EFFICIENT AND DYNAMIC TOPOLOGY IN DELAY TOLERANT NETWORKS

G.PARTHIPAN  
PG Scholar, CSE  
Jay Shriram Group of Institutions, Tirupur  
g.parthipan3@gmail.com

Mr.A.M RAVisHANKKAR M.E.,  
Assistant Professor/ CSE  
Jay Shriram Group of Institutions, Tirupur  
Ravi662shankkar@gmail.com

Dr.S. RAJALAKSHMI Ph.D.,  
Associate Professor & HOD/CSE  
Jay Shriram Group of Institutions, Tirupur  
mrajislm@gmail.com

ABSTRACT

Delay tolerant networks (DTNs) have attracted much attention from research workers due to their wide applications in various challenging environments. Existing Delay tolerant networks research mainly concentrates on information propagation and packet delivery. Delay tolerant networks where the time evolving topology is known a priori or can be judged. We framed such a time-evolving network as a weighted directed space time graph which includes both special and temporal information. Links that are inside the space time graph are unreliable due to either the dynamic nature of wireless communications. The purpose of our topology design problem is to build a sparse structure from the original space-time graph such that for any pair of devices, there is a space-time path connecting them with reliability higher than the required threshold the total cost of the structure is reduced. Such an optimization problem is NP-hard, thus we propose several heuristics which can significantly downs the total cost of the topology while maintain the “reliable” connectivity over time. In this work we consider both single direction and broadcast reliability of a topology. Extensive simulations are conducted on random DTNs, a synthetic space DTN, and a real-world DTN tracing data. For Encryption process, we are using RC4 Algorithm.

Keywords

DTN’s, positions, Magnets, Nodes.

1. INTRODUCTION

Energy-efficient routing is an effective mechanism for reducing energy cost of data communication in wireless adhoc networks. In general, routes are considering the energy consumed for end-to-end (E2E) packet traversal. Nevertheless, this should not result in finding minimum reliable routes or overusing a specific set of nodes in the network. Efficient routing in adhoc networks is neither complete nor efficient without the consideration of reliability of links and residual energy of nodes. Finding reliable routes can improves quality of the service. Considering the residual energy of nodes in routing can avoid nodes from being used and can eventually lead to an increase in the operational lifetime of the network. The last century, various routing algorithms have been proposed aiming at increasing energy-efficiency, reliability, and the lifetime of wireless ad hoc networks.

We can broadly group them into three categories. The first category includes algorithms that consider the reliability of links to find more reliable routes. For instance, De Couto et al. introduced the notion of expected transmission count (ETX) to find reliable routes that consist of links requiring less number of retransmissions for lost packets. Although such routes may consume less energy since they require less number of retransmissions, they do not necessarily minimize the energy consumption for E2E packet traversal. Considering a higher priority for reliability of routes may result in overusing some nodes. If there are some links more reliable than others, these links will frequently be used to forward packets. Nodes along
these links will then fail quickly, since they have to forward many packets on behalf of other nodes. The other category includes algorithms that aim at finding energy-efficient routes. These algorithms don’t consider the remaining battery energy of nodes to avoid overuse of nodes, even though some of them namely address energy-efficiency and reliability together. Many routing algorithms including energy efficient algorithms proposed have a major drawback. They do not consider the actual energy consumption of nodes to discover energy-efficient routes.

They only consider the transmission power of nodes neglecting the energy consumed by processing elements of transmitters and receivers. What is considered as energy cost of a path by these algorithms is only a fraction of the actual energy cost of nodes for transmission along a path. This negatively affects energy-efficiency, reliability, and the operational lifetime of the network altogether. In our in-depth work in this paper considers energy efficiency, reliability, and prolonging the network lifetime in wireless ad hoc networks holistically. They proposed a novel energy-aware routing algorithm, called reliable minimum energy cost routing (RMECR). RMECR finds energy efficient and reliable routes that increase the operational lifetime of the network. In the design of RMECR, they used an in-depth and detailed analytical model of the energy consumption of nodes. RMECR is proposed for networks with hop-by-hop retransmissions providing link layer reliability, and networks with E2E retransmissions providing E2E reliability. Hop By Hop retransmission is supported by the medium access control (MAC) layer to increase reliability of packet transmission over wireless links. Some MAC protocols such as CSMA and MACA may not support Hop-By-Hop retransmissions. In such a case, E2E retransmission could be used to ensure E2E reliability.

2 RELATED WORKS

Q. Yuan, I. Cardei, and J. Wu, in Proc. ACMMobiHoc, 2009, said that Routing is one of the most challenging open problems in disruption tolerant networks (DTNs) because of the short lived wireless connectivity environment. To deal this issue, scholars’ have investigated routing based on the prediction of future contacts, taking advantage of nodes’ mobility history. Most of the previous work focused on the prediction of whether two nodes would have a contact, without considering the time of the contact. This paper presents predict and relay (PER), an efficient routing algorithm for DTNs, where nodes determine the probability distribution of future contact times and choose a proper next hop in order to improve the end-to-end delivery probability. This algorithm is based on two observations: one is that nodes usually move around a set of well-visited landmark points instead of moving randomly; and another one is that node mobility behavior is semi-deterministic and could be predicted once there is sufficient mobility history information. Our method employs a time-homogeneous semi markov process model that describes node mobility as transitions between landmarks. Landmark transition and sojourn time probability distributions are determined from nodes’ mobility history.

PREDICT AND RELAY:

We consider a DTN with a finite number of mobile nodes with unique IDs that move mostly between a set of landmarks. A landmark is defined as a place where nodes can communicate directly, i.e. any two nodes that are located at a landmark at the same time can establish a contact to exchange messages. Nodes at different landmarks cannot establish a contact. Landmarks are also assigned unique IDs.

As described in the introduction, the networks of social nature have nodes follow a semi-deterministic trajectory, with small deviations from a repetitive sequence of land-marks with constant dwell times. For
I

nternational Journal On Engineering Technology and Sciences – IJETS™
ISSN(P): 2349-3968, ISSN (O): 2349-3976

illustration in this article, we use a campus network where the landmarks are independent WLANs installed in classrooms and buildings, while nodes are the students and faculty with PDAs or lap-top. We acknowledge that in the real world the WLANs are actually connected by a backbone. Another good example of this type of DTN is a network in a rural area where the landmarks consist of WLANs located in villages, interconnected by buses that carry messages on portable computers.

ATTACKS ON ROUTING PROTOCOL

Many sensor network routing protocols were very simple and not developed as security in mind, so the attackers can launch various attacks in the network. Mainly network layer protocol suffers from many attacks like; IP spoofing or modifying the route information, selective jamming, sinkhole attack, wormhole attack, Injection attack, etc.

IP Spoofing, Modifying or replaying the route information

An adversary can launch the routing information corruption by IP spoofing, modifying or replaying the routing information. By this an adversary can attracts or redirects the traffic, increases the latency, generate routing loops or creates false data etc.

Selective jamming attack

In the selective jamming attack, compromised node may refuse to forward certain packets and simply drop it. If an adversary drops the entire received packets, it behaves like a black hole attack. An adversary explicitly includes on the path of data flow to perform selective jamming.

Sinkhole and Wormhole attack

Basically, in the both sinkhole and wormhole attacks; the adversary tries to attract all the traffic from a particular area through a compromised node. Sinkhole attack mainly works by making a compromised node look attractive to the neighbor nodes to route the data packet and generally spoof, modify or drop the packet. Sinkhole attack give birth to many attacks like; selective forwarding, black hole, tempering the routing information etc. An adversary launch wormhole with two distant malicious nodes and try to attract the traffic by showing one hop distance to the sink. Wormhole attack is very difficult to detect because it uses out-of-bound channel to route packets.

Sybil attack

In this attack a single node presents multiple identities to the other node in the network. It tries to mislead the node in neighbor detection, route formation and topology maintenance. The Sybil attack is a significant threat to many geographic and multi path routing protocols.

3 OUR WORK

Last, we test the proposed methods over a real-world wireless tracing data. Particularly, we select a data set from the Cambridge Haggle data set. In this data set, connections among 78 mobile iMote Bluetooth nodes carried by researchers and additional 20 stationary nodes are recorded over 4 days during IEEE Infocom 2006. In our simulations, we only consider the 78 mobile nodes and the first half of the period in the tracing data. We divide the time period of the tracing data into 20 time slots. For each time slot t, if there is a contact trace which is overlapping with this slot, we add a spacial link between the two corresponding nodes in Gt. For each round of simulation, we extract a slice of the network which contains 10 mobile nodes. Once again, we check and make sure that the generated space-time graph G is connected over the period of 20 time slots. Costs and reliability probabilities are
randomly generated from 1 to 50 and 0:8 to 1:0 respectively for both spacial and temporal links. Then our topology design algorithms are performed over these 10-node DTNs. In our simulation, 14 rounds of simulations are conducted and average measurements are plotted in Fig. 1. And the reliability requirement $g$ is set to 0:15 and 0:4 for unicast and broadcast cases respectively. The same conclusions can be drawn from these results: (1) all algorithms can reduce the cost remarkably (more than 75 percent) except for GAL; (2) ULCP uses the least cost among all methods but cannot satisfy the reliability requirement; (3) all the other methods can satisfy the reliability requirement; (4) topologies with similar amount of cost or links can achieve higher reliability by using flooding-based methods than single-copy methods.

Fig. 1. Simulation results on networks from Cambridge Haggle tracing data. Results are averages over 14 small networks.

Also for security purpose we are also encrypting the data packets during transmission. So that the intermediate nodes are not able to view the data during transmission. For Encryption process, we are using RC4 Algorithm.

Reliable topology design problem is to build a sparse structure from the original. Space Connecting Time. Static design for the Dynamic topology.

Algorithm Explanation:

**RC4**

- A symmetric key encryption algo. Invented by Ron Rivest.
- Normally uses 64 bit and 128 bit key sizes.
- Most popular implementation is in WEP for 802.11 wireless networks and in SSL.
- Cryptographically very strong yet very easy to implement.
- Consists of 2 parts: Key Scheduling Algorithm (KSA) & Pseudo-Random Generation Algorithm
  - Using a secret key generate the RC4 key stream using the KSA and PRGA.
  - Read the file and xor each byte of the file with the corresponding key stream byte.
  - Write this encrypted output to a file.
  - Transmit file over an insecure channel.

**Results**

We have conducted extensive simulations to evaluate our proposed algorithms devoted to the RTDP problem over random networks, a synthetic space DTN, and pocket switched networks extracted from real tracing data. We implement and test five proposed algorithms, and three existing topology algorithms from, which maintain the connectivity over time but cannot guarantee the reliability. Here, ULCP is the union of least cost paths from $v_i$ to $v_T$ for $i; j \neq 1; \ldots; n$, while GrdLCP and GrdLDB are greedy algorithms which add either the least-cost path or the least-density bunch in each round to connect nodes from $v_0$ to $v_T$ until all pairs are connected. We use them as the references to our proposed methods since they are the only existing topology solutions for time-evolving networks.

**CONCLUSIONS**

We studied reliable topology design problem in a predictable time-evolving DTN with unreliable links modeled by a probabilistic space-time graph. We
first show that it is NP hard, then propose a set of heuristics which can significantly reduce the cost of topology while maintain the connectivity and reliability of paths over time. Simulation results from random networks, a synthetic space DTN, and real-world tracing data demonstrate the efficiency of our methods. We believe that this work presents the first step in exploiting topology design for time-evolving DTNs with unreliable links.

The topology design problem defined in this paper and our proposed algorithms have several limitations and weaknesses. (1) in our problem, the connectivity and reliability are only considered for a fixed time period $T$; (2) we still assume that the predictions of future links and their reliability are feasible, which limit the application of this problem to certain DTNs; (3) here we mainly consider the connectivity and reliability of the constructed topology, however, removing links may hurt the performance of communication protocols (such as routing). Thus it is interesting to conduct a study of the tradeoff between the cost saving for our design and the reduction of network performance.

REFERENCES


