Volume 5, Issue 6, June 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Issues in Delay Tolerant Networks: A Comparative Study

Inadyuti Dutt*
Dept. of Computer Applications,
B. P. Poddar Institute of Management & Technology,
West Bengal University of Technology, West Bengal, India

Abstract: ***Delay-tolerant networks exhibit the ability to connect in diverse environments where end-to-end connectivity is intermittent and network resources are not abundant. Due to scarce connectivity and lack of resources they often have to address several issues more strenuously than a traditional network, which follows the TCP/IP protocol. This paper emphatically takes care of these issues related to routing, congestion and security in delay-tolerant networks. This paper compares various routing strategies and evaluates them with respect to transmission delay, latency, delivery ratio and resource consumptions. Further, it surveys the various congestion control protocols with respect to buffer management. The security issue in delay-tolerant network is another important area which has been addressed in this paper. Security in delay-tolerant network differs from the traditional security model in the way it includes network routers as participants of an authentication process. In networks where link capacity is a very costly resource, good security approaches become necessity to be implemented. This paper also attempts to unfold the security issues related to key management, handling replays, routing protocols and multicast scenarios.***

Keywords: Delay-Tolerant Network (DTN), Routing protocols, Security, TCP/IP, Latency

I. INTRODUCTION

Delay-tolerant networks are intended to function in different and dissimilar environments that are characterised by three prime features respectively: i) there is no persistent end-to-end connectivity among the nodes, ii) there are long delays in paths and iii) frequent packet drops. DTNs apply in many application instances, especially in developing regions lacking network infrastructure [1]. Because there is no guarantee of end-to-end connectivity in delay-tolerant networks, the routing protocols which have good performance in the conventional networks are not suitable for delay-tolerant networks. DTNs are characterized by latency, bandwidth limitations, error probability, node longevity, or path stability [2].

The concept of delay-tolerant networks emerged when the traditional TCP/IP protocol failed to work in environments that use acoustic or optical modulation with frequent interruptions, terrestrial mobile networks with no constant end-to-end connectivity and sensor nodes with limited end-node power and CPU capability. Such networks violate the functioning of TCP/IP suite and are often termed as Challenged Networks. In these networks no end-to-end path between source and destination nodes prominently exists. Hence, in those types of scenario TCP/IP network starts to work inappropriately or even stops to work at all. A good example of such environment is the communication in Interplanetary Internet where speed-of-light delay to outer planets from Earth becomes significantly higher. A normal file transfer initiated from Earth to Mars might take about an hour. The main limitations that are prevalent in the aforesaid challenged networks are namely: frequent disconnections, non-existent routing paths, low data rate, high latency, bandwidth limitation, lack of power and energy. These shortcomings gave way to ascertain some network characteristics like contact, contact schedules, waiting time, queuing time, propagation and transmission delay respectively.

Delay-tolerant networks became apparent at this critical juncture and thus have been designed to operate in environments where Internet Protocol Suite does not fit in the demanded situation. DTN works as an overlay on top of an already existing TCP/IP stack which supports intermittent connectivity and overcomes communication disruptions as well as delays. Data transmission between the source and destination is also allowed where persistent route might not exist. Since the delay-tolerant networks exhibit limited resource connectivity, some better connected nodes in the network become congested and unusable causing even more disconnection and lower delivery rates. This may cause congestion in network. Again congestion in these networks becomes a critical issue as the TCP/IP congestion protocols do not suite their purposes. Researches based on congestion in delay-tolerant networks primarily focus on buffer management where the goal is to remove unnecessary messages from the buffer. Few others recommend some judicious approaches using probabilistic methods in order to take care of congestion in the routes.

Just as the routes become congested due to the presence of unnecessary packets in the network, there may be fair chances of packets flooding from unauthorised users. Delay-tolerant networks become vulnerable to security issues when unauthorised applications are carried forward without proper information. There may be circumstances where these applications assert the control over the delay-tolerant architecture. Such situations may arise in battlefields where the access control of the army has been taken over unknowingly by the opponent army. Another issue which may take place is the damage of packets in transit. Such damaged packets are susceptible to security issues and thus need to be discarded. The research area is open and still remains unexplored with regards to security in delay-tolerant networks.

Thus the primary issue that needs to be addressed in delay-tolerant networks is routing as the route between source and destination is merely non-existent at times. All of the current DTN routing methods share a similar paradigm, the "store and forward" fashion. If there is no connection available at a particular time, a DTN node can store and carry the data until it encounters other nodes [4]. In this area, named as delay tolerant networks(DTNs), 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 [5]. Once the routing issue is satisfied, the main challenge becomes to send data in a route which is congestion-free. When a route is determined between a sender and a receiver, it again becomes necessary to ensure that the route is congestion-free. As it is evident that searching for a route becomes a significant job in delay-tolerant networks therefore once a route has been established it is also very necessary to determine its traffic. Since very few routes can be established in such cases hence such routes may become over-flooded at a time of sending the packets.

Security issues in DTN differ from traditional security model in the way it includes network routers as participants of an authentication process. In DTNs where link capacity is a very costly resource, good security approaches become inevitable to be implemented.

This paper reviews the existing literature that addresses these issues in delay-tolerant networks by comparing them on their own merits. Section II of the paper deals with routing strategies and issues addressing them. This section describes two well-known routing principles and further explains the strategies adopted by them. Moreover, the performances of each routing protocols under these strategies are evaluated. Section III addresses the congestion issues related to delay-tolerant network. The majority of work in congestion control is based on buffer management. Some recent developments are also concerned with replication management and distribution. Section IV takes care of the various security issues with respect to key management, handling replays, routing protocol and multicast security. Section V concludes the survey of the several issues of the delay-tolerant network, which needed to be concentrated on.

II. ROUTING STRATEGIES in DTN

Routing in delay-tolerant networks can be categorized using two principles. The first one being the replication principle where multiple copies of a message are send to each node until the destination receives one of them. The second one chooses network knowledge in order to make routing decisions.

A. Principle of Message Replication

Delay-tolerant networks communicate with components that are totally unreliable or unpredictable at times. The representatives of replication principle allow making multiple copies of the same message in order to increase the probability that one of them will definitely find its way to the destination. In this scenario, the message will not be reaching the destination only if all the other nodes carrying the copy of the message are unable to deliver. This principle of replication consumes bandwidth and buffer resources proportional to the number of nodes in the network. However, the approach produces high delivery ratios and if provided with infinite bandwidth and buffer resources, it would deliver all the messages that could be delivered in the least amount of time. The principle of replication comes up with several issues that need to be addressed. The most important being the number of copies to be made for a single message. As the number of copies of a single message increases, more and more copies propagate in the network unnecessarily. This can further become bottleneck for buffer management and bandwidth consumption. The issue becomes more unmanageable when large number of nodes takes the responsibility to replicate a single message and there is no significant control on message replication. Another issue that needs to be addressed is the number of message copies to be transferred to a node upon each contact opportunity.

B. Principle of Network Knowledge

This principle believes in acquiring network information before sending a message along a path. A path is carefully selected after gathering network information of the neighbouring nodes. Each node in the network cannot constitute itself the network information as it requires the complete contact schedule of the pair of communicating nodes. The major challenges that are faced in this technique are probably the chance of predicting the next contact time and schedule as well as to determine the rank of each neighbours. This gives rise to two questions namely: i) can the next contact time or chance of contact with destination in near future be predicted? and ii) how to determine that and rank the neighbours accordingly? This leads to simple implementation where the complete information of the neighbours if constructed accurately can make very efficient usage of network resources. The disadvantage is that the strategy cannot adapt to different networks or conditions so it may not make optimal decisions.

C. Routing Strategies

Based on principles' of replication and knowledge, the delay-tolerant routing strategies can be divided into two types namely, flooding strategies and forwarding strategies. The families of flooding strategies rely primarily on principle of replication, and forwarding strategies, rely on the knowledge of the network. The following sections would try to elucidate the various types in each family and then conclude them by comparing their individual performances.

i. Flooding Strategies

This strategy firmly believes in sending as many copies of a message to all neighbouring nodes until the message is successfully received by the destination. The earliest and simplest form of flooding strategy was the *Direct Contact*. This

technique neither replicate the message to be sent and nor does need the knowledge of the network in order to select a path. Instead, it forwards the message to the first node it comes in contact with. It is thus most likely to face problems like large delay (in transmission) and low delivery ratios. However, due to its simplicity it does not consume many resources as it uses exactly one message transmission. It works only if the source contacts the destination. The worst case scenario may occur when the node carrying the data never gets to the range of the final destination and the message never gets transmitted [3]. The next member of this flooding family, copies the message to the first n nodes that it contacts. These nodes are called the relay nodes, which along with the source node hold back the message until it finds the destination node. This approach is known to be the *Two-Hop Relay*. This approach is said to be a better one in comparison to the *Direct Contact* approach as it uses limited resources, reduces the delay and enhances the delivery ratios. *Tree-Based Flooding* technique extends the philosophy of Two-hop relay technique. Once the message is copied to a relay, the relay node sends the copy of the message to n nodes. This becomes very decisive because the scheme needs to determine the number of replicas it has to make for a message. There are number of ways to decide how to make the copies. A simple scheme is to allow each node to make unlimited copies but to restrict the message to travel a maximum of n hops from the source [6]. This limits the depth of the tree, but places no limit on its breadth [7]. An enhanced scheme offers to limit the node to make at most m copies. This limits both the depth and the breadth of the tree, which limits the total number of copies to a maximum of m^n [8]. Tree-based flooding is said to be more efficient than the earlier ones as it can deliver messages to destinations that are multiple hops away. The major challenge in implementing this scheme would be to determine the parameters like the number of multiple copies to be made and the number of hops these copies have to be sent. The most popular flooding strategy is *Epidemic Routing* where no network knowledge is used and maximum replication of the message is accomplished. On contact, two nodes first exchange summary vectors – list of messages they each have. Then copies of messages they don't have are exchanged. Eventually all nodes may have replicas of all messages. This scheme represents the extreme end of the flooding family as it tries to send each message to all possible paths in the network. It offers high delivery ratio, low delay (if no resource constraints are there) but at the same time consumes bandwidth and buffer.

Table I. Performance Comparison of different Flooding Strategies in DTN

Routing Name	**Replication**	**Network Knowledge**	**Transmission Delay**	**Latency**	**Delivery Ratio**	**Bandwidth**	**Buffer usage**
Direct Contact	Not needed	Uses any available contact	Large	High	Minimum	Low	Low
Two-Hop Relay	N relay nodes, partial replication	Contacts neighbouring nodes	Better than Direct Contact	High	Better than Direct Contact	Better utilized than Direct Contact	Better utilized than Direct Contact
Tree-Based Flooding	N relay nodes partial replication	Contacts neighbouring nodes	Better than Two-Hop Relay	High	Better than Two-Hop Relay	Better than Two-Hop Relay	Better utilized than Two-Hop Relay
Epidemic Routing	Full replication	No network knowledge needed	Least	Very Low	High	Maximum Consumption	Maximum Usage

ii. Performance Evaluation of Flooding of Strategies

In this section the performance of the four routing strategies in delay tolerant network namely: Direct Contact, Two-Hop Relay, Tree-Based Flooding and Epidemic Routing have been evaluated with respect to parameters like replication, network knowledge, transmission delay, latency, delivery ratio, bandwidth and buffer usage. Table I, presents a comparative study by which the flooding protocols can be evaluated. It concludes the overall performance and suggests that the more a flooding protocol relies on replication, the more it consumes the network resources like bandwidth, buffer and so on. The delivery ratio also increases with reduction in latency and transmission delay. Thus it can be inferred that replication is one of the better approaches that can be relied upon but not the fairest one.

iii. Forwarding Strategies

Forwarding strategies are attributed to careful selection of paths by attaining more and more information from the network topology. They assign some metrics to the links and try to evaluate their merits according to them. These metrics can assume some weights to each link between a pair of nodes or information of their coordinates in order to circumspectly select a path from a set of given paths. By classification, the strategies in this family demand some network knowledge prior to the selection of a path. It attempts to take care of the network resources like bandwidth and buffer by judiciously selecting the paths.

The first and foremost member of this strategy is called the *Location-Based Routing*. It requires the information with reference to the coordinates of each node. A distance function is used to estimate the cost of delivering messages from

one node to another [8]. Usually a message is forwarded to the next node if and only if its coordinates are closer to the coordinates of the current node. The major advantage of using this strategy is that it demands very little information of the network and its topology as because it needs to know its own coordinates, the coordinates of the destination and the coordinates of the potential next hops respectively. However, such routing strategy yields some problems regarding the distance between two communicating nodes. The two communicating nodes that are the potential next hops in the routing protocol might know each others' coordinates but at the same time might not obtain information about the physical obstruction present between them. The presence of such obstacle might hinder the communication between them. Another issue which arises is the constant mobility of the nodes due to which the coordinates' information keeps altering. This increases the complexity of traversing as the source needs the coordinates of the destination node.

Another approach called *Gradient Routing* in forwarding strategies' family is to assign weight to each node depending upon some parameters like time of last contact between the node and the destination, remaining battery, energy, contact schedule or mobility. To accomplish this strategy each node must store such information for each one of its destination node. Also sufficient information must be propagated through the network to allow each node to compute it's metric for all destinations [7]. Gradient Routing has shown to decrease the delay time. Although this approach is efficient for routing in delay-tolerant networks but it also increases the overhead of constantly building the metrics by gathering native information from the neighbouring nodes. This strategy also takes time initially to find a good custodian node as it may take some time for the metrics to get initialized.

Link Metrics strives on the most popular traditional networking routing protocols. They attempt to build a topology graph for the network, assign weights to each link and finally run a shortest path algorithm. This approach needs the maximum information of the network to implement the routing algorithm. The weights assigned to the links are based on some metrics: the highest bandwidth, lowest latency, highest contact schedule or highest delivery ratio. There are some other metrics which consider in minimizing buffer or power consumptions.

Jain [9] *et al.* proposed different metrics to implement the concept of forwarding strategies using certain network knowledge. Their first metric was referred to as *Minimum Expected Delay*(MED) was based on the assumption of queuing time to be zero and that the average sum of transmission time, propagation delay and waiting time is specifically known. The sum depicts the average amount of time it takes for a message to move from one node to another. MED needs little knowledge of the network as it determines the average value of the waiting time.

They proposed another metric called *Earliest Delivery*(ED) which was a variation of the first one as it assumed the queuing time to be zero and the propagation and transmission delays were assumed to be known accurately. This metric demands the information of the complete contact schedule. Thus ED can be considered as a more enhanced approach in comparison with MED but at the same time needs the complete contact history of the nodes in contact.

Jain *et al.* proposed another variant of ED called *Earliest Delivery with Local Queuing* (EDLQ) by considering buffer occupancy at each node so as to estimate the queuing delay to the ED metric. This metric not only demands the history of the contact schedule but also keeps information of the buffer space. Thus it is considered to be a revised version of ED with more knowledge of the network needed.

The *Earliest Delivery with All Queues* (EDAQ) protocol by Jain *et. al.* uses the Contacts and the Queuing oracles. In EDAQ, routes are not recomputed for messages in transit since the initial route predicts accurately all delays. EDAQ works only if capacity is reserved for each message along all contact edges. In practice, EDAQ is very difficult to implement in most DTNs with low connectivity, as it requires global and accurate distribution of queuing state. Limited connectivity also severely limits practical implementations of edge capacity reservations.

The aforesaid proposed metric by Jain *et al.* attempts to solve the issue of routing by seeking the accurate information about the complete contact schedule known in advance. This becomes impractical at times in DTN as the connectivity in the network is totally unpredictable and unreliable. Jones et al. [10] improvised the aforesaid work further and the metric presented by them is called *Minimum Estimated Expected Delay* (MEED), where the weights of each node are based on record connection and disconnection time of each contact with another node over a sliding history window to get average waiting time till next contact with that node.

Linear Programming (LP) is an enhanced protocol that attempts to consider the contact schedule history, queuing delays and traffic demands of each node in order to determine a better solution. It works by taking into considerations the contact schedule at disjoint time intervals, their queuing delays and traffic demands of each node so as to minimize the average queuing delays under constraints of buffer and other network capacities.

iv. Performance Evaluation of Forwarding Strategies

Performance trade-offs of the forwarding strategies with respect to the parameters like network knowledge, transmission delay, latency, delivery ratio, bandwidth and buffer usage are evaluated. Fig.1 represents the percentage utilization of buffer by various protocols like ED, MED, MEED, Epidemic and its effects on the delay in message transmission. It is perceived that the lower availability of buffer affects the overall efficiencies of the protocols. We have considered Epidemic routing protocol with these comparisons in order to get a clear picture of the efficiency of forwarding strategies with respect to replication strategies. It is observed that Epidemic routing protocol does not perform well when the buffer availability is low. Protocols like MED, MEED and ED rely more on buffer availability and their transmission delay reduces accordingly. Moreover, other protocols adapting the forwarding strategy like Gradient Routing, EDAQ, EDLQ and LP exhibit more or less similar patterns of delay due to buffer unavailability and therefore are not exhibited in this figure.

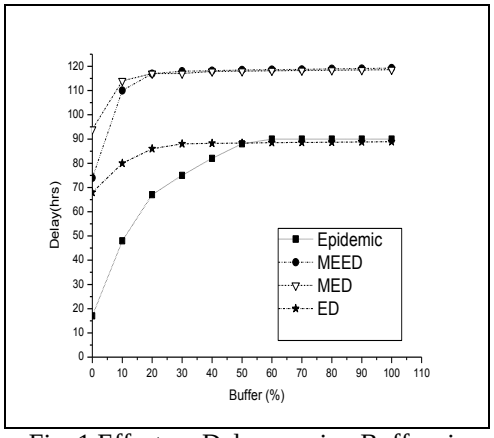

Fig. 1 Effect on Delay varying Buffer size

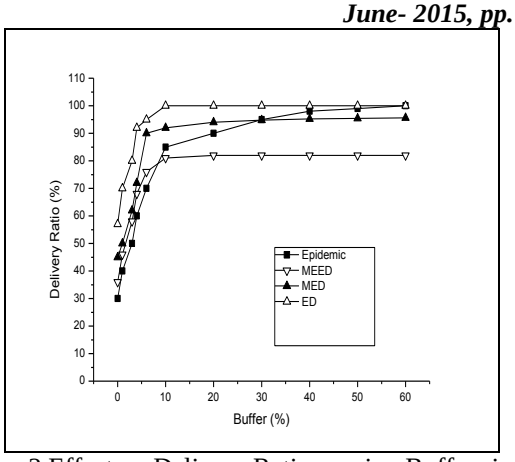

Fig. 2 Effect on Delivery Ratio varying Buffer size

Fig. 2 equates the delivery ratio with respect to varying buffer occupancy for ED, MED, MEED and Epidemic routing protocols. This figure shows that the delivery ratio rises with buffer availability. Delivery ratio seems to be the maximum for ED as it considers the complete contact schedule whereas the other protocols rely heavily on getting contact information from each node. The major reliance on such information exhibit dependencies on buffer availability and thereby affects the delivery ratio.

Fig.3 illustrates the affect of bandwidth with regards to the delivery ratio. It suggests the efficiency of the protocols with increase in bandwidth availability. Epidemic routing protocol exhibit maximum delivery ratio with increase in availability of bandwidth because epidemic routing protocol uses flooding technique to deliver the bundles successfully. Thereby its bandwidth usage increases with increased replication. Moreover, the other protocols like ED, MED and MEED also suffer in their delivery ratios on reducing the bandwidth. It is depicted that the overall reliance of the protocols are majorly on buffer and bandwidth availability and therefore their delivery ratio gets affected accordingly.

Fig.4 exhibits that the delay for all the protocols increases as the bandwidth decreases. This is due to the fact that when the bandwidth availability is less then messages take longer time to transfer. From this Fig. 4 it is evident that *Epidemic* routing outcasts all the other protocols. The figure also suggests that the MEED's performance is slightly worse than MED. MED's delay increases unusually at around 2 Mbps before it settles down for a lower delay. At an initial stage of bandwidth 1 Mbps, the protocols perform poorly and show abnormal bump in their behaviour. Overall Epidemic and ED show lower delay than MED and MEED protocols.

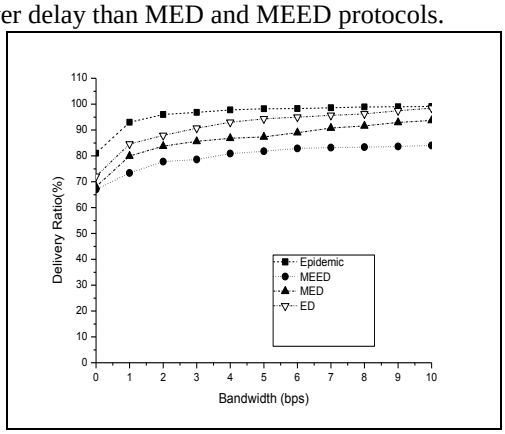

Fig. 3 Effect on Delivery Ratio varying Bandwidth

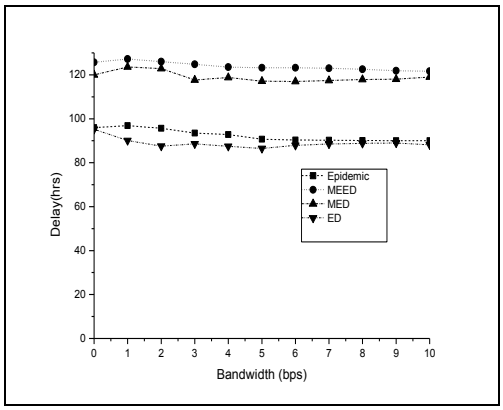

Fig. 4 Effect on Delay varying Bandwidth

III. CONGESTION ISSUES

Detecting and dealing with congestion in delay-tolerant networks is an important and challenging problem. Current DTN forwarding algorithms typically direct traffic towards particular nodes in order to maximise delivery ratios and minimize delays, but as the traffic demands increase these nodes may become unusable at times. Early works in congestion focuses primarily on reducing the delivery latency and cost. They attempt to reduce these by taking into considerations unlimited transfer and storage capacity [11]. The majority of work in congestion control is based on buffer management [12, 13, 14, 15]. Recent developments have been concerned with replication management [15, 16, and 17] and distribution [18, 19].

i. Queuing Strategies

A number of queuing strategies have been proposed in [14] more specifically: First in first out (FIFO), evict Most FOrwarded first (MOFO), evict MOst favourably forwarded first (MOPR), evict SHortest LIfe time first (SHLI) and evict LEast PRobable first (LEPR).

FIFO drops messages based upon the order in which they enter the buffer. Thus the first message that entered the queue is the first to be dropped.

MOFO relies on the philosophy of dissemination of messages by dropping the message that has been forwarded the largest number of time, enabling messages that have a lower hop count to travel further within the network.

MOPR assigns an ageing value for each message in its queue. And each time a message is replicated the age of the message is increased based on the predictability of the message being delivered. The message with the highest ageing value is dropped first.

SHLI assigns the message timeout value, which specifies that when the message is no longer useful, such that the message with the shortest remaining life time is dropped first.

LEPR uses probability of statistics by ranking the messages within its buffer. Based on the predicted probability of delivery; the message with the lowest probability is dropped first.

Resource Allocation Protocol (RAPID) [21] models DTN by forwarding messages based on some utility functions. Routing is achieved by prioritising messages to be forwarded and messages to be dropped based upon a utility function. The utility metric is dependent on the goal of the network, RAPID defines 3 metrics: Minimising Average Delay, Minimising Missed Deadlines and Minimising Maximum Delay. When using the Minimising Average Delay Metric a node attempts to greedily replicate the message that reduces the average delay among all packets in its buffer.

The Minimising Missed Deadlines Metric replicates the message that has the highest probability of being delivered within its specified deadline. The Minimising Maximum Delay Metric replicates the packet with the earliest creation time in order to minimise the maximum delay for each message.

Storage Routing (SR) [15] chooses two algorithms: a node selection algorithm and a message selection algorithm. The node selection algorithm targets alternative custodians needed to deliver the message either by forwarding towards the destination or back through the congested node, by allowing the message to loop. The message selection algorithm chooses either the first message in the buffer, the last message in the buffer or the oldest message in the buffer [11].

FairRoute [19] uses the popularity of a node to evaluate in addition to contact histories. A node's queue length is evaluated, such that a node with a larger number of messages in its queue is nominated more often as a next-hop. FairRoute also argues that in order to determine the popularity of a node the size of the messages in the queue indicate that the node is more capable of forwarding the messages it receives. In Fair Routing, the perceived interaction strength originated from social influence is used to reflect a social relationship between pair-wise nodes, depending on both the short term value and long term value [19].

Retiring Replicas (RR) [21] is an adaptive and dynamic replication algorithm that adjusts a node's initial replication limit based on the current traffic congestion information. RR allots a value to the congestion according to the level of congestion (CV) by calculating an

exponentially weighted moving average of the ratio of dropped and replicated packets during a window of time. A node increases or decreases the value of CV by noticing the congestion in the routes. RR introduces an online adaptive replication technique that treats the network as if it has a globally uniform level of congestion, but this is not typical in such fragmented networks, as different islands of connectivity each have their own traffic demands and as the topology of the network changes burst of traffic spread across the network producing congestion hotspots [11].

ii. Performance Evaluation of Queuing Strategies in DTN

Table II shows the performance evaluation of congestion control using queuing strategies. It suggests that the protocols are mostly based on evicting the messages according to the order in which they enter the buffer. FIFO has large transmission delay as it evicts messages from the buffer first in order to accept messages in its buffer. While its delivery ratio of messages is low and utilizes sizeable buffer. Due to its poor deliver ratio, the bandwidth usage seems to be low too. Protocols like MOFO, MOPR, SHLI and LEPR exhibit better performance with respect to the parameters being considered. RAPID, SR, FR and RR protocols are based on some metrics and capture dynamic behaviour of traffic. Hence, they showcase better delivery ratio, buffer usage, bandwidth utilization and lower transmission delay respectively. The evaluation of the queuing strategies suggests that the performance increases when there is an absolute mechanism of capturing the dynamic behaviour of the traffic. It states that the efficiency of accepting or evicting message in a buffer is majorly dependent upon the changing information gathered from the network.

Table II. Performance Comparison of different Queuing Strategies in DTN

Queuing Strategy Name	Strategy used	Transmission Delay	Delivery Ratio	Buffer usage	Bandwidth
First In First Out(FIFO)	Drops the message that has entered first	Large	Minimum	High	Low
MOst FOrwarded(MOFO)	Drops the message that has been forwarded maximum number of times	Lesser than FIFO	Better than FIFO	Better utilized than FIFO	Better utilized than FIFO
Most favourably forwarded first(MOPR)	Drops the message that has highest ageing value	Lesser than MOFO	Better than MOFO	Better utilized than MOFO	Better utilized than MOFO
SHortest Life time first(SHLI)	Drops the message that has the shortest remaining life	Lesser than MOPR	Better than MOPR	Better utilized than MOPR	Better utilized than MOPR

LEast Probable first(LEPR)	Drops the message that has lowest probability of delivery	Lesser than SHLI	Better than SHLI	Better utilized than SHLI	Better utilized than SHLI
Resource Allocation Protocol(RAPID)	Drops or forwards message based on some utility function	Metrics dependent	Better than LEPR	Depends upon the metrics used	Depends upon the metrics used
Storage Routing(SR)	Uses two algorithms namely i) node selection algorithm and ii) message selection algorithm	Custodian node dependant	High when better custodian node is selected	High	High
FairRoute(FR)	Selects a node that has maximum queue length to deliver a message	Queue length dependent	High	Higher than SR	Higher than SR
Retiring Replica(RR)	Uses dynamic replication algorithm that adjust node's replication limit based on current traffic information	Lower than FR, SR or RAPID	Higher than FR	Higher than FR	Higher than FR

IV. SECURITY ISSUES

Delay-tolerant network attends issues that are largely related to end-to-end services where end-to- end data forwarding paths might not exists at all. Due to the severe scarcity of network resources possibly, the issues related to risk are often not addressed. Therefore, it is essential to have some kind of authentication and access control in the network in order to deal with such circumstances.

Several goals have been established for the security component of the DTN architecture. The first and foremost goal is to promptly prevent unauthorized applications from having their data carried through the delay-tolerant networks. Then the next intention would be to prevent unauthorized applications from asserting control over the delay-tolerant network infrastructure. The third goal firmly states to prevent otherwise authorized applications from sending bundles at a rate or class of service for which they lack permission. The fourth goal is to promptly discard bundles that are damaged or improperly modified in transit. Lastly, the goal is to promptly detect and de-authorize compromised entities.

In almost all the network security methods, it is seen that the users mutually authenticate their identities and attempt to conserve the integrity of the messages. However, they do not attempt to authenticate routers that forward their information. In delay-tolerant networks, forwarding nodes (routers and gateways) are also authenticated, and sender information is authenticated by forwarding nodes, so that network resources can be conserved by preventing the carriage of prohibited traffic at the earliest opportunity [22].

In the public key cryptography, each user has a private key and public key pair. A certificate is a file, digitally signed by a Certificate Authority (CA), confirming the user's identity and containing a conformed copy of the user's public key. In DTN, both user and forwarding nodes have key-pair and certificates and the certificates of the users also indicate their Class of Service (CoS) rights. Sender can sign their bundle with their private key, producing the bundle specific digital signature. This signature allows receiver using the sender public key to confirm the authenticity of the sender, the integrity of the message, and the sender's CoS rights.

i. Key management

One of the prime issues in DTN security is the lack of a delay-tolerant method for key management. We are at the stage where we only really know how to use existing schemes, which ultimately require an on-line status checking service or key distribution service which is not practical in a high delay or highly disrupted environment [22]. The basic application schemes regarding key are equivalent to shared secrets or else irrevocable public key (or certificate based) schemes. Thus not much has been discussed on the key management schemes in delay-tolerant network.

ii. Handling Replays

It becomes a challenge to address the replay issues in networks where connectivity is intermittent. In most networking scenarios, the goal is to either eliminate or reduce the probability of messages being replayed. In some DTN contexts this will also be the case particularly as replaying a (e.g., authenticated, authorized) message can be a fairly straight forward way to consume scarce network resources [22].

Thus it becomes difficult at times to define a generic DTN replay detection scheme where lack of proper network paths and resources hinder the replay schemes.

iii. Routing Protocol Security

DTN routing protocol security is another open issue that needs to be addressed. However, if a putative DTN routing protocol was to use either the Bundle protocol or LTP (Licklider Transmission Protocol), it could clearly make use of their existing security features [22].

The security mechanism proposed for metadata blocks has been generalized for other non-payload blocks and may provide a solution to some of these issues [18].

iv. Multicast Security

Another aspect that needs to be addressed in delay-tolerant networks is to restrict nodes from entering in any "multicast" or "any cast" endpoint. The security architecture currently does not address the security aspects of enabling a node to register with a particular multicast or anycast [22]. Without such restriction in multicast or anycast endpoints, any node may register in such an endpoint and thereby receive traffic sent to that endpoint.

v. Performance Evaluation of Security Management Strategies

The security management strategies have various trade-offs as because most of the issues that need to be addressed have been taken care of in traditional networks. Table III presents their implementation and trade-offs. The Key management scheme is based on the traditional cryptography and does not support router authentication. The scheme based on handling replays majorly depends upon the probability of a message being replayed. But its implementation becomes questionable in a network where the connectivity is intermittent. Similarly the security protocols based on routing throw a challenge on the authentication of routers. Performance of multicast nodes degrades due to the absence of security authentication of such nodes. Therefore issues of security in DTNs have multiple facets which need to be addressed as the traditional cryptography does not always hold true for them.

Table III. Performance Comparison of different Security Management Strategies in DTN

Security Management Strategies	**Implementation**	**Trade-offs**
Key Management	Public/private key cryptography	Presence of node authentication but absence of any router authentication
Handling Replays	Eliminate or reduce the probability of messages being replayed	Proper replay detection scheme not present due to lack of network connectivity
Routing Protocol Security	Public/private key cryptography	Not acceptable for router authentication
Multicast Security	No restriction in delivering messages to multicast nodes	Absence of security authentications on multicast nodes

V. CONCLUSIONS

This paper surveys some of the open issues of delay-tolerant network which needs to be addressed. The various routing protocols which come under the umbrella of flooding and forwarding strategies are compared and evaluated in accordance with some performance centric parameters. It can be perceived that a routing protocol which is more knowledgeable about the network yields better performance with respect to delivery ratio. The paper surveys another issue related to congestion control with regards to buffer management. The protocols are based on buffer management which largely deals with queuing strategies. These strategies address the issue of congestion by incorporating some ordering techniques to remove unnecessary messages from the communicating nodes. Lastly, the paper attempts to unfold the security issues which become predominant unless it is not addressed properly. The security of DTN has to pay attention to the issues related to key management, replay management, routing protocol and multicast security. The basic security in DTN remains unexplored as even now the keys use the public-key and private-key to access the confidential information. The router authentication as well as nodal verification of nodes in multicast still remains uncultivated.

REFERENCES

[1] Agoston Petz, Chien-Liang Fok, and Christine Julien, Brenton Walker and Calvin Ardi, *"Network Coded Routing in Delay Tolerant Networks: An Experience Report, University of Texas-Austin, ExtremeCom '11,* September 26-30, 2011, Manaus, Brazil, Copyright 2011 ACM 978-1-4503= 1079-6/11/09.

[2] Jian Shen, Sangman Moh, Ilyong Chunh, *"Routing Protocols in Delay Tolerant Networks: A Comparative Survey",* in: Proceedings of The 23rd International Technical Conference on Circuits/Systems, Computers and Communications (ITC-CSCC 2008), pp.1577-1580, 2008.

[3] Christoph P. *Mayer "Hybrid Routing in Delay-tolerant Networks",* Karlsruher Institut für Technologie (KIT), KIT Scientific Publishing 2012, ISBN 978-3-86644-807-0.

[4] Ying Zhu, Bin Xu, Member, IEEE, Xinghua Shi, and Yu Wang, Senior Member, IEEE, *"A Survey of Social-Based Routing in Delay Tolerant Networks: Positive and Negative Social Effects",* IEEE Communications Surveys & Tutorials, Vol. 15, No. 1, First Quarter 2013.

[5] B. Gu, X. Hong, P. Wang, *"Analysis for bio-inspired thrown-box assisted message dissemination in delay tolerant networks",* Telecommunication Systems, Springer, 2013.

[6] A. Vahdat and D. Becker, *"Epidemic routing for Partially-Connected Ad-Hoc Networks",* Tech. Rep. CS-2000-06, Duke University, July 2000.

[7] T. Small and Z.J. Haas, *"Resource and Performance Tradeoffs in Delay-Tolerant Wireless Networks",* in Proceedings of the ACM SIGCOMM Workshop on Delay-Tolerant Networking (WDTN'05), pp. 260-267, August 2005.

[8] Evan P.C. Jones, Paul A.S. Ward, *"Routing Strategies for Delay-Tolerant Networks",* s.l. : ACM, 2006, Computer Communication Review.

[9] S. Jain, K. Fall and R. Patra, *" Routing in a delay-tolerant network",* in Proceeding of ACM SIGCOMM, vol. 34, pp. 145-158, ACM Press, October 2004.

[10] E.P.C. Jones, L. Li and P.A.S. Ward, *"Practical Routing in Delay-Tolerant Networks",* Proc. ACM SIGCOMM Workshop Delay-Tolerant Networking (WDTN '05), pp. 237-243, Aug. 2005.

[11] Andrew Michael *Grundy "Congestion Control Framework for Delay-Tolerant Communications",* Thesis submitted to the University of Nottingham, Jul. 2012.

[12] A. Balasubramanian, B. Levine, and A. Venkataraman, *"DTN Routing as a Resource Allocation Problem",* In ACM SIGCOMM Computer Communication Review, volume 37, pages 373-384, ACM, 2007.

[13] S. Burleigh, E. Jennings, and J. Schoolcraft, *"Autonomous Congestion Control in Delay-Tolerant Networks",* SpaceOps, 2006.

[14] A. Lindgren and K.S. Phanse, *"Evaluation of Queuing Policies and Forwarding Strategies for Routing in Intermittently Connected Networks",* in Proc. of IEEE COMSWARE, pages 1-10, 2006.

[15] M. Seligman, K. Fall, and P. Mundur. *"Storage Routing for DTN Congestion Control",* Wireless Communications and Mobile Computing, 7(10):1183-1196, 2007.

[16] P.U. Tournoux, J. Leguay, F. Benbadis, V. Conan, M.D. De Amorim, J. Whitbeck, et al. *"The accordion phenomenon: Analysis, characterization, and impact on DTN routing",* In IEEE Infocom. Citeseer, 2009.

[17] M. Radenkovic and A. Grundy, Poster*: "Congestion Aware Data Dissemination in Social Opportunistic Networks",* SIGMOBILE Mobile Computing and Communications Review (MC2R), 14(3):31-33, 2010.

[18] S.C. Nelson, M. Bakht, R. Kravets, and A.F. Harris, *"Encounter based routing in DTNs",* ACM SIGMOBILE Mobile Computing and Communications Review, 13(1):56-59, 2009.

[19] J.M. Pujol, A.L. Toledo, and P. Rodriguez. *"Fair routing in delay tolerant networks",* in IEEE Infocom, pages 837-845. IEEE, 2009.

[20] Yue Cao and Zhili Sun, *"Routing in Delay/Disruption Tolerant Networks: A Taxonomy, Survey and Challenges",* Member, IEEE, IEEE Communications Surveys & Tutorials, Accepted For Publication, 2013.

[21] N. Thompson, S. Nelson, M. Bakht, T. Abdelzaher, and R. Kravet, *"Retiring replicants: Congestion Control for Intermittently Connected Networks",* IEEE Infocom, 2010.

[22] Harminder Singh Bindra, Amrit Lal Sangal, *"Considerations and Open Issues in Delay Tolerant Networks (DTNs) Security",* Wireless Sensor Network, Scientific Research, pp. 645-648, Aug 2010.

