DELAY/DISRUPTION TOLERANT NETWORK – SURVEY

R. Esther Raja Pushpa
Assistant Professor,
Department of Computer Science and Engineering,
Dr. Sivanthi Aditanar College of Engineering, Tiruchendur.

ABSTRACT

This paper provides an introduction to Delay/Disruption Tolerant Networks (DTN) and would touch upon some basic features. Continuous connectivity is difficult in today's wireless world. The data preservation and security in challenged and intermittent network, is of paramount importance. In this paper, we will see how DTN provides an effective alternative. This will also try to explain basic architecture of DTN and routing techniques that can be incorporated for effective data forwarding. Security of data becomes important in disrupted networks; this paper would also discuss security concerns with DTNs. This paper also discusses possible applications and areas where DTN can be effectively used.

Keywords: Bundle Protocol, Contact Patterns, DTN, Flooding, Forwarding, Routing

I. INTRODUCTION

Internet has been successfully connecting communicating devices worldwide today. TCP/IP protocol suite plays most important role in achieving this effectively. Every device on the countless sub- networks that comprise the Internet makes use of this protocol for data transfers from source to destination with the minimal possible delay and high reliability. End to end data transfer is the basic principle on which TCP/IP is based on. However assumptions of internet cannot hold in many regions. If there instances where end-to-end connectivity is broken or intermittent, then TCP/IP may not work correctly and reliably, in many cases it can completely fail to transfer data from source to destination.

Basically internet (TCP/IP protocol) works based on certain assumptions:

- End-to-end path between source and destination exists forthe duration of a communication session
- Retransmissions based on timely and stable feedback from data receivers is an effective means for repairing errors
- End-to-end loss is relatively small
- All routers and end stations support the TCP/IP protocols
- Applications need not worry about communication performance
- Endpoint-based security mechanisms are sufficient for meeting most security concerns
- Packet switching is the most appropriate abstraction for interoperability and performance
- selecting a single route between sender and receiver is sufficient for achieving acceptable communication performance

Such networks suffer from frequent temporary partitions which can be termed as Intermittently Connected Networks (ICNs). This problem occurs mainly in remote areas, or villages that lack basic infrastructure to support internet.

Due to suchcircumstances, a newer network has evolved which is independent of end-to-end connectivitybetween nodes. This network is called as Delay Tolerant Networks (DTN).Delay Tolerant Networking (DTN) is an approach to computer network architecturethat aims to address the technical issues in heterogeneous networks that experience lack ofcontinuous network connectivity. Delay Tolerant Networks (DTNs) enable data transferwhen mobile nodes are only intermittently connected. Since the connectivity is not expected to be consistent in DTN, it employs what is called a store-carry-and- forward routing

mechanism. In this, the intermediate mobile nodes carry data packets when they receive it and forward it to the next node as and when contact is established. As DTN depends on mobile nodes to carry data, the performance of routing the data solely depends on whether the nodes come in contact with each other or not.

What is DTN

Delay tolerant networks (DTNs) represent a class of wireless systems that virtually need minimum to none infrastructure and would support the functionality of networks experiencing frequent and long lasting partitions. DTNs are intended to deal with scenarios involving heterogeneity of standards, intermittent connectivity between adjacent nodes, lack of *contemporaneous* end-to-end links and exceptionally high delays and error-rates. Also the mobile nodes available in challenged environments can be extremely limited in their resources; such as CPU processing power, memory and network capacity. As DTNs are expected to tackle such dared environments, they are usually intended to achieve interoperability and eventual connectivity to a range of complex applications that include:

- Wireless sensor networks (WSNs) deployed in wildlife tracking or in extreme regions (e.g. volcanic and underwater areas).
- Mobile Ad-Hoc networks connecting remote and rural communities via GPSs, cellular devices and portable storages.
- Exotic Media Networks (EMNs) interconnecting extra-terrestrial nodes such as satellites and deep space probes in Inter-Planetary Networks (IPNs).

Each of the potential field of applications mentioned above is intended to operate under stressful circumstances and in environments that are considered to be challenging for ordinary wireless nodes within a traditional network settings.

DTN architecture represents an attempt to extend the reach of networks. It promises to enable communication between instances of such challenged networks and to act as an integral platform between instances that originally adopt heterogeneous or inconsistent standards, even if they exist in territories lacking a proper communication infrastructure. The main purpose of the DTN approach is to provide a means for message delivery in such challenged settings.

II. ARCHITECTURE OF DELAY TOLERANT NETWORK

The architecture of DTN is designed in such a way that it counters most of the assumptions and conditions that traditional TCP/IP based networks are based on. DTN architecture is based on following design principles:

- Use variable-length (possibly long) messages (not streams or limited-sized packets) as the communication abstraction to help enhance the ability of the network to make good scheduling/path selection decisions when possible.
- Use a naming syntax that supports a wide range of naming and addressing conventions to enhance interoperability.
- Use storage within the network to support store- and-forward operation over multiple paths, and over potentially long timescales (i.e., to support operation in environments where many and/or no end-to-end paths may ever exist); do not require end-to-end reliability.
- Provide security mechanisms that protect the infrastructure from unauthorized use by discarding traffic as quickly as possible.
- Provide coarse-grained classes of service, delivery options, and a way to express the useful lifetime of data to allow the network tobetter deliver data in serving the needs of applications.

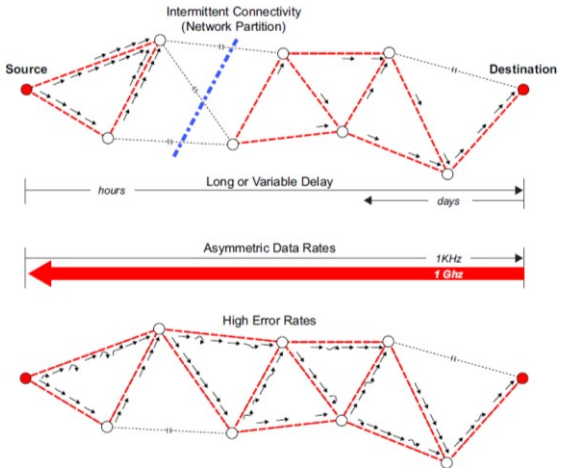

Fig 1: DTN Architecture Principles

a. Concept of Bundle Protocol

A Delay Tolerant Network can be considered as an overlay on the existing

regional networks. This overlay is called as the bundle layer. This layer is intended to function above the existing protocol layers and provide the function of a gateway when two nodes come in contact with each other. The main advantage of this kind of protocol is flexibility. It can be easily linked with the already existing TCP/IP protocol networks or can be used to link two or more networks together. The position of the bundle layer can be seen in the following fig. 2.

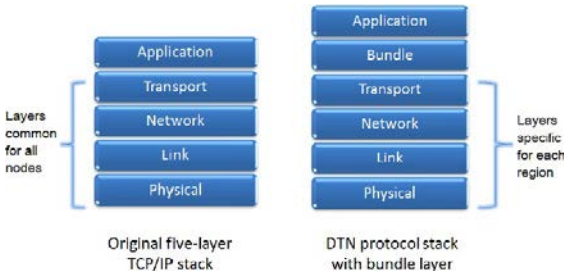

Fig 2: Bundle Layer

Bundles are also called as messages. The transfer of data from one node to another can be made reliable by storing and forwarding entire bundles between nodes. The bundles comprise of three things, source node's user-data, control information (e.g., source node ID, destination node ID, TTL etc.), a bundle header. Besides Bundle transfer, custody transfer is also done. The custodian node for a bundle keeps the message until it is successfully transferred to the next node and it takes the custody for that message or until the TTL of the message expires.

b. Store and Forward Technique

Delay Tolerant Networks have overcome the problems associated with the conventional protocols in terms of lack of connectivity, irregular delays, asymmetric bidirectional data rates etc. using the concept of store and forward. The method of store and forward is very analogous to the real life postal service. Every letter has to pass through a set of post offices, here it is processed and forwarded, before reaching the destination. Here the complete message or a chunk of it is transferred and stored in nodes successively until it reaches the destination. The following figure (fig. 3), gives a rough graphical representation of how a message is propagated through a network.

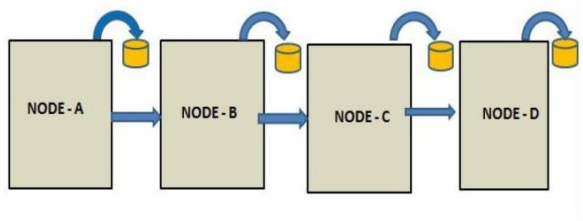

Fig 3: Store and Forward Approach

c. Types of Contacts

Store and forward mechanism solely depends on whether or how the nodes make contact with each other. Contacts typically fall into one of several categories, based largely on the predictability of their performance characteristics and whether some action is required to bring them into existence. Following are major types of contacts that can be defined:

a. Persistent Contacts

Persistent contacts are always available (i.e., no connection-initiation action is required to instantiate a persistent contact). An 'always-on' Internet connection such as a DSL or Cable Modem connection would be a representative of this class.

b. On-Demand Contacts

On-Demand contacts require some action in order to instantiate, but then function as persistent contacts until terminated. A dial-up connection is an example of an On-Demand contact (at least, from the viewpoint of the dialer; it may be viewed as an Opportunistic Contact, below, from the viewpoint of the dial-up service provider).

c. Intermittent - Scheduled Contacts

A scheduled contact is an agreement to establish a contact at a particular time, for a particular duration. An example of a scheduled contact is a link with a low-earth orbiting satellite. A node's list of contacts with the satellite can be constructed from the satellite's schedule of view times, capacities, and latencies. Note that for networks with substantial delays, the notion of the "particular time" is delay-dependent. For example, a single scheduled contact between Earth and Mars would not be at the same instant in each location, but would instead be offset by the (non-negligible) propagation delay.

d. Intermittent – Opportunistic Contacts
Opportunistic contacts are not scheduled, but rather present themselves unexpectedly.

For example, an unscheduled aircraft flying overhead and beaconing, advertising its availability for communication, would present an opportunistic contact. Another type of opportunistic contact might be via an infrared or Bluetooth communication link between a personal digital assistant (PDA) and a kiosk in an airport concourse. The opportunistic contact begins as the PDA is brought near the kiosk, lasting an undetermined amount of time (i.e., until the link is lost or terminated).

e. Intermittent - Predicted Contacts
Predicted contacts are based on no fixed schedule, but rather are predictions of likely contact times and durations based on a history of previously observed contacts or some other information. Given a great enough confidence in a predicted contact, routes maybe chosen based on this information.

III. ROUTING TECHNIQUES

Connectivity of nodes in DTN is always going to be intermittent, no two nodes can be always connected. So end-to-end connectivity never exists. DTN uses store-carry-forward mechanism to transfer the data packets across source and destination nodes. To make this possible the intermediate nodes take custody of data packets or bundles and forward it when the opportunity arises.

So for effective data transfer and performance of a DTN, a route must be optimally and strategically formed between the nodes. There are several strategies that are employed for routing, a brief overview of these strategies is presented here. The routing strategies are categorized as Flooding Strategies and Forwarding Strategies.

a. Flooding Strategies

In a flooding strategy, a message is duplicated into several messages and the copies are delivered to a set of nodes called relay nodes. Relay nodes stores the messages until they come in contact with destination node. As soon as the contact is made during "contact" phase, the messages are delivered by the relay nodes. Many of the strategies are workout by the researchers before this DTN get popular. These strategies are studied in the context of, mobile adhoc network where random mobility is good chance of bringing the source in contact with destination. Message replication is then used to increase the probability that the message is successfully delivered to the intended node. These protocols do not require any prior global or local knowledge about network.

b. Forwarding Strategies

In forwarding strategy knowledge about the network is used to calculate a best path of nodes between source and destination. A message is then forwarded from node to node along this path. So there is not duplication of data in these strategies. However the protocols designed for such strategies need to have the knowledge about network topology so as to find optimal path without replicating the data packets.

IV. SECURITY

Delay-tolerant networks can face some serious resource crunches in some situations, this demands some form of authentication and access control to the network in such situations. IT should not be possible for an un-authorized user to flood the network with traffic. Access should be controlled strictly for such users. In most of the cases it is also not acceptable for unauthorized traffic to be forwarded over certain network links at all. This is critical especially for exotic, mission-critical links.

Considering these potential security issues, several goals have been established for designing the security of a typical DTN architecture:

Immediately prevent unauthorized applications from having their data carried through or stored in the DTN.

Strictly avoid unauthorized applications from declaring control over the DTN infrastructure.

Do not allow to send bundles at non-permissible rate or class of service, even though the application is authorized for transfers.

Bundles may be damaged or tampered with in transit, such should be identified and discarded.

There should be a mechanism to detect compromised entities, and when they are found their authorization should be revoked immediately.

Most of the existing authentication and access control mechanisms or protocols are designed for operation in non-delayed and always connected networks, and may not necessarily function efficiently when applied to DTNs. Especially dynamic updates to ACLs (Access Control Lists) and blacklisting or revoking credentials for a particular compromised node can be difficult. Also, methods that require frequent access to centralized servers to complete an authentication or authorization transaction are not very suited for DTNs. As a consequence of these problems, there is a delay in the commencement of communication detecting and recovering from system compromise. Completing transactions due to inappropriate access control or authentication settings.

Due to these challenges, to meet the security requirements, DTN architecture implements a standard but optionally deployed security architecture that uses hop-by-hop and end-to-end authentication and integrity mechanisms. The purpose of using both approaches is to be able to handle access control for data forwarding and storage separately from application-layer data integrity. For a principal such as a user (of which there may be many), the end-to- end mechanism provides effective authentication. Whereas the hop-by-hop mechanism is intended to authenticate DTN nodes as genuine transceivers of bundles for each-other. It is plausible to construct a DTN in which not all of the nodes participate in the security mechanisms, but rather a subset of nodes take part, which results in a secure DTN overlay existing on top of an apparently insecure DTN overlay.

DTN nodes are expected to discard traffic as soon as practically possible if the authentication or access control fails, this will help satisfy above goals of secure network. This approach has the associated benefit of making denial-of-service attacks considerably harder to stand as compared with conventional Internet routers. However, the obvious cost for this capability is potentially larger computation and credential storage overhead required at DTN nodes.

V. APPLICATIONS OF DTN

The store-carry-forward architecture of DTN was originally an idea that was designed to fulfil the requirements of the Interplanetary Internet (IPN). DTN is just a simplified form of this network architecture. So, the primary objectives of DTN were to survive complex and challenging network environments and failures in hardware as well as software e.g. protocol failures. Even if the DTN was originally designed to be more of tactical purpose. It may and will have far greater applications in real day-to-day world. Some of such applications are listed here:

Space Agencies: International Space Station communication (currently operational for research), interplanetary communication, future space-debris monitoring.

Military and Intelligence: Mobile ad-hoc networks (MANETs) for wireless communication and monitoring, cargo tracking, search and rescue communication, unmanned aerial vehicle (UAV) communication and control.

Commercial: Cargo and vehicle tracking (by road, rail, sea, and air), in-store and in-warehouse asset tracking, data transactions (e.g., financial, reservations), agricultural crop monitoring, processing-plant monitoring, communication in underground mines.

Public Service and Safety: Security and disaster communication, search and rescue communication, humanitarian relief monitoring, smart-city event-response, smart transportation networks, smart electric-power networks, global airport-traffic control, infrastructure-integrity monitoring, unmanned aerial vehicle (UAV) communication and control, remote learning.

Personal Use: Personal monitoring and communication in wilderness and urban areas, fire- and-forget text messaging.

Environmental Monitoring: Animal migration, soil properties and stability, atmospheric and oceanographic conditions, seismological events.

Engineering and Scientific Research: Network subject-matter experts, academic research by faculty and students.

VI. CONCLUSION

Delay Tolerant Networks will form one of the most important facets of modern day networking, given the necessity of connectivity. The traditional TCP/IP protocol suite is not suited to these modern day mobile networks as it relies on end-to-end connectivity being always present and a very low error rate.

Bundle protocol in DTN offers a viable solution for challenged or intermittent networks and can be easily plugged into existing TCP/IP network. This uses store-carry-forward mechanism to transfer the data between intermittently connected nodes.

DTN can have most common application in modern social networks where social contacts are connected intermittently, however it has capabilities that can extend it to be applicable to much challenged network conditions such as used by space agencies or military and intelligence agencies.

However the biggest challenge for DTN remains to be effective security implementation. As the data transfers are intermittent and data may end up to be with relay node for longer durations, the security of data must be carefully designed and should be very strict.

REFERENCES

[1] V. Cerf, S. Burleigh, A. Hooke, L. Torgerson *"Delay-Tolerant Networking Architecture" Networ kWorking Group Google/ Jet Propulsion Laboratory, April 2007*

[2] Fall, K.. "Adelay-tolerant network architecture for challenged internets", *SIGCOMM'03: Proceedings of the2003 conference on Applications, technologies, architectures, and protocols for computer communications,ACM, New York, NY, USA, pp. 27–34. 2003*

[3] Forrest Warthman "*Delay- and Disruption- Tolerant Networks (DTNs)*" Version 2.0, Warthman Associates, based on technology developed by the Interplanetary Internet Special Interest Jully2012

[4] JianShen, Sangman Moh and Ilyong Chung "Routing protocol in Delay tolerant Networks:Comparative Survey"*The 23rd International Conference on Circuits/System computer and communications (ITC-CSCC 2008)*

[5] Shyam Kapadia, Bhaskar Krishnamachari, and Lin Zhang"Data Delivery in Delay Tolerant Networks:A Survey"*Cisco Systems Inc., San Jose, CA* 2006

[6] Artemios G. Voyiatzis, Member, IEEE "A Survey of Delay- and Disruption-Tolerant Networking Applications*" Journal of Internet Engineering, Vol. 5, No. 1, June2012*