess, Brian Gallagher et al [9], attempt to direction network messages using sporadically connected nodes. Routing is difficult in such environments because peers have slight data about the position of the separation network and reassign opportunities among peers are of imperfect duration. The author proposed the MaxProp, it is one of the protocol for successful routing of DTN messages. MaxProp is related to the prioritizing both the program of packets sharing to another peers and the program of packets to be dropped. This precedence is based on the path likelihoods to peers according to past data and also on numerous harmonizing mechanisms, together with acknowledgments, a head-start for new packets, and lists of earlier intermediaries. Their evaluations show that MaxProp achieves better than protocols that have admittance to an oracle that knows the program of meetings among peers. Their network, called UMassDieselNet, serves a huge geographic area among five colleges.

They also appraise MaxProp on replicated topologies and show it execute well in an extensive assortment of DTN environments. From this paper [10], author proposed an attribute-based secure data reclamation method using CP-ABE for decentralized DTNs. Their proposed method achieves. Immediate feature revocation develops backward/forward privacy of private data by tumbling the windows of vulnerability; encryptors can classify a fine-grained admission policy with any monotone admittance structure below attributes issued from any selected set of authorities, the key escrow problem is determined by an escrow-free key issuing protocol that develop the attribute of the decentralized DTN architecture.

The key issuing protocol produce and issues user secret keys by achieves a secure two-party computation (2PC) protocol between the key authorities with their own master secrets. The 2PC protocol prevents the key authorities from attaining any master secret information of each other such that none of them could produce the whole set of user keys alone. Thus, users are not requisite to fully hope the authorities in order to defend their data to be shared.

From the view of [11] with this current world and technology the security is more significant in all fields. The data that is shared among any must be repossessed strongly. For this secure data repossession they use cryptographic solutions. Disruption Tolerant Network (DTN) technologies have become unbeaten solutions that authorize wireless devices to share with one another and admittance the leadership consistently by developing the

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 4, April 2015

additional storage nodes. The cryptographic explanations used for the recouping of data are encryption algorithms.
From [12] they were analyzed the DTN in wireless network. It is a sporadically associated mobile network. Here, at utmost time there does not survive a clear way from source to the destination. It also has a restriction in network resources. The DTN allows communication only if it is in the broadcast range. Because of this restriction there is a possibility of reducing the received packets by the egotistical or malicious nodes. Finally this escorts to attacks. Many methods were proposed to resolve the problems which are transpired in DTN. Their survey is referring some approaches that are used to conquer diverse problems in the Disruption Tolerant Network.

III. SECURE TRANSMISSION USING DIFFERENT METHODS

In network data sharing is one of the essential one, they were occurred lot of issues while transferring of data and they were no surety of data among the nodes in DTN. For those issues they were use many techniques like cryptographic method of cipher text, encrypted text, ABE, etc. using those technique they were some limitations were occurred this survey provide those limitations they are,

3.1 DTN operations

The DTN operations were (i) Neighbor determination: Peers must determine one another before a sharing occasion can commence; and they do not know next opportunity when will begin. (ii) Data Transfer: While two peers meet, the amount of data they can sharing is incomplete. Peers do not know the period of each opportunity. (iii) Storage management: As packets are established from a neighbor, each peer must supervise its finite local buffer space by selecting packets to remove according to some instructions or rules.

3.2 Cryptographic method

Using the cryptographic method they control the access issues in the network, they were guarantee about right to gain entrance control issues in network. Cipher text method is one of the techniques for encrypting the data into some format like mingle of work so incase an information may leak means the message may not known by anyone because on mingle of words. In this cryptographic method they were played in 2 role encryption and decryption. Sender of the node share the information from one to another in the network share the message in the format of mingled data with the help of private or public key they were called encryption. Another one is decryption the receiver of the node decrypt the data or removes the mingled word with the help of the receiver private or public key. Then the message will show clearly to the receiver node [13].

3.3 Attribute based encryption

The idea of Attribute based encryption (ABE) is a guaranteeing method that satisfies the fundamentals for secure data recovery in DTNs. ABE distinctiveness a system that authorize a right to gain entry control over tousled information exploiting access control approaches and recognized behaviors among the private keys and ciphertexts. Another one is ABE, the problem of using ABE to DTNs provides less security and protection challenges were occurred. Since only some of clients may modify their associated property quicker or later or some private keys may be bargained, key renouncement (or promote) for each one attribute is essential with an explicit end goal to make frameworks secure. Hence, this problems is considerably more bothersome, mostly in ABE frameworks. ABE comes in 2 way they were key-policy ABE (KP-ABE) and ciphertext-policy ABE (CP-ABE) [8].

3.4 Key-Policy ABE

In network KP-ABE is one of the secure data transfer mechanism, here the encryptor only acquire to make a ciphertext with a set of attributes or a key. Only the key authority decides a policy for each user that establishes which ciphertexts he can decrypt and provide the key to each user by embedding the policy into the user‟s key. In KP-ABE, attributes are used to describe the encrypted data and policies are built into users' keys [8].

3.5 Ciphertext-Policy ABE

In network CP-ABE is another secure data transfer mechanism In CP-ABE, the ciphertext is encrypted with an access policy chosen by an encryptor, but a key is simply produced with admiration to an attributes set. CP-ABE is more suitable to DTNs than KP-ABE because it enables encryptors 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. Ciphertext-policy attribute-based encryption (CP-ABE) is an assured cryptographic answer for the right to gain entry control issues. In any case, the issue of applying CP-ABE in decentralized DTNs provides a few securities and defense challenges as to the property disavowal, key escrow, and synchronization of distinctiveness issued from distinctive powers [14].

IV. CONCLUSION

In this survey, we study a comprehensive overview of various algorithms of cryptographic method for DTN. In this shared environment security is one of the essential one. In DTN transfer of data were done in intermediate node in secure manner. It provide the data transfer using cryptographic method to provide better security, here the data were encrypted in some format, hence if hacker hack the data means they cannot know the message which they transmitted from the one to another node. For this issue this survey provides a various technology of transferring data with the secure manner.

REFERENCES

[1]. Ioannis Psaras, Lloyd Woodb, Rahim Tafazolli, "Delay-/Disruption-Tolerant Networking State of the Art and Future Challenges.
[2]. Delay- and Disruption-Tolerant Networks (DTNs) A Tutorial.
[3]. Mooi-Choo Chuah and Peng Yang, "Performance Evaluation of Node Density-Based Adaptive Routing Scheme for Disruption Tolerant Networks1

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 4, April 2015

[4]. Anjula Mehto and Meenu Chawla, "Comparing Delay Tolerant Network Routing Protocols for Optimizing L-Copies in Spray and Wait Routing for Minimum Delay", CAC2S 2013
[5]. Sribhashyam Sathvik and K.M.V Madan Kumar, "A Strategic Review on Cipher Text Policy Attribute Based Encryption". 2650-2654, December 2014
[6]. S.Revathi 1, A.P.V.Raghavendra, "Advanced Data Access Scheme in Disruption Tolerant Network" Vol. 2, Issue 10, October 2014.
[7]. P. Yang and M. Chuah, "Context-Aware Multicast Routing Scheme for Disruption Tolerant Networks"
[8]. Praveena.S, RajeshKannan.C, "Data Rescue Process in Network Medium with Higher End Security Measures" Volume 3 Issue 11, November 2014.
[9]. John Burgess, Brian Gallagher et al, "MaxProp: Routing for Vehicle-Based Disruption-Tolerant Networks".
[10]. Arshiya Tabassum R.A.Khan, Ashwitha Reddy, "Secure Data Retrieval For Decentralized Disruption Tolerant Military Network".
[11]. A.Rekha, P.Anitha, A.S.Subaira, C.Vinothini, "A SURVEY ON ENCRYPTION ALGORITHMS FOR DATA SECURITY", Volume: 03 Issue: 12 | Dec-2014.
[12]. D.S.Delphin Hepsiba, S.Simla Mercy and S.Prabu, "Secured Data Forwarding Technique in Disruption Tolerant Networks-Survey". Vol. 3, Issue 2, February 2014.
[13]. Nalin Subramanian, Chanjun Yang, and Wensheng Zhang, "Securing Distributed Data Storage and Retrieval in Sensor Networks"
[14]. Thrasyvoulos Spyropoulos, Rao Naveed Bin Rais, et al "Routing for Disruption Tolerant Networks: Taxonomy and Design".

DOI 10.17148/IJARCCE.2015.4414