International Journal of Engineering In Advanced Research Science and Technology
ISSN:2278-256

February 2016
VOLUME -1
ISSUE-2
Page:7795-100

ENHANCED RELIABLE DATA DELIVERY IN MOBILE ADHOC NETWORKS USING OPPORTUNISTIC PETAL ROUTING PROTOCOL

[1]. S.Joy Kumar, [2]. Dr.A.Yesu Babu
[1]. Research scholar, Bharathiyar university
[2]. Professor & HOD, Sir.C.R.REDDY COLLEGE of Engineering, Eluru

ABSTRACT: This paper addresses the problem of delivering data packets for highly dynamic mobile ad hoc networks in a reliable and timely manner. Most existing ad hoc routing protocols are susceptible to node mobility, especially for large-scale networks. Driven by this issue, we propose an efficient Position-based Opportunistic Petal Routing (OPR) protocol which takes advantage of the stateless property of geographic routing and the broadcast nature of wireless medium. In the case of communication hole, a Virtual Destination-based Void Handling (VDVH) scheme is further proposed to work together with OPR. Both theoretical analysis and simulation results show that OPR achieves excellent performance even under high node mobility with acceptable overhead and the new void handling scheme also works well.

Index Terms — Geographic routing, opportunistic forwarding, Petal routing, reliable data delivery, void handling, mobile ad hoc network.

I. INTRODUCTION

MOBILE ad hoc networks (MANETs) have gained a great deal of attention because of its significant advantages brought about by multihop, infrastructure-less transmission. However, due to the error prone wireless channel and the dynamic network topology, reliable data delivery in MANETs, especially in challenged environments with high mobility remains an issue. Traditional topology-based MANET routing protocols (e.g., DSDV, AODV, DSR [1]) are quite susceptible to node mobility. One of the main reasons is due to the predetermination of an end-to-end route before data transmission. Owing to the constantly and even fast changing network topology, it is very difficult to

maintain a deterministic route. The discovery and recovery procedures are also time and energy consuming. Once the path breaks, data packets will get lost or be delayed for a long time until the reconstruction of the route, causing transmission interruption.

Geographic routing (GR) [2] uses location information to forward data packets, in a hop-by-hop routing fashion. Directional flooding is used to select next hop forwarder with the minimum duplication and positive progress toward the destination while void handling mechanism is triggered to route around communication voids [3] by increasing the width‟w‟ of the petal. No end-to-end routes need to be maintained, leading to GR‟s high efficiency and scalability. However, GR is very sensitive to the inaccuracy of location information [4]. In the operation of greedy forwarding, the neighbor which is relatively far away from the sender is chosen as the next hop. If the node moves out of the sender‟s coverage area, the transmission will fail. In GPSR [5] (a very famous geographic routing protocol), the MAC-layer failure feedback is used to offer the packet another chance to reroute. In fact, due to the broadcast nature of the wireless medium, a single packet transmission will lead to multiple reception. If such transmission is used as backup, the robustness of the routing protocol can be significantly enhanced. However, most of them use link-statestyle topology database to select and prioritize the forwarding candidates. In order to acquire the internode loss rates, periodic network-wide measurement is required, which is impractical for mobile environment. Recently, location-aided opportunistic routing has been proposed which directly uses location information to guide packet forwarding.

II RELATED WORK:-

Before developing the tool it is necessary to determine the time factor, economy n company strength. Once these things r satisfied, ten next steps is to determine which operating system and language

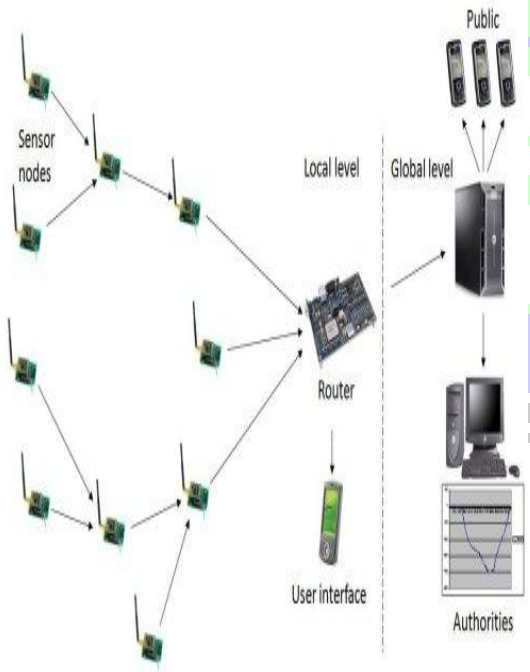
March 2016
VOLUME -2
ISSUE-3
Page:7795-100

can be used for developing the tool. Once the programmers start building the tool the programmers need lot of external support. This support can be obtained from senior programmers, from book or from websites. Before building the system the above consideration r taken into account for developing the proposed system.

Networking:

In the world of computers, networking is the practice of linking two or more computing devices together for the purpose of sharing data. Networks are built with a mix of computer hardware and computer software.Networks consist of the computers, wiring, and other devices, such as hubs, switches and routers that make up the network infrastructure. Some devices, such as network interface cards, serve as the computer's connection to the network. Devices such as switches and routers provide traffic- control strategies for the network. All sorts of different technologies can actually be employed to move data from one place to another, including wires, radio waves, and even microwave technology.

Network architecture:



Asynchronous Transfer Mode:

Asynchronous Transfer Mode (ATM) is a switching technique for telecommunication networks. It uses asynchronous time-division multiplexing and encodes data into small, fixed-sized cells. This differs from other protocols such as the Internet Protocol Suite or Ethernet that use variable sized packets or frames. ATM has similarity with both circuit and packet switched networking. This makes it a good choice for a network that must handle both traditional high-throughput data traffic, and real-time, low-latency content such as voice and video. ATM uses a connection-oriented model in which a virtual circuit must be established between two endpoints before the actual data exchange begins.

Network topology

Common layouts

A network topology is the layout of the interconnections of the nodes of a computer network. Common layouts are:

- A bus network: all nodes are connected to a common medium along this medium. This was the layout used in the original Ethernet, called 10BASE5 and 10BASE2.
- A star network: all nodes are connected to a special central node. This is the typical layout found in in a Wireless LAN, where each wireless client connects to the central Wireless access point.
- A ring network: each node is connected to its left and right neighbor node, such that all nodes are connected and that each node can reach each other node by traversing nodes left- or rightwards. The Fiber Distributed Data Interface (FDDI) made use of such a topology.
- A mesh network: each node is connected to an arbitrary number of neighbors in such a way that there is at least one traversal from any node to any other.
- A fully connected network: each node is connected to every other node in the network.

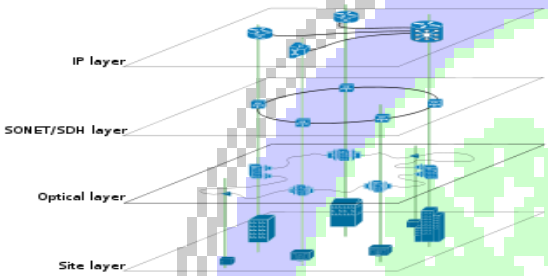
Note that the physical layout of the nodes in a network may not necessarily reflect the network topology. As an example, with FDDI, the network topology is a ring (actually two counter-rotating

March 2016
VOLUME -2
ISSUE-3
Page:7795-100

rings), but the physical topology is a star, because all neighboring connections are routed via a central physical location.

Overlay network

An overlay network is a virtual computer network that is built on top of another network. Nodes in the overlay are connected by virtual or logical links, each of which corresponds to a path, perhaps through many physical links, in the underlying network. The topology of the overlay network may (and often does) differ from that of the underlying one.



For example, many peer-to-peer networks are overlay networks because they are organized as nodes of a virtual system of links run on top of the Internet. The Internet was initially built as an overlay on the telephone network .[14]

The most striking example of an overlay network, however, is the Internet itself: At the IP layer, each node can reach any other by a direct connection to the desired IP address, thereby creating a fully connected network; the underlying network, however, is composed of a mesh-like interconnect of subnetworks of varying topologies (and, in fact, technologies). Address resolution and routing are the means which allows the mapping of the fully-connected IP overlay network to the underlying ones.

Overlay networks have been around since the invention of networking when computer systems were connected over telephone lines using modems, before any data network existed.

Another example of an overlay network is a distributed hash table, which maps keys to nodes in the network. In this case, the underlying network is an IP network, and the overlay network is a table (actually map) indexed by keys.

Overlay networks have also been proposed as a way to improve Internet routing, such as through quality of service guarantees to achieve higher-quality streaming media. Previous proposals such as IntServ, DiffServ, and IP Multicast have not seen wide acceptance largely because they require modification of all routers in the network. On the other hand, an overlay network can be incrementally deployed on end-hosts running the overlay protocol software, without cooperation from Internet service providers. The overlay has no control over how packets are routed in the underlying network between two overlay nodes, but it can control, for example, the sequence of overlay nodes a message traverses before reaching its destination.

Routers

A router is an internetworking device that forwards packets between networks by processing information found in the datagram or packet (Internet protocol information from Layer 3 of the OSI Model). In many situations, this information is processed in conjunction with the routing table (also known as forwarding table). Routers use routing tables to determine what interface to forward packets (this can include the "null" also known as the "black hole" interface because data can go into it, however, no further processing is done for said data).

Network security

In the field of networking, the area of **network security**[20] consists of the provisions and policies adopted by the network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of the computer network and network-accessible resources. Network Security is the authorization of access to data in a network, which is controlled by the network administrator. Users are assigned an ID and password that allows them access to information and programs within their authority. Network Security covers a variety of computer networks, both public and private that are used in everyday jobs conducting transactions and communications among businesses, government agencies and individuals. Networks can be private, such as within a company, and others which might be open to public access. Network Security is involved in organization, enterprises, and all other type of institutions. It does as its titles explains, secures the

network. Protects and oversees operations being done.

III FEATURE WORK:-

Castelluccia et al [13] proposed a simple and provably secure encryption allowing encrypted data to be efficiently and additively aggregated. Only a modular addition is needed for cipher-text aggregation. Scheme security is based on the in distinguish ability property of a pseudorandom function (PRF), a standard cryptographic primitive. It was proved that aggregation based on this can efficiently compute statistical values, like mean, variance, and sensed data's standard deviation, while achieving great bandwidth savings. To protect aggregated data's integrity, an end-to-end aggregate authentication scheme was constructed which was secure against outsider-only attacks.

IV CONCLUSION:-

In this article, we have introduced physical layer cooperative communications, topology control, and network capacity in MANETs. To improve the network capacity of MANETs with cooperative communications, we have proposed a Capacity-Optimized Cooperative (COCO) topology control scheme that considers both upper layer network capacity and physical layer relay selection in cooperative communications. Simulation results have shown that physical layer cooperative communications techniques have significant impacts on the network capacity, and the proposed topology control scheme can substantially improve the network capacity in MANETs with cooperative communications. Future work is in progress to consider dynamic traffic patterns in the proposed scheme to further improve the performance of MANETs with cooperative communications.

V BIBLIOGRAPHY:-

References Made From:

1. J. Laneman, D. Tse, and G. Wornell, "Cooperative Diversity in Wireless Networks: Efficient protocols and Outage Behavior," *IEEE Trans. Info. Theory*, vol. 50, no. 12, 2004, pp. 3062–80.
2. P. H. J. Chong *et al.*, "Technologies in Multihop Cellular Network," *IEEE Commun. Mag.*, vol. 45, Sept. 2007, pp. 64–65.
3. K. Woradit *et al.*, "Outage Behavior of Selective relaying Schemes," *IEEE Trans. Wireless Commun.*, vol. 8, no. 8, 2009, pp. 3890–95.
4. Y. Wei, F. R. Yu, and M. Song, "Distributed Optimal Relay Selection in Wireless Cooperative Networks with Finite-State Markov Channels," *IEEE Trans. Vehic. Tech.*, vol. 59, June 2010, pp. 2149–58.
5. Q. Guan *et al.*, "Capacity-Optimized Topology Control for MANETs with Cooperative Communications," *IEEETrans. Wireless Commun.*, vol. 10, July 2011, pp. 2162–70.
6. P. Santi, "Topology Control in Wireless Ad Hoc and sensor Networks," *ACM Computing Surveys*, vol. 37, no. 2, 2005, pp. 164–94.

Sites Referred:

http://www.sourcefordgde.com
http://www.networkcomputing.com/