International Journal of Trend in Research and Development, Volume 2(3), ISSN: 2394-9333
www.ijtrd.com

Reliable Routing and Buffer Management Based On Delivery Probability In Intermittently Connected Delivery Networks

M.Dinesh and R.Sivakumar
M.E (Computer Science & Engineering) and Professor and Head, Department of IT,
Tamilnadu College of Engineering, Karumathampatti, Coimbatore, India.

Abstract: Wireless networks have become a common means of communication, and their popularity continues to rise as they enable communication in locations and settings where it was previously unfeasible. While promising many advantages, these networks also pose new challenges. The limited radio coverage, unreliable nature of the wireless channel, and mobility of network nodes can lead to frequent disruption of communication links, dynamic network topology, variable bandwidth availability, and high channel error rates. These challenges seek novel solutions to allow a growing number of wireless, mobile users to run applications and avail network services in ways similar to that in wired networks. This project makes contributions to three research areas related to wireless and disruption tolerant networks. Routing and forwarding to enable disruption tolerant communication in intermittently connected networks, Analysis of properties of human mobility and their effect on network protocols in disruption tolerant networks, and Quality of service mechanisms for wireless and mobile networks. In intermittently connected networks, there may rarely or never exist a fully connected path between a source and destination. This invalidates the basic assumption of end-to-end communication prevalent in the Internet and renders traditional routing protocols impractical. It is proposed, PRoPHET, a novel routing protocol for intermittently connected networks. It takes advantage of the mobility of nodes, and the predictability of that mobility for routing. The protocol and various forwarding strategies and queuing policies are studied in detail. The benefits of PRoPHET are evident on comparing its performance with contemporary work. Communication in intermittently connected and disruption tolerant networks is often highly dependent on the mobility of the nodes in the network. Thus, it is important to have good understanding of basic properties of user mobility in order to design network protocols that can operate under those conditions. Using real-life traces, characterize human mobility patterns and their impact on forwarding algorithms in mobile networks with and without infrastructure. Finally, it is presents evaluated four mechanisms for providing service differentiation in a wireless LAN, and give recommendations on their use in different scenarios. We propose a novel admission control scheme for mobile ad hoc networks, which is able to better cope with high mobility in the network compared to previous solutions.

1.INTRODUCTION

Wireless networks have many advantages over wired networks. Flexibility by allowing users to access the network from a variety of locations, and also while users are mobile. In areas where deployment of wired infrastructure is prohibitively expensive, e.g., in rural areas and in poor and developing countries, wireless networks provide a cost-effective alternative for communication. In hostile environments such as disaster sites and battlegrounds, wireless communication is often the only feasible solution as it is physically difficult to deploy and ensure the continued operation of infrastructure. Over the past decade, wireless networks have become more and more common. Technological advances have taken wireless technologies from being expensive, having low capacity, and being cumbersome to deploy, to being cheap and simple to deploy with capacity close to that of wired networks. Mobile phones are becoming a ubiquitous part of every-day life, and in certain parts of the world they are now more common than their wired counterparts. A variety of portable computers and consumer electronics can now be equipped with a range of wireless technologies. While wireless and mobile networks create many opportunities for computer communication, they also pose new challenges:

frequent disconnections, limited bandwidth, long delays, and high bit-error rates. Most of the networking protocols that are widely used today, e.g., the TCP/IP protocol suite, were designed with wired networks in mind; fixed network topology, reliable links, and continuous end-to-end connectivity were the implicit assumptions. The fundamental differences between wired and wireless mobile networks render many of the traditional network protocols impractical.

1.1. Routing and Forwarding in Disruption Tolerant Networks.

Wireless mobile networks may suffer from intermittent connectivity for various reasons: limited radio coverage of base stations, mobility of nodes, sparse network density, and harsh radio channel conditions. In these circumstances, a contemporaneous end-to-end path between source and destination nodes may never exist, rendering traditional routing protocols and forwarding mechanisms incapable of delivering packets to the destination. In particular, we focus on leveraging non-random user mobility patterns for this purpose. Routing and Quality of Service in Wireless and Disruption Tolerant Networks

1.2. Quality of Service in Wireless and Mobile Networks.

Channel capacity is often a scarce resource in wireless networks. As the number of nodes in a network grows, there will be contention among the nodes for the available channel capacity. Service differentiation is the key to provide acceptable performance to a heterogeneous mix of applications with different QoS requirements. It is also vital to perform admission control to the network to ensure that the network does not become overloaded, resulting in performance degradations. The significant scientific contributions of this thesis are:

- Proposal of PRoPHET, a novel routing protocol for intermittently connected networks, including a detailed specification of the protocol for use in implementations.
- Proposal of various forwarding and queue management strategies for use in intermittently connected networks.
- New insights into methodologies for collecting and analysing user mobility traces.
- Proposal of MACMAN, an admission control scheme for mobile ad hoc networks.

1.3. Wireless Local Area Networks (WLANs)

Wireless Local Area Networks (WLANs) provide a good trade-off between the flexibility of wireless networks, and the capacity of wired networks. As a result, wireless LANs have become the popular choice of wireless access for many settings. Wireless LANs are deployed at many sites such as university campuses, corporate offices, coffee shops, and airports, and it is expected that the number of installations of these networks will increase to cover even larger areas. As hardware prices have recently dropped drastically for both end-host WLAN adaptors and infrastructure equipment, the future growth of WLAN deployments can be expected to be even more rapid. With its extensions is the dominant technology used in this kind of network. Other competing technologies have been proposed, but have not succeeded as well.

1.4. Ad hoc Networks

An ad hoc network is a wireless network where no fixed infrastructure is in place. Nodes in an ad hoc network communicate directly with the other nodes when possible. Communication between nodes that are not within transmission range is made possible by other nodes in the network taking part in the routing and forwarding of packets. This means that each node can act both as an end-host as well as a router in the network. Nodes in an ad hoc network may also be mobile. Thus, these networks are characterized by properties different from those of wired networks. Error-rates can be high, and topology changes in the network can be frequent. This renders most traditional routing protocols impractical for ad hoc networks. Ad hoc routing protocols can be broadly classified into two types, proactive and reactive. The following sections will discuss these main two types of protocols, as well as some other possible design choices for routing in ad hoc networks.

1.5. Proactive Routing Protocols

Proactive routing protocols such as the Destination Sequence Distance Vector (DSDV) routing protocol, Optimized Link State Routing (OLSR), and the Topology Broadcast based on Reverse-Path Forwarding (TBRPF) routing protocol are similar to the routing protocols used in wired networks in that they try to always maintain entries in their routing tables for all possible destinations in the network. This approach works well at low mobility, and allows packet transmission to occur as soon as a data packet is generated by the application since the route to the destination is known. However, since nodes in an ad hoc network are mobile, topology changes can be frequent, generating lots of control traffic for maintaining routing tables.

1.6. Reactive Routing Protocols

On the other hand, reactive protocols such as the Dynamic MANET On-demand routing protocol (DYMO), Ad-hoc On-demand Distance Vector (AODV), Dynamic Source Routing (DSR), and the Temporally Ordered Routing Algorithm (TORA) try to reduce the amount of control traffic required, by only determining routes on-demand. This means that nodes do not acquire a route to a certain destination until the need for it arises A route discovery process is then initiated to find a route to the destination.

1.7. Other Types of Routing Protocols

The two main types of protocols can also be combined into a hybrid protocol such as the Zone Routing Protocol (ZRP). Hybrid protocols perform proactive route maintenance in a local region, but use a reactive route discovery process to find routes to destinations further away. Several other hierarchical routing schemes have also been proposed to reduce control traffic overhead. Most of the available ad hoc routing protocols take the traditional approach when selecting among several paths, and try to find the shortest path between source and destination. In many cases, this is probably the most favourable path to choose, but there also exist routing protocols that take other aspects into account such as link stability, load balancing, and power consumption. This is usually done in order to choose routes that remain stable longer, provide fairness in the forwarding responsibilities among the nodes, or to maximize the lifetime of the network.

1.8. Internet Engineering Task Force MANET Working Group

The Internet Engineering Task Force (IETF) is the standardization body that creates and maintains standards for the Internet and related areas. In the Mobile Ad hoc Networks (MANET) working group of the IETF, work is being done on the standardization of ad hoc routing protocols. The group has now entered a new phase, where it will use the experiences from the work on these previous protocols to create two new routing protocols, one proactive and one reactive. Previous protocols have all have been created by individual groups of researchers or engineers and submitted into the IETF process. The new protocols will be the joint product of the people involved in the group; the goal is to create IETF standards.

1.9. Delay and Disruption Tolerant Networks

An ad hoc network can be considered a rather harsh networking environment,but routing in in such networks is still based on the assumption of end-to-end connectivity. There are however still many more extreme scenarios.

1.10. Remote/Indigenous Communities

Communication between villages of the reindeer herding population in the north of Sweden suffer from lack of infrastructure such as wired network access, and other means of networking are either unavailable, intermittent, or too expensive to be viable . Through the use of community gateways, and mobile relays, it is possible to use the existing infrastructure of vehicles and human mobility to provide connectivity between remote and more populated areas. Similar problems exist among other indigenous populations and populations in developing countries.

1.11. Sensor Networking

In sensor networks, a large number of sensors is often deployed to achieve a high degree of redundancy. However, in certain sensor network scenarios it might be possible or desirable to deploy only a smaller number of sensors, to only have a limited subset of the

sensors active at any given time to conserve energy, or sensors may be mobile. Despite this, it is required that data from all sensors be collected even though the network might never be fully connected. Examples of such scenarios include collection of oceanographic data from tags attached to seals or whales in the ocean, or from zebras on the African savanna. Networks such as the ones described above, violate some of the fundamental assumptions required for the operation of conventional network protocols such as the TCP/IP protocol suite. Unless a fully connected path exists, traditional routing protocols cannot correctly route IP packets to their destination, and TCP cannot set up a connection between two hosts. TCP will also experience poor performance if round-trip times are as high as they can be in the networks just described. Thus, there is a need for architectures and protocols that are suitable for these kinds of networks. Work is going on to define an architecture suitable for such networks, and the area has attracted much attention within the research

1.12. The Delay Tolerant Networking (DTN) Architecture

Severe violations of the fundamental requirements for the TCP/IP suite like the ones mentioned above were first noticed in the context of deep space communication. This led to the creation of the interplanetary Networking Special Interest Group (IPNSIG) within the Internet Society. This group considered a network architecture to enable communication in such environments. However, it was realized that the architecture developed was not only applicable to interplanetary networking, but also to several terrestrial scenarios. This effort finally converged into the Delay Tolerant Networking (DTN) architecture. Within the Internet Research Task Force (IRTF), the Delay Tolerant Networking Research Group (DTNRG) was established to work on developing the DTN architecture and supporting technologies. While a fair amount of effort have been put into defining the DTN architecture, algorithms for routing in various DTN scenarios is still an open research issue. More and more research is being done on routing algorithms in general, but there has been few efforts to thoroughly design and specify protocols that can be easily implemented and integrated with the DTN architecture.

1.13. Quality of Service

Traditionally, the Internet has offered one single level of service known as the best-effort service to all traffic in the network. In a best-effort model, all traffic flows share the link bandwidth on equal terms, and the quality of service (QoS) that a flow can get depends on the current traffic load on the links used, the round trip time of the end-to-end path used by the flow, and other network properties. This type of service was sufficient for most applications that were common when the Internet protocols were designed. Since then, many new killer applications have emerged that are inelastic and expect better service guarantees, for example: Internet telephony, video conferencing, audio and video streaming. To enable the users to use these multimedia applications with satisfactory performance even when network resources are scarce, some form of quality of service provisioning scheme must be used. Such QoS schemes can be used to differentiate between traffic flows to give higher priority to one traffic flow over another, to perform admission control to ensure that only a certain number of flows are allowed to use a certain type of service, or a combination of both. Within the IETF, work has been done on defining quality of service architectures. The two different architectures are Integrated Services. and Differentiated Services. In IntServ, admission control and traffic flow prioritization is done in the routers in the network for individual flows. Routing and Quality of Service in Wireless and Disruption Tolerant Networks The resource reservation protocol RSVP is used to set up the state in the network for the reservations required by the flows. Since this architecture requires per-flow state to be stored in the routers in the network, this can quickly become a scalability problem as the number of flows grows. The DiffServ framework is designed to be more scalable than IntServ. Instead of keeping per-flow states and setting up explicit reservations through the network, DiffServ routers support a small number of service classes. A small label is added to the headers of IP packets which is used by routers to determine which service class the packet belongs to. This is then used to provide service differentiation. In this

architecture it is vital that there are mechanisms in place at the edges of the network to ensure that packets are labelled properly to ensure that no more traffic than can be supported is allowed in any service class. Given the proliferation of wireless networks, it was natural for users to expect similar QoS support when accessing services over a wireless link, and even when users are mobile. Section 7 discusses in more details the special requirements for providing quality of service in wireless and mobile networks.

1.14. Routing in Intermittently Connected Networks

Routing in intermittently connected networks, and propose how routing and forwarding can be done effectively and efficiently by making use of the non-random properties of contact patterns among users. In intermittently connected networks, disconnections are so frequent that there may never exist a fully connected path through the network between a source and a destination that wish to communicate. To enable eventual message delivery in such networks, the mobility of nodes together with a transitive propagation of messages in a store-and-forward manner must be relied upon as shown .This means that nodes may have to buffer messages for other nodes for a long time. When a node encounter a potential message carrier, it transfers relevant messages to the carrier. This continues until the message eventually reaches its destination.

1.2.1. NETWORK SIMULATOR

A network simulator is a software program that imitates the working of a computer network. In simulators, the computer network is typically modeled with devices, traffic etc and the performance is analyzed. Typically, users can then customize the simulator to fulfill their specific analysis needs. Simulators typically come with support for the most popular protocols in use today, such as WLAN, Wi-Max, UDP, and TCP.

Why Network simulation?

- Protocol validation
- Controlled experimental conditions
- Low cost, time, collaboration, complexity

Why NS?

Provides:

- Protocols: TCP, UDP, HTTP, etc.
- Traffic Models: Web Traffic, CBR,
- Topology Generation tools
- Visualization tools
- Large validation package

NS Structure:

- C++ event scheduler protocols.
- TCL scripts protocols.
- TCL objects expose an interface to C++ objects system configuration.

Advantages:

- Flexible and state of the art tool
- Contains wide classes of internet protocols including Multicasting, SRM, RTP, ATM and wireless networks
- Widely used => respectful results + easy to compare

Disadvantages:

- “Alpha” quality
- Minimal docs
- Incomplete API

1.2.2. Simulations

Most of the commercial simulators are GUI driven, while some network simulators require input scripts or commands (network parameters). The network parameters describe the state of the network (node placement, existing links) and the events (data transmissions, link failures, etc). Important outputs of simulations are the trace files. Trace files can document every event that occurred in the simulation and are used for analysis. Certain simulators have added functionality of capturing this type of data directly from a functioning production environment, at various times of the day, week, or month, in order to reflect average, worst-case, and best-case conditions. Network simulators can also provide other tools to facilitate visual analysis of trends and potential trouble spots.

Most network simulators use discrete event simulation, in which a list of pending "events" is stored, and those events are processed in order, with some events triggering future

events -- such as the event of the arrival of a packet at one node triggering the event of the arrival of that packet at a downstream node.

Some network simulation problems, notably those relying on queuing theory, are well suited to Markov chain simulations, in which no list of future events is maintained and the simulation consists of transiting between different system "states" in a memory less fashion. Markov chain simulation is typically faster but less accurate and flexible than detailed discrete event simulation. Some simulations are cyclic based simulations and these are faster as compared to event based simulations.

Simulation of networks can be a difficult task. For example, if congestion is high, then estimation of the average occupancy is challenging because of high variance. To estimate the likelihood of a buffer overflow in a network, the time required for an accurate answer can be extremely large. Specialized techniques such as "control variates" and "importance sampling" have been developed to speed simulation.

2.SYSTEM ANALYSIS

2.1. GENERAL

The purpose of the system analysis phase of a project is to analysis the problem statement and finds the additional requirements in the project. In the system analysis phase, the project team defines the problem statement in the project.

2.2. EXISTING SYSTEM

2.2.1. Related works-
Decentralizing Attribute-Based Encryption

Multi-Authority Attribute-Based Encryption (ABE) system. In their system, any party can become an authority and there is no requirement for any global coordination other than the creation of an initial set of common reference parameters. A party can simply act as an ABE authority by creating a public key and issuing private keys to different users that react their attributes. A user can encrypt data in terms of any Boolean formula over attributes issued from any chosen set of authorities. Finally, our system does not require any central authority. In constructing their system, their largest technical hurdle is to make it collusion resistant. Prior Attribute-Based Encryption systems achieved collusion resistance when the ABE system authority "tied" together different components of a user's private key by randomizing the key. However, in their system each component will come from a potentially different authority, where they assumed no coordination between such authorities. They created new techniques to tie key components together and prevent collusion attacks between users with different global identifiers. Attribute-Based Encryption system. In our system, any party can become an authority and there is no requirement for any global coordination other than the creation of an initial set of common reference parameters. A party can simply act as an authority by creating a public key and issuing private keys to different users that reflect their attributes. Different authorities need not even be aware of each other. They used the Chase concept of global identifiers to "link" private keys together that were issued to the same user by different authorities. A user can encrypt data in terms of any boolean formula over attributes issued from any chosen set of authorities. They thus avoided the performance bottleneck incurred by relying on a central authority, which makes their system more scalable. They also avoided placing absolute trust in a single designated entity which must remain active and uncorrupted throughout the lifetime of the system. This is a crucial improvement for efficiency as well as security, since even a central authority that remains uncorrupted may occasionally fail for benign reasons, and a system that constantly relies on its participation will be forced to remain stagnant until it can be restored. In their system, authorities can function entirely independently, and the failure or corruption of some authorities will not affect the operation of functioning, uncorrupted authorities. This makes their system more robust.

2.2.2. Bounded Cipher text Policy Attribute Based Encryption

In a cipher text policy attribute based encryption system, a user’s private key is associated with a set of attributes and an encrypted cipher text will specify an access policy over attributes. A user will be able to decrypt if and only if his attributes satisfy the cipher text’s policy. In this work, they presented the first construction of a cipher text-policy attribute based encryption scheme having a security proof based

on a number theoretic assumption and supporting advanced access structures. Previous CP-ABE systems could either support only very limited access structures or had a proof of security only in the generic group model. Their construction can support access structures which can be represented by a bounded size access tree with threshold gates as its nodes. The bound on the size of the access trees is chosen at the time of the system setup. Their security proof is based on the standard Decisional Bilinear Diffie-Hellman assumption.

2.2.2.1. Techniques.

Their construction can be seen as a way to reinterpret the KP-ABE scheme of with a fixed "universal" tree access structure as a CP-ABE scheme. Such a reinterpretation does not follow directly because in a KP-ABE scheme, the key material for each attribute is "embedded" into the access structure in a unique way depending on where it occurs in the access policy. To overcome this difficulty, they introduced many "copies" of each attribute for every position in the access structure tree where it can occur. This causes a significant increase in private key size, but does not significantly affect cipher text size. However, since the actual access structure to be used for a particular cipher text must be embedded into the fixed "universal" tree access structure in the KP-ABE scheme, this causes a blow up in cipher text size. This effect can be moderated by having multiple parallel CP-ABE schemes with different sized "universal" tree access structures underlying the scheme, which allows for a trade-off between cipher text size and the size of the public parameters and private keys. As a result of the issues discussed above, their scheme has significantly worse efficiency than the scheme. They have left constructing CP-ABE schemes based on number-theoretic assumptions with better efficiency and unbounded access structures as important open problems.

2.2.3. Improving Privacy and Security in Multi-Authority Attribute-Based Encryption

Attribute based encryption (ABE) determines decryption ability based on a user's attributes. In a multi-authority ABE scheme, multiple attribute-authorities monitor different sets of attributes and issue corresponding decryption keys to users, and encrypts can require that a user obtain keys for appropriate attributes from each authority before decrypting a message. Chase gave a multi-authority ABE scheme using the concepts of a trusted central authority (CA) and global identifiers (GID). However, the CA in that construction has the power to decrypt every cipher text, which seems somehow contradictory to the original goal of distributing control over many potentially untrusted authorities. Moreover, in that construction, the use of a consistent GID allowed the authorities to combine their information to build a full profile with all of a user's attributes, which unnecessarily compromises the privacy of the user. A solution which removes the trusted central authority, and protects the users' privacy by preventing the authorities from pooling their information on particular users, thus making ABE more usable in practice. It is presented a multi-authority ABE with user privacy and without the trusted authority. These requirements are non-trivial to satisfy, due in both cases to the collusion resistance requirement of ABE. Brent Waters suggested an approach for removing the CA requirement, in which each pair of attribute authorities would share a secret key. They formalized this idea, and proved that it is secure as long as at least two of the AAs are honest. The new solution uses techniques for distributed pseudorandom functions (PRF). Note that Lin et al. recently proposed a different approach for building a multi-authority ABE scheme without a central authority. However, their construction requires designers to fix a constant m for the system, which directly determines efficiency. The resulting construction is such that any group of m + 1 colluding users will be able to break security of the encryption. Our scheme on the other hand is secure no matter how many users collude. They also presented an anonymous key issuing protocol which allows multi-authority ABE with enhanced user privacy - 1) They allow the users to communicate with AAs via pseudonyms instead of having to provide their GIDs in the clear, and 2) They prevented the AAs from pooling their data and linking multiple attribute sets belonging to the same user.

In a real network, DTN operations proceeds roughly in three stages.

- **Neighbor Discovery**. Peers must discover one another before a transfer opportunity

can begin; they do not know when the next opportunity will begin.

- **Data Transfer**. When two peers meet, the amount of data they can transfer is limited. Peers do not know the duration of each opportunity.
- **Storage management**. As packets are received from a neighbor, each peer must manage its finite local buffer space by selecting packets to delete according to some algorithm. Messages that are destined for a receiving peer are passed up to the application layer and removed from the buffer.

Each peer carries all messages until the next meeting occurs. A peer will continue to forward a message to any number of other peers until its copy of the message times out, it is notified of delivery by an ack, or the message is dropped due to a full buffer.

2.3. PROPOSED WORK

2.3.1. Disruption tolerant networks (DTNs)

Delay and disruption tolerant networks (DTNs) are a new class of wireless networks that seek to address the networking issues in mobile or challenging environments that lack continuous network connectivity. DTNs have emerged recently and are continuing to gain extensive efforts from the networking research community. In the literature, these networks are found under different terminologies such as sparse mobile ad hoc networks, extreme wireless networks, or under another commonly used term intermittently connected networks. Basically, DTNs appear in areas where the network spans over large distances with low node density and/or with high node mobility. DTNs might appear also due to short radio range, power saving mechanism at the nodes, or nodes failure. Generally speaking, DTNs are wireless networks that do not conform to Internet or to traditional multihop and ad hoc wireless networks underlying structures and assumptions. In particular, they are characterized mainly by the following specific features :

- Intermittent connectivity where an end-to-end path between a given source-destination pair does not exist most of the time. Path disconnections are frequent and arise from two main factors, namely motion and/or limited power at the nodes. Disconnection due to motion can arise when one or both nodes at the end of a communication link move, or due to some intervening object or signal that obstruct the communication. These disconnections can be predicted, for instance when the nodes move away according to a predetermined schedule or, an opportunistic for instance according to random walk of the nodes. Disconnections that are due to power outage result commonly from some power saving mechanisms at the wireless devices, e.g. case of sensor networks. The latter disconnections are often predictable.
- Nodes have low power capabilities and limited resources. In many DTNs, nodes are generally battery powered and/or deployed in areas lacking power infrastructure. In some other situations, nodes have limited memory and/or processing capabilities.
- Large delays which are basically due to long queueing times resulting from frequent disconnections, or from low data rate at the devices.

2.3.2. Routing in DTNs

Due to frequent disconnections in DTNs, instantaneous end-to-end routes do not exist, and hence most of the traditional Internet and/or mobile ad hoc routing protocols fail. However, end-to-end routes may exist over time if the nodes can take advantage of their mobility by exchanging and carrying other node messages upon meetings, and by delivering them afterward to their corresponding destinations. The latter concept has given rise to a novel routing paradigm in these networks called the store-carry-and-forward approach, in which intermediate nodes serve as relays for each other. Thus, the term “mobility-assisted routing approach” that is used in conjunction to describe these schemes. Unfortunately, these techniques result in high latency, since packets need to be carried for long time periods before being delivered. When the delivery latency is not critical, as the case of delay-tolerant networks, the store-carry-and-forward paradigm can prove to be adequate. For instance, this is the case when the delivery of the messages is very important, possibly more important than the delay. Basically, with the

store-carry-and-forward approach, the delivery delays of packets depend on the rate at which contact opportunities1 are created in the network, as well as the availability of network resources, such as storage space and energy. The various studies that considered routing techniques in DTNs have examined the tradeoffs between optimizing the delivery ratio and delivery delay from one side, and reducing node resource consumptions in terms of storage and battery usage from the other side. However, the intricacy of each one depends on the particularity of network environment at hand, the mobility model of the nodes, the performance objectives to attain, and other criteria. The survey and classify various research works that have considered routing schemes for DTNs. Actually, there are different approaches to categorize these schemes. Hereafter, we propose a classification that is based on the way that these schemes make use of the knowledge of potential contact opportunities of the nodes in order to perform routing. Specifically, depending on whether these contact opportunities are scheduled, controlled, predicted or opportunistic, these approaches can be grouped into one of the four following families.

2.3.3. Scheduled-contact based routing

This section surveys the routing approaches that attempt to improve the performance of a sparse network when its dynamics are known in advance such as for instance Low-earth Orbiting satellites (LEO) based networks. In a given network scenarios, the most important metrics of interest are the following: contact times between nodes, queue lengths at the nodes, the network traffic load. The complete knowledge of these three metrics by the routing protocol allows it to select optimal routes between the nodes. Despite that the implementation of the complete knowledge in a distributed environment is a very hard task, its evaluation is important as it constitutes the best case scenario compared with other cases where only a partial knowledge is available to the routing protocol. On the other side, the approaches that use no knowledge constitute the worst case scenario.

2.3.4. Controlled-contact based routing approaches

In this section, we discuss some routing approaches in DTNs which control the mobility of some dedicated additional mobile nodes in order to improve the network performance by increasing the contact opportunities between participating nodes. The additional mobile nodes can either have fixed predetermined paths conceived in a way to permit them to meet a large number of nodes, or their paths can be adjusted dynamically to meet traffic flows between the nodes. Their main task is to relay packets between the participating nodes by providing a store-carry-forward service. Indeed, by controlling the mobility of the additional nodes, a DTN network administrator would be able to limit the delivery delay and to provide bounds on some other performance metrics of the network. In the literature, several research works have discussed the integration of some special mobile nodes and the design of travel paths of these nodes to meet certain optimization criteria.

2.3.5. Predicted-contact based routing approaches

Predicted routing techniques attempt to take advantage of certain knowledge concerning the mobility patterns or some repeating behavioural patterns. Based on an estimation of that knowledge, a node will decide on whether to forward the packet or to keep it and wait for a better chance. Basically, each node is assigned a set of metrics representing its likelihood to deliver packets to a given destination node. When a node holding a packet meets another node with a better metric to the destination, it passes the packet to it, hence increasing the packet likelihood of being delivered to its corresponding destination. According to the nature of knowledge, we propose to reclassify the algorithms falling under this category as based on mobility-pattern or based on history.

2.3.6. Mobility-pattern based approaches

Approaches falling under this section attempt to take advantage of common behaviours of node mobility patterns in the network in order to derive decisions on packet forwarding. In fact, by letting the nodes learn the mobility pattern characteristics in the network, efficient packet forwarding decisions can be taken. Two main issues are related to these approaches. The first issue concerns the definition and the

characterization of the node mobility pattern where several ways can exist to characterize and acquire such a pattern. For instance, the appearance of stable node clusters in the network, or the acquisition of statistical information related to meeting times or to the visit frequencies of nodes to a given set of locations are examples of mobility patterns that can be exploited by the nodes. The second issue is related to the way through which a node can learn and acquire its own pattern as well as those of other nodes. In particular, the presence of some external signals to the nodes such as GPS coordinates or some fixed beacons help greatly the nodes to acquire easily the mobility patterns in the network. Alternatively, nodes can also learn their own mobility patterns without any external signal by relying only on previous observations and measurements, or by exchanging pattern information with other nodes. Several routing works in DTNs that use mobility patterns to derive forwarding decisions have appeared in the literature.

2.3.7. History based approaches

History based approaches are developed mainly for heterogeneous mobility movements. They rely on the observation that the future node movements can be effectively predicted based on repeating behavioral patterns. For instance, if a node had visited a location at some point in time, it would probably visit that location in another future time. Actually, if at any point in time a node can move randomly over the network area, an estimate based on previous contacts is of no help to decide on packet forwarding. However, if the mobility process has some locality, then last encounter times with other nodes can be associated with some weights that can be ranked based on their likelihood to deliver the messages to the corresponding destinations. The following works illustrate the working mechanisms of some of these approaches.

One of the pioneer work that considered history-based routing in sparse mobile networks is the work of Davis et al. The objective of their work is to study the impact of different buffer management techniques on an extended variant of the epidemic protocol on nodes with limited buffer size. Even though their work is not related to routing, the way by which the packets are sorted upon a contact influences implicitly the performance of the routing protocol. More precisely, when two nodes meet, they will first transfer the packets destined to each other, then they will exchange the lists of their remaining stored packets. The combined list of remaining packets is next sorted according to the used buffer management strategy, and each node will request the packets it does not have among the top K sorted packets. The authors have explored four different buffer management techniques, among them the Drop-Least-Encountered (DLE) technique which makes use of previous contacts with other nodes to decide on packet ranking. Basically, nodes using the DLE technique keep a vector indexed by addresses of other nodes where each entry estimates the likelihood of meeting the corresponding node. At each time step, a given node A updates its likelihood meeting values for every other node C with respect to the co-located node B according to the temporal difference rule. If node A meets B, it is likely that A meets B again in the future, and hence A is a good candidate for passing the packets to B. Thus, node A should increase its likelihood for node B. If B has a high encounter for node C, then A should increases its likelihood of meeting C by a factor proportional to the likelihood of meeting between B and C. Last, if at a given time step, node A did not meet any other node, the different likelihood values decrease in a constant rate.

2.3.8. Opportunistic-contact based routing approaches

Opportunistic based approaches are generally characterized by random contacts between participating nodes followed by potential pair-wise exchanges of data. Given that meeting, and consequently, data exchanges are subject to the characteristics of the mobility model which are in general unpredicted, these approaches rely on multi-copy schemes to speed up data dissemination within the network. In the following, we subdivide these approaches into epidemic-based approaches and coding based approaches.

2.3.9. Epidemic based approaches

Epidemic based approaches imitate the spread of contagious disease in a biological environment. Similarly to the way an infected individual passes on a virus to those who come

into contact, each node in an epidemic-based system will spread copies of packets it has received to other susceptible nodes. The number of copies that an infected node2 is allowed to make, termed as the fan-out of the dissemination, and the maximum number of hops that a packet is allowed to travel between the source and the destination nodes, represented by a hop count field in the packet, define the epidemic variant of the algorithm. These two parameters can be tuned to trade delay for resource consumption. Clearly, by allowing the packet to spread throughout the mobile nodes, the delay until one of the copies reaches the destination can be significantly reduced. However, this comes at the cost of introducing a large overhead in terms of bandwidth, buffer space and energy consumption. Several variants of epidemic-based approaches have been proposed and their performance in terms of delay and resource consumption have been evaluated.

2.3.10. Coding based approaches

The approaches in previous sections are primarily based on packet flooding in order to improve the efficiency of packet delivery. Unfortunately, these improvements come at the expense of introducing large overhead in the network due to redundant packet transmissions. The approaches presented in this section alleviates the effect of flooding through the use of smarter redundant algorithms that are based on coding theory. In the following, we consider two main coding algorithms that appeared in the literature and which have shown their suitability to the opportunistic contact networks, namely the erasure coding and the network coding. In the erasure coding scheme, upon receiving a packet of size m, the source produces n data blocks of size l < m. The coding algorithm composes these blocks in a such way to allow the destination to retrieve the original message on receiving any subset of these blocks. More precisely, the transmission of the packet is completed when the destination receives the kth block, regardless of the identity of the k ¼ m/l < n blocks it has received. The blocks are forwarded to the destination through the relay nodes according to store-carry-and-forward approach. The performance analysis of this approach in opportunistic contact network has shown to improve significantly the worst case delay with fixed amount of overhead. Further, it has been shown that erasure coding improve the probability of packet delivery in DTNs with transmissions failures. In the network coding scheme, instead of simply forwarding the packets, nodes may transmit packets with linear combinations of previously received ones. For example, consider the three nodes case where nodes A and C want to exchange packets via the intermediate node B. A (resp. C) sends a packet a (resp. c) to B, which in turn broadcasts a xor c packet to A and C. Both A and C can recover the packet of interest, while the number of transmissions is reduced. Different aspects of network coding with limited storage resources have been discussed and different techniques have been proposed. The main result is that network coding benefits more from node mobility and performs well in scenarios of high packet drop rate where simple flooding approaches fail.

2.3.11. Security threat in DTN

Mobile nodes in military environments such as a battlefield or a hostile region are likely to suffer from intermittent network connectivity and frequent partitions. Disruption-tolerant network (DTN) technologies are becoming successful solutions that allow wireless devices carried by soldiers to communicate with each other and access the confidential information or command reliably by exploiting external storage nodes. Some of the most challenging issues in this scenario are the enforcement of authorization policies and the policies update for secure data retrieval. Cipher text-policy attribute-based encryption (CP-ABE) is a promising cryptographic solution to the access control issues. However, the problem of applying CP-ABE in decentralized DTNs introduces several security and privacy challenges with regard to the attribute revocation, key escrow, and coordination of attributes issued from different authorities. It is propose a secure data retrieval scheme using CP-ABE for decentralized DTNs where multiple key authorities manage their attributes independently. We demonstrate how to apply the proposed mechanism to securely and efficiently manage the confidential data distributed in the disruption-tolerant military network.

CONCLUSION

In this paper it have looked at intermittently connected networks, an area where a lot of new applications are viable, vouching for an exciting future the mechanisms are present. Therefore, proposed the use of probabilistic routing using observations of non-randomness in node mobility in such networks. To accomplish this, we have defined a delivery predictability metric, reflecting the history of node encounters and transitive and time dependent properties of that relation. We have proposed PRoPHET, a probabilistic protocol for routing in intermittently connected networks, that is more sophisticated than previous protocols. PRoPHET uses the new metric to enhance performance over previously existing protocols. Simulations performed have shown that in a community based scenario, PRoPHET clearly gives better performance than Epidemic Routing. Further, it is also shown that even in a completely random scenario, the performance of PRoPHET is still comparable with the performance of Epidemic Routing. Thus, it is fair to say that PRoPHET succeeds in its goal of providing communication opportunities to entities in a intermittently connected network with lower communication overhead, less buffer space requirements, and better performance than existing protocols.

REFERENCES

1. Ahmed Elwhishi, pin Han Ho, K. Nail and Basem Shihaday (2011), 'Contention Aware Routing for Intermittently Connected Mobile Networks', IEEE Transaction on Vehicular Technology.

2. Andr´es Ferragut and Fernando Paganini (2012), 'Network resource allocation for users with multiple connections: fairness and stability', IEEE/ACM Transactions on networking.

3. Anders Lindgren, Avri Doria and Olov Schel´en (2003), 'Probabilistic Routing in Intermittently Connected Networks', IEEE MobiHoc'03.

4. Daniel E. Lucani, Milica Stojanovic and Muriel M´edard (2012),'Random Linear Network Coding For Time Division Duplexing: Energy Analysis', IEEE.

5. Daojing He, Chun Chen, Jiajun Bu and Sammy Chan (2013), 'Security and Efficiency in Roaming Services for Wireless Networks Challenges, Approaches, and Prospects', IEEE Communications Magazine.

6. Elias Bou-Harb, Claude Fachkha, Makan Pourzandi, Mourad Debbabi, and Chadi Assi (2013), 'Communication Security for Smart Grid Distribution Networks', IEEE Communications Magazine.

7. Hany Samuel, Weihua Zhuang and Bruno Preiss (2011), 'Improving the Dominating-Set Routing over Delay-Tolerant Mobile Ad-Hoc Networks via Estimating Node Intermeeting Times', Hindawi Publishing Corporation, EURASIP Journal on *Wireless Communications and Networking*, Volume, Article ID 402989, 12 pages, doi:10.1155/2011/402989.

8. John Whitbecka,b, Vania Conana (2010), 'HYMAD: Hybrid DTN-MANET Routing for Dense and Highly Dynamic Wireless Networks', IEEE.

9. Manohar. G, Kavitha. D and Sreedhar. S (2011), 'Autonomic Diffusion Based Spray Routing in Intermittently Connected Mobile Networks with Multiple Copies',International Journal of *Smart Sensors and Ad Hoc Networks (IJSSAN)* ISSN, No. 2248-9738 Volume-1, Issue-2.

10. Ramesh. S, Indira. R, Praveen. R and P. Ganesh Kumar (2013),'s-spray routing protocol for intermittently connected mobile networks', Ictact journal on *Communication Technology*, volume: 04, issue: 03

11. Samuel C. Nelson, Mehedi Bakht, and Robin Kravets (2007), 'Encounter–Based Routing in DTNs', IEEE Communications Magazine.

12. Spyropoulos.T, Psounis.K and Raghavendra.C.S (2004), 'Single-copy routing in intermittently connected mobile networks', 1st Annual IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks (SECON '04).

13. Xiaolan Zhang, Giovanni Neglia, Jim Kurose and Don Towsley (2007), 'Performance modeling of epidemic routing', IEEE Computer Networks.

14. Yanwu Ding, Lun Li, and Jian-Kang Zhang (2013), 'Blind Transmission and Detection Designs with Unique Identification and Full Diversity for Non coherent Two-Way Relay Networks', IEEE Network.
15. Zhaoxu Wang and Wenyi Zhang (2013), 'A Separation Architecture for Achieving

16. Zhihui Shu, Yi Qian, and Song Ci (2013), 'On Physical Layer Security for Cognitive Radio Networks', IEEE Network.