Globus An International Journal of Management & IT
A Refereed Research Journal
Vol 7/ No1 / Jul-Dec 2015 ISSN: 0975-721X

A SURVEY ON EFFICIENT ROUTING PROTOCOLS IN ADHOC NETWORK

*Richa Verma

Introduction

A mobile ad-hoc network (MANET) is a self-configuring infrastructure less network of mobile devices connected by wireless. *Ad hoc* is Latin and means "for this purpose".

Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Such networks may operate by themselves or may be connected to the larger Internet.

MANETs are a kind of wireless ad hoc networks that usually has a routable networking environment on top of a Link Layer ad hoc network.

The growth of laptops and 802.11/Wi-Fi wireless networking have made MANETs a popular research topic since the mid-1990s. Many academic papers evaluate protocols and their abilities, assuming varying degrees of mobility within a bounded space, usually with all nodes within a few hops of each other. Different protocols are then evaluated based on measure such as the packet drop rate, the overhead introduced by the routing protocol, end-to-end packet delays, network throughput etc.

Types of MANET

- Vehicular Ad-hoc Networks (VANETs) are used for communication among vehicles and between vehicles and roadside equipment
- Internet Based Mobile Ad-hoc Networks (iMANET) are ad-hoc networks that link mobile nodes and fixed Internet-gateway nodes. In such type of networks normal adhoc routing algorithms don't apply directly.

Simulation of MANETs

There are several ways to study MANETs. One solution is the use of simulation tools like OPNET, NetSim and NS2.

Data Monitoring and Mining Using MANETs

MANETS can be used for facilitating the collection of sensor data for data mining for a variety of applications such as air pollution monitoring and different types of architectures can be used for such applications. It should be noted that a key characteristic of such applications is that nearby sensor nodes monitoring an environmental feature typically register similar values. This kind of data redundancy due to the spatial correlation between sensor observations inspires the techniques for in-network data aggregation and mining. By measuring the spatial correlation between data sampled by different sensors, a wide class of specialized algorithms can be developed to develop more efficient spatial data mining algorithms as well as more efficient routing strategies. Also researchers have developed performance models for MANET by applying Queueing Theory.

Security of MANETs

A lot of research was done in the past but the most significant contributions were the PGP (Pretty Good Privacy) and the trust based security but none of the protocols made a decent trade off between security and performance. In an attempt to enhance security in MANETs many researchers have suggested and implemented new improvements to the protocols and some of them have suggested new protocols.

Classification of Attacks on MANETs

These attacks on MANETs challenge the mobile infrastructure in which nodes can join and leave easily with dynamics requests without a static path of routing. Schematics of various attacks as described by Al-Shakib Khan on individual layer are as under:

- Application Layer: Malicious code, Repudiation
- Transport Layer: Session hijacking, Flooding
- Network Layer: Sybil, Flooding, Black Hole, Grey Hole. Worm Hole, Link Spoofing, Link Withholding, Location disclosure etc.
- Data Link/MAC: Malicious Behavior, Selfish Behavior, Active, Passive, Internal External
- Physical: Interference, Traffic Jamming, Eavesdropping

*MPhil Student, Swami Vivekanand University, Sagar, MP

DSR Overview

The Dynamic Source Routing Protocol such as these, DSR can take advantage of additional optimizations, such as the ability to reverse a source route to obtain a route back to the origin of the original route.

The IP address used by a node using the DSR protocol MAY be assigned by any mechanism (e.g., static assignment or use of Dynamic Host Configuration Protocol (DHCP) for dynamic assignment [RFC2131]), although the method of such assignment is outside the scope of this specification

Source Routing

The routes that DSR discovers and uses are *source routes.* That is, the sender learns the complete, ordered sequence of network hops necessary to reach the destination, and, at a conceptual level, each packet to be routed carries this list of hops in its header. The key advantage of a source routing design is that intermediate nodes do not need to maintain up-to-date routing information in order to route the packets that they forward, since the packets themselves already contain all the routing decisions.

Route Discovery

Route Discovery works by flooding a request through the network in a controlled manner, seeking a route to some target destination. In its simplest form, a source node A attempting to discover a route to a destination node D broadcasts a ROUTE REQUEST packet that is re-broadcast by intermediate nodes until it reaches D, which then answers by returning a ROUTE REPLY packet to A. Many optimizations to this basic mechanism are used to limit the frequency and spread of Route Discovery attempts..

Route Maintenance

When sending or forwarding a packet to some destination **D**, Route Maintenance is used to detect if the network topology has changed such that the route used by this packet has broken. Each node along the route, when transmitting the packet to the next hop, is responsible for detecting if its link to the next hop has broken. In many wireless MAC protocols, such as IEEE 802.11, the MAC protocol retransmits each packet until a link-layer acknowledgment is received, or until a maximum number of transmission attempts have been made. Alternatively, DSR may make use of a *passive acknowledgment* or may request an explicit network-layer acknowledgment. .

DSR Optimizations

Optimizations to Route Discovery

Nonpropagating ROUTE REQUESTS, when performing Route Discovery, nodes first send a ROUTE REQUEST with the maximum propagation limit (hop limit) set to zero, prohibiting their neighbors from rebroadcasting it. At the cost of a single broadcast packet, this mechanism allows a node to query the route caches of all its neighbors for a route and optimizes the case in which the destination node is adjacent to the source. If the nonpropagating ROUTE REQUEST fails to elicit a reply within a 30 ms time limit, a propagating ROUTE REQUEST with a hop limit set to the maximum value is sent. The 30 ms timeout was chosen based on the distribution of REPLY latencies.

Evaluation Of Protocols For AD HOC Networks

This chapter describes a methodology for evaluating protocols in an ad hoc network environment, concentrating on the simulation system and the metrics I used for analyzing and comparing protocols later in this thesis.

The value of simulation in studies of protocols is that it allows near perfect experimental control: experiments can be designed at will and then rerun while varying an experimental variable and holding all other variables constant. With simulation, it is also possible to test the behavior of networks with more nodes than physical equipment is available for, or networks with equipment that does not even exist yet.

The drawback of simulation is that inherently runs the risk of oversimplification. It is not possible to exactly replicate the entire world inside a computer model, so when creating a simulation some factors must be statistically or otherwise approximated. The failure to properly capture the behavior of first-order factors can lead to dramatically incorrect results.

Extensions to ns-2 Simulator

ns-2 is a discrete event simulator developed by the University of California at Berkeley and the VINT project. Prior to our work on it, it had established itself as a prominent environment for studying TCP and other protocols over networks like the conventional wired Internet. However, it did not provide the support needed for accurately simulating the physical aspects of multi-hop wireless networks or the MAC protocols needed in such environments. Our extensions to *ns-2* as described below have now been adopted by the VINT project as the general support for modeling

ad hoc networks in *ns-2* and included into their mainstream releases.

Evaluation Metrics

In evaluating DSR and the other protocols studied in this thesis, I used several sets of metrics. To characterize the basic performance of the protocols, I used a set of high-level summary metrics that are of interest to network users. To understand the internal functioning of the protocols, I used other sets of metrics: some of which are protocol specific and described as needed in the text, and some of which are general to all on-demand routing protocols and described below.

Summary Metrics

The following three metrics capture the most basic overall performance of DSR and the other protocols studied in this thesis:

Packet delivery ratio: The ratio between the number of packets originated by the "application layer" sources and the number of packets received by the sinks at the final destination.

Conclusion

Mobile Ad hoc Networks are an ideal technology to establish in an instant communication infrastructure less for military application or a flawed architecture has been bought out in this position paper. As we have proved using the three main technical topics of the Wireless Adhoc Networks, We hold the position that the Wireless Ad hoc Networks are a flawed architecture for the following technical reasons:

- The most important thing for the networks is security. It is even important for Wireless Ad hoc Networks because its applications are in military. The MANET can not appropriately solve the problem of the security.
- Routing is also a big problem. All the routing protocols for Wireless Ad hoc Networks are need patches. No suitable and stable routing protocols until now.
- Energy consumption problem still cannot be solved even much of efforts have been done to it. All these prove that the Wireless Ad hoc Networks is a flawed architecture. Not only because it is almost never used in practice but also because there are several technical difficulty that cannot be conquered.

References

1. Imad Aad and Claude Castelluccia. Differentiation Mechanisms for IEEE 802.11. In *Proceedings of IEEE INFOCOM 2001*, pages 209–218, Anchorage, Alaska, April 2001.
2 J.S. Ahn, Peter B. Danzig, Z. Liu, and L. Yan. TCP Vegas: Emulation and Experiment. In *Proceedings of the SIGCOMM '95 Conference: Communications Architectures & Protocols*, pages 185–195, August 1995.
3 M. Allman, V. Paxson, and W. Stevens. TCP Congestion Control. Internet Request For Comments RFC 2581, April 1999.
4 R. Bagrodia, R. Meyer, M. Takai, Y. Chen, X. Zengand J. Martin, and H.Y. Song. PARSEC: A Parallel Simulation Environment for Complex Systems. *IEEE Computer*, 31(10), October 1998.
5. Bikram S. Bakshi, P. Krishna, N. H. Vaidya, and D. K. Pradham. Improving the Performance of TCP over Wireless Neworks. In *Proceedings of the 17th International Conference on Distributed Computing Systems (ICDCS'97)*, pages 365–373, May 1997.
6 H. Balakrishnan, S. Seshan, E. Amir, and R. H. Katz. Improving TCP/IP Performance Over Wireless Networks. In *Proceedings of the First Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom'95)*, pages 2–11, November 1995.
7 R. L. Bargodia and W.-T. Liao. Maise: A Language for the Design of Efficient Discrete-Event Simulation. *IEEE Transactions on Software Engineering*, 20(4), April 1994.