The Significance of Delayed and Disrupted Tolerant Networks for Challenged Internet Where the End Nodes are Inconsistent

Y. Sobhan Babu,
Research Scholar,
Shri Venkateshwara University.

Dr Duvvuri B K Kamesh,
Professor.

Abstract- Disruption Tolerant Network (DTN) innovation is becoming dominant solution that allows wireless devices carried people to communicate with each other and access the private or confidential information by exploiting external storage nodes. Now a day's people want to store and share their data without worrying about how they internally work. Attribute based encryption has a great role in data sharing by providing great security and access control on data. This can be achieved by using encryption and decryption process of data. Access structure is a method used in security systems, which makes possible in sharing the resources in secured manner. The access tree structure makes the policy defines way of accessing the resources by the heterogeneous parties need to work together to get a resource. Policy over attributes has been defined along with access tree structure by using CP-ABE. Cipher text policy attribute-based encryption (CP-ABE) is a one of the best cryptographic solution in access control issues. CP-ABE is a very complex access control method on encrypted data. The CP-ABE provides match between user's private key and cipher text, and then only decryption is possible. In the cipher text-policy attribute-based encryption scheme, each user's private key (decryption key) is tied to a set of attributes representing that user's permissions. The DTN uses CP-ABE methodology to store and forward data on the network. DTN supports the internet in challenged Mobile Networks, Media Networks, Military Ad-Hoc Networks or Sensor Networks, etc. DTN's are designed to work in environments where end-to-end paths may not be available. In DTN bundle protocol is used for unstable communication network areas .It combines data into bundles and transmits the bundle data using a store and forward mechanism. It is also helps to provide connection among different subnets as a single network.

Keywords: TCP/IP, Internet, CP-ABE, Switches, Routers, Nodes, DTN, Throw-Box

I. INTRODUCTION

The TCP/IP model is basically an advanced model of the OSI model. TCP is a connection-oriented network protocol .The present TCP/IP related Internet service provides inter-process communication where the source node and destination is connected. Delayed Tolerant Networking is an advanced architectural model over the TCP/IP. Space Communication is implementing a set of international high standards, on the whole referred to as Disruption Tolerant Networking. DTN supports the internet in challenged Mobile Networks, Media Networks, Military Ad-Hoc Networks, Sensor Networks, etc. DTN's are designed to work in environments where end-to-end paths may not be available.[Dr. Farid Farahmand, Delay Tolerant Networks: Challenges and Applications] It is a trial convention implemented by the Delay and Disruption Tolerant Networking Research Group, which works under the Internet Research Task Force and it is a different Approach over TCP/IP. DTN works s 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 mechanism.

II. TCP/IP & INTERNET

The most popular network protocol in the world, TCP/IP protocol suite, was designed in 1970s by DARPA (Defence Advanced Research Projects Agency) scientists - Vint Cerf and Bob Kahn. They are treated as fathers of the Internet. TCP/IP, or the Transmission Control Protocol/Internet Protocol, is a set of communication protocols. In general all the networking devices are communicating because of TCP/IP. TCP/IP can also be used as a communications protocol in a private network.[history computer.com/ Internet/ Maturing/ TCP IP. html]. The arrangement of the current Internet service model is depend on a few expectations. They are - the continuation of end to-end path connection between a source node and destination node, and low round-trip latency (intermission) between any source node and destination node . However these arrangements are not suitable or not strong enough for other types of networks arranged by the movements of network participants. Here understanding and influencing the participants' motions can have a significant impact on network performance.

III. DELAY AND DISRUPTION TOLERANT NETWORK

The modern wireless networks have provided a wide range of applications making it possible to successfully interconnect devices and systems which have the wireless connection facility, such as mobile phones, tablets, laptops etc. all around the Globe. The internet TCP/IP protocol performance is capable where the end nodes are in connection. A robust protocol is introduced where the the source and end nodes connection is inconsistence, called Disrupted Tolerant Network. It uses different methodology than TCP/IP. DTN uses a bundle Protocol, which is very stronger to delay or disruption networks than TCP/IP. The Bundle Protocol (RFC 5050), sits at the application layer of TCP/IP in webs . The bundle protocol uses a store and-forward technology where the source nodes and end nodes are not continuously in connection. It stores the sender data at the intermediate nodes and retransmits from closest Node rather than sender. It supports information exchange in the process of store-and-forward methodology over switches that are more delayed

and disturbance tolerant areas than TCP/IP [Pratiksha Khodade, Vaishnavi Dhongade, Sapana Bhandare, Priyanka Agavane, Prof. Shital Salve].

Figure 1 : Store and Forward Message

DTN administrations are like email, yet DTN incorporates upgraded directing, naming and security capacities. There are different paradigms on Delay and Disturbance Tolerant Networking Process. But a new research is termed as Vehicular Delay Tolerant Network (VDTN) is proposed. VDTN architecture appears as a network architecture proposal based on DTN architecture that aims to provide innovative solutions for challenged vehicular communications. Anyhow, the routing algorithm in VDTNs is still under study[Syed Hassan Ahmed ; Hyunwoo Kang ; Dongkyun Kim] . The major difference between Conventional Internet (IP packet forwarding) and DTN (using RFC 5050 Bundle Protocol) is IP packet forwarding is capable of Independently handled packets with immediate forward or discard, and the DTN (using RFC 5050 Bundle Protocol) Unitary Transfer of 'Bundles' with Store, Carry and Forward at each intermediate hop node, nodes maybe mobiles. Hence 'carry' from one location to another location.

Consigning the security issues has been one of the major focuses in DTNs [Kate, A. Zaverucha, G.M. Hen Gartner, U, 2007]. Security establishment in DTN range from reckoning upon the background circumstances and application, however authentication and privacy are fundamentally critical. These security assurances are hard to build up in a network which is without consistent availability, on the grounds that the network prevents sophisticated cryptographic protocols, obstructs key exchange and every mobile device must recognize other irregularly visible devices. Solutions have regularly been adjusted from versatile ad hoc networks and distinguished security analysis, for example, the utilization of decentralized certificate authorities. Unique solutions from the Delay Tolerant Networking Research Group2 include: Identity based encryption [Oliveira et al., 2007] [Geng Yang, Chumming Rong, Christian Veigner, Jiangtao Wang and Hongbing Cheng, 2006] and usage of Gossip protocol [Ruggero Lanotte and Massimo Merro, 2011]. Coming to Military DTN's, the problem here is not just the lack of continuity in network but also the other external disturbances such as jamming, inconsistent mobility of the nodes, damage causing agents, eavesdropping by the opponents and many other adversaries. Military applications need advanced organized information including access control paths that are cryptographically developed [M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, 2003] [L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker, 2009]. The DTN uses CP-ABE methodology to store and forward data on the network. In CP-ABE methodology, key authorities cannot access the secret keys of all other users and this leads to conclusion that keys authorities do not collude with one another. [Y.Sobhan Babu, Dr Duvvuri B K Kamesh-Scenario of Cipher text Policy Attribute Based Encryption for Secure Data Sharing-2017]. There are different levels of implementations for storage and forward data through nodes in Delayed and Disrupted Tolerant Networks. Nodes play the important Role in store and forward mechanism. Here the data is reserved and reproduced through the privileged and authorized nodes can access/share the needed data amongst themselves in an efficient , effective and a rapid way. Generally , it is apt to give distinguished access approaches such that information access frames are classified over client attributes or designations , which are controlled by the key authorities. Therefore, it is a Logical assumption that diverse key authorities are likely to deal with their own particular attributes for troopers in their deployed areas or a level or rank in an organization, a profession, or society, which could be distinguished by continuous change or vigorous activity, high effectiveness in nature. We advert this DTN schematic where numerous authorities issue, furthermore, deal with their own attribute keys autonomously as a decentralized DTN[A. Lewko and B. Waters, 2008]. With the development of wireless technology and networking, wireless mobile devices such as laptop, cell phone and personal digital assistant have become the essential parts in our daily life to help people obtain information. Compared with the wired networks, the wireless networks can cover more regions and the deployment tends to be relatively convenient and flexible, meanwhile the resultant ad hoc networking brings new challenges to the network researchers. Instead of assuming fully connected networking state in traditional wireless networks, the mobility of wireless nodes, the limited transmission range and low-density nodes could cause a partitioned network which has no instantaneous communication path between the source and destination. Every mobile node in such network could participate in routing through forwarding data to neighbouring nodes within the transmission range and the communication can be finally achieved by means of store-carry-forward message transmission. Such networks with intermittent connectivity are usually called disruption tolerant networks or delay tolerant networks or (DTNs), in which the network application is subject to longer delay.

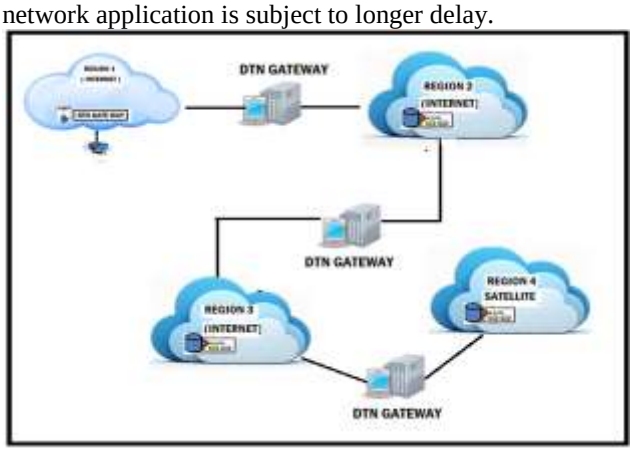


Figure 2 : Delayed and Disrupted Tolerant network Architecture

Despite of the likely longer communication latency, the advantages and applications of DTNs should not be neglected. For one thing, the networking only relying on the cooperation of wireless nodes without infrastructure provides a low-cost communication mode.

3.1 SWITCHES, ROUTERS & NODES

Switches are the networking devices, which are used to connect different devices on networks. A switch receives data from source and sends to the other devices which are connected through switch. Generally switches are used in two ways – Managed Switches and Un Managed Switches. Managed switches are more control on LAN, But Un Managed switches are used to perform simple operations on Ethernet network. Routers are used to direct traffic in networks. Routers connect different networks for data packet forwarding. Data packets forwarded from one router to another router. Different routers like Wired Routers, Wireless Routers, Core Routers, Edge Routers, Virtual Routers. A different paradigm is shown by the node in DTN scenario. Each nodes stores a data packet which was sent by another node and forwards the data packet to another relay node. So nodes are special devices or data store and forward points in the Delayed and Disruption Tolerant Network. Node may be personal computer, mobile, printer, tablet, etc. The devices which has IP address in network is treated as Node.

3.2 CONNECTIVITY EVOLUTION

In a wireless network, the connectivity in multi-hop way is often accepted by node density, transmission range, residual energy and node mobility. A partitioned wireless ad hoc network can turn into a connected network when some of the above factors change. The number of nodes being deployed in a designated area can influence the network connectivity greatly. Understanding the transition phase of the network between partition and connectivity can help network management, planning, maintenance and performance monitoring. The importance of the connectivity issue has drawn great attention recently to obtain fundamental properties of the problem in many application domains. For example, the minimum number of average neighbors for network connectivity in static topology [F. Xue and P. Kumar, 2004] the last connection time and the first partition time about node failure models in wireless networks [F. Xing and W. Wang, 2008]; the impact of interference on the connectivity [O. Dousse, F. Baccelli, and P. Thiran, 2005] the relationship between power saving on sensor networks and maintaining connectivity [O. Dousse, P. Mannersalo, and P. Thiran, 2004. In these works, the percolation theory has been used leading to results of critical densities defined based on statistical concept of giant component [H. Kesten Thesis, 1982]. Viewing the need of parsimonious use of networking devices in some applications, for example, a large area with scarce available resources like in some surveillance scenarios, an understanding of the transition phase becomes extremely important.

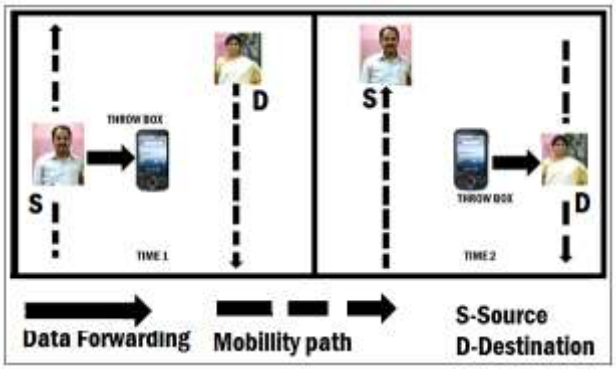
3.3 LATENCY ANALYSIS IN THROW-BOX BASED DTNS

Throw-boxes are low expensive and small devices arranged within wireless devices to improve data delivery performance in Delay Tolerant Networks. Intermittent communication connections between mobile wireless nodes can be observed in many network scenarios, such as wildlife tracking, surveillance, robotic search, emergency rescue, etc. Message dissemination in above networks for non-real time tasks and missions is achieved by using store-carry-and-forward methods based on encountering opportunities, because the instant end-to-end paths may not exist when mobile nodes initialize communications. In this delay, tolerant networks, a variety of methods are proposed to achieve message dissemination which include estimating a better forwarder to carry a message or utilizing several copies of a message to speed up the delivery.

Some recent works have used the idea of deploying stationary devices at specific locations [W. Zhao, Y. Chen, M. Ammar, M. Corner, B. Levine, and E. Zegura, 2006]. The stationary devices called throw-box can be small and cheap devices with wireless antennas and limited memory. They can be deployed quickly for the role of message relay. Issues of enhancing the capacity and optimizing the deployment of these boxes are studied in [W. Zhao, M. Ammar, and E. Zegura, 2004] [W. Zhao, Y. Chen, M. Ammar, M. Corner, B. Levine, and E. Zegura, 2006].

3.4 ROUTING IN THROW-BOX BASED DTNS

Deploying throw-boxes as static nodes can help message dissemination among mobile Nodes in delay tolerant networks. This approach is especially helpful when mobility is localized, i.e. mobile nodes may only move within a region of the network field, and the entire network field lacks a global movement of most nodes. In this network scenario, communicating through pure encountering of mobile nodes may be in effective due to the reduced chances of encountering. Careful deployment of the throw-boxes can enhance the network connectivity and decrease the transmission delay. There are usually two message relay patterns in the throw-box based message dissemination. One relay pattern is that the message is exchanged between the message sender and the receiver when they are at the same location.



The other is that the message will be relayed across multiple throw boxes and the sender and the receiver communicate with different boxes at different locations. For the former, the issue of searching the optimal location for boxes and An ad hoc network is a network that is a combination of different individual devices communicating with each other directly without any interruption. Latency is the delay from input into a device to required outcome. latency issues vary from one device to another device. It greatly affects the performance of the

devices, latency analysis are studied in [W. Zhao, Y. Chen, M. Ammar, M. D. Corner, B. N. Levine, and E. Zegura, 2006] [B. Gu, X. Hong, P. Wang, and B. Richard, 2010].

For the latter, the messages left at a box could be carried by one or more mobile nodes to other boxes to increase the probability for being collected by the receiver. A routing scheme is needed for the latter case. Various routing strategies have been proposed for DTN, such as PROPHET [A. Lindgren, A. Doria, and O. Schelen, 2003], SPRAY [T. Spyropoulos, K. Psounis, and C. S. Raghavendra, 2008], EPIDEMIC [A. Vahdat and D. Becker, 2000], scheduled based routing [S. Jain, K. Fall, and R. Patra, 2004][C. Liu and J. Wu, 2008] [W. Zhao, M. Ammar, and E. Zegura, 2004], and multicast [W. Gao, Q. Li, B. Zhao, and G. Cao, 2009]. Yet, routing through throw-boxes is quite different from these previous works in that it must address additional challenges. The challenges come from the characteristics of the potential links between two boxes. Such a link is formed by various mobile nodes that travel from one node to another at different times and with different moving speeds. The traveling time of mobile nodes between two boxes reflects the link delay. Thus, a routing protocol must address the time-varying nature of the link delay between two boxes.

In addition, the mobile nodes travel between two boxes may have different loading capacity in terms of its buffer sizes. A node with large buffer size can take more messages from one box to another. Different mobile nodes that formalize a link also reveal a time-varying nature of link capacity. Thus a routing scheme must consider jointly the time-dependent link delay and link capacity. In this study, we redefine link" bandwidth" to present this joint consideration of delay and loading capacity over a link. Thus, the link bandwidth in this paper denotes the ratio of loading capacity to link delay. In this routing study, we introduce a novel routing scheme that searches the path with the highest expected link bandwidth from source to destination over time-dependent multiple links.

IV. CONCLUSION

Secured communication in the hostile environment can be successfully achieved through delayed and disrupted tolerant networks. Attackers do not attack the secured data due the robust technology of Disrupted Tolerant Network strategies. But the DTN to be made strong enough due to unpredictable nature.

REFERENCES

[1] J Bettencourt, Admit Sahai, and Brent Waters, "Cipher text-Policy Attribute-Based Encryption", SP'07 IEEE Symposium on. IEEE,2007.

[2] The Internet Research Task Force's Delay-Tolerant Networking Research Group (DTNRG), http://www.dtnrg.org.

[3] Pratiksha Khodade, Vaishnavi Dhongade, Sapana Bhandare, Priyanka Agavane, Prof. Shital Salve- A Proposed System on Disruption-Tolerant MilitaryNetworks for Secure Data Retrieval

[4] Oliveira et .al, "Identity-Based Encryption for Sensor Networks", Pervasive Computing and Communications Workshops, Fifth Annual IEEE International Conference at White Plains, NY 2007. PerCom Workshops '07, p.290-294.

[5] Geng Yang, Chumming Rong, Christian Veigner, Jiangtao Wang and Hongbing Cheng "Identity-Based Key Agreement and Encryption For Wireless Sensor Networks", IJCSNS International Journal of Computer Science and Network Security, VOL.6 No.5B, May 2006, p.182-189.

[6] 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, p. 29–42.

[7] Kate, A. Zaverucha, G.M. Hengartner, U., "Anonymity and security in delay tolerant networks",IEEE, Security and Privacy in Communications Networks and the Workshops, 2007, Third International Conference at Nice, France, SecureComm 2007, p. 504-513.

[8] A. Lewko and B. Waters, "Decentralizing attribute-based encryption", Cryptology ePrint Archive:Rep.2010/351,2010,https://eprint.iacr.org/2010/351.pdf (Date Accessed November 17,2015).

[9] S. S.M. Chow, "Removing escrow from identity-based encryption", 2009, LNCS 5443, p. 256–276.http://link.springer.com/chapter/10.1007%2F978-3-642-00468-1_15 (Date Accessed November 15,2015) .

[10] F. Xue and P. Kumar. The number of neighbors needed for connectivity of wireless networks. Kluwer Wireless Networks, 10(2):169 – 181, 2004.

[11] F. Xing and W. Wang. On the critical phase transition time of wireless multi-hop networks with random failures. In Proceedings of the 14th ACM international conference on Mobile computing and networking, San Francisco, California, USA, 2008.

[12] O. Dousse, F. Baccelli, and P. Thiran. Impact of interferences on connectivity in ad hoc networks. IEEE/ACM Transactions on Networking (TON), 13(2):425 – 436, 2005.

[13] O. Dousse, P. Mannersalo, and P. Thiran. Latency of wireless sensor networks with uncoordinated power saving mechanisms. In Proceedings of the 5th ACM international symposium on Mobile ad hoc networking and computing, Roppongi Hills, Tokyo, Japan, 2004.

[14] H. Kesten. Percolation theory for mathematics. Birkhauser, 1982.

[15] W. Zhao, Y. Chen, M. Ammar, M. D. Corner, B. N. Levine, and E. Zegura. Capacity Enhancement using Throwboxes in DTNs. In IEEE MASS, 2006.

[16] A. Lindgren, X. Hong, P. Wang, and B. Richard. Latency Analysis for Thrown Box Based Message Dissemination. In GLOBECOM 2010: 2010 IEEE Global Telecommunications Conference, MIAMI, Florida, USA, 2010.

[17] A. Lindgren, A. Doria, and O. Schelen. Probabilistic routing in intermittently connected

networks. SIGMOBILE Mobile Computing and Communications Review, 7(3), 2003

[18] A. Vahdat and D. Becker. Epidemic routing for partially connected ad hoc networks. 2000.

[19] S. Jain, K. Fall, and R. Patra. Routing in a Delay Tolerant Network. In Proc. ACM Sigcomm, pages 145–158, 2004.

[20] W. Gao, Q. Li, B. Zhao, and G. Cao. Multicasting in delay tolerant networks: a social network perspective. In Proceedings of the tenth ACM international symposium on Mobile ad hoc networking and computing, 2009.

[21] Y.Sobhanbabu, Dr. DBK Kamesh - Scenario of Cipher text Policy Attribute Based Encryption for Secure Data Sharing- IJASTEMS-ISSN: 2454-356X) Volume.3,Issue.8,August.2017