ijiarec.com

ISSN: 2348-2079

FEB-2015

International Journal of Intellectual Advancements and Research in Engineering Computations

GEOGRAPHIC ROUTING FOR MOBILE LOCATION UPDATE USING MANET

N.VAITHEEKA[1], R.INDUPOORNIMA[2], C.B.SIVAPARTHIPAN[3], M.BALAANAND[4]

ABSTRACT

In geographic routing, nodes need to maintain up-to-date positions of their immediate neighbors for making effective forwarding decisions. Periodic broadcasting of beacon packets is a popular method used by most geographic routing protocols to maintain neighbor positions. But it will increase the update cost and reduce the performance of the router. To eliminate this problem we propose this Mobile Location Update (MLU),MLU works on two principles ,1.Nodes whose movements are harder to predict, update their positions more frequently (and vice versa).2.Nodes which are static and closer to the forwarded path, update their positions more frequently (and vice versa).

Keywords: Mobile Location Update, Personal Digital Assistants

INTRODUCTION

Mobile Ad-hoc Networking (MANET) is receiving growing attention as a means of providing communications in environments where there is no existing infrastructure. First responders at a disaster site or soldiers in a battlefield must provide their own communications. A MANET is a possible solution for this need to quickly establish communications in a mobile and transient environment. A MANET has several security vulnerabilities. This proposal will study these vulnerabilities and investigate possible solutions. Closing these security vulnerabilities will influence the acceptability of a MANET for critical applications. A secure MANET system, called SMANET, will be created. SMANET will secure routing updates, enhance intrusion detection and respond to intrusion with an enhanced group key distribution scheme.

The Internet Engineering Task Force has defined a Mobile Ad hoc Network (MANET) as:“An autonomous system of mobile routers (and associated hosts) connected by wireless links--the union of which form an arbitrary graph. The routers are free to move randomly and organize themselves arbitrarily; thus, the network's wireless topology may change rapidly and unpredictably. Such a network may operate in a standalone fashion, or may be connected to the larger

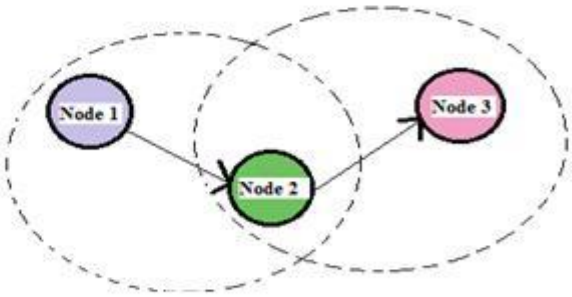


Figure 1.1 Example of MANET

Author for Correspondance:
[1]Assistant Professor/Department Of It, Karpgam College Of Engineering, Coimbatore,India, Vaitheeka.p@gmail.com
[2]Assistant Professor/Department Of CSE, SNS College Of Technoogy, Coimbatore,India, indupoornima@kce.ac.in
[3]Assistant Professor/Department of CSE, V.R.S. College of Engineering & Technology,Villupuram,India, sivaparthipanece@gmail.com
[4]Assistant Professor/Department Of IT, Karpgam College Of Engineering, Coimbatore,India, balavdy@gmail.com

Internet". The Mobile Ad hoc network is a collection of wireless mobile hosts forming a temporary network without the aid of any established infrastructure or centralized administration.. Under these circumstances, routing is much more complex than in conventional (static) networks. Many of the possible solutions are determined by the characteristics of the media, the behavior of nodes and the data flow. For a successful deployment, this is an important problem, since a wrong choice may have a severe impact on the performance, and consequently on the acceptance of the new technology. Also, providing just any protocol is not feasible, due to the different requirements on hardware and lower network layers.

INTRODUCTION TO MANET

A Mobile Ad-hoc Network is a set of mobile devices (nodes), which shared over a wireless medium, communicate with each other without the presence of predefined infrastructure or a central authority. The member nodes are themselves responsible for the creation operation and maintenance of the network. Each node in the MANET is equipped with a wireless transmitter and receiver, with aid of which its communicate with the other nodes in its wireless vicinity. The node which are not in wireless vicinity, communicate with each other hop by hop following a set of rules (routing protocol) for the hopping sequence to be followed.

Figure 1.1 shows a simple ad-hoc network with 3 nodes. Node 1 and node 3 are not within range of each other, however the node 2 can be used to forward packets between node 1 and node 2. The node 2 will act as a router and these three nodes together form an ad-hoc network.

ROUTING ATTACKS IN MANET

All of the Routing protocols in MANETs depend on active cooperation of nodes to provide routing between the nodes and to establish and operate the network. The basic assumption in such a setup is that all nodes are well behaving and trustworthy. Albeit in an event where one or more of the nodes turn malicious, security attacks can be launched which may disrupt routing operations or create a DOS (Denial Of Service) condition in the network. Due to dynamic, distributed infrastructure less nature of MANETs, and lack of centralized authority, the ad-hoc networks are vulnerable to various kinds of attacks.

The challenges to be faced by MANETs are over and above to those to be faced by the traditional wireless networks. The accessibility of the wireless channel to both the genuine user and attacker make the MANET susceptible to both passive eavesdroppers as well as active malicious attackers. The limited power back up and limited computational capability of the individual nodes hinders the implementation of complex security algorithms and key exchange mechanism. There is always a possibility of a genuine trusted node to be compromised by the attackers and subsequently used to launch attacks on the network.

Node mobility makes the network topology dynamic forcing frequent networking reconfiguration which creates more chance for attacks. The attacks on MANETs can be categorized as active or passive. In passive attacker does not send any message, but just listens to the channel. Passive attack are non-disruptive but is information seeking, which may be critical in the operation of protocol. Active attacks may either be directed to disrupt the normal operation of a specific node or target the operation of the whole network.

A passive attacker listens to the channel and packets containing secret information (e.g., IP address, location of nodes, etc.) may be stolen, which violates confidentiality paradigm. In a wireless environment it is normally impossible to detect this attack ,as it does not produce any new traffic in the network. The action of an active attacker includes ,injecting packets to invalid destinations into the network, deleting packets, modifying the contents of packets, and non repudiation paradigm. Contrary to the passive attacks, active attacks can be detected and eventually avoided by the legitimate nodes that participate in an ad hoc network.

LOCATION UPDATES IN MANET

In situation where nodes are mobile or when nodes often switch off and on, the local topology rarely remain static. Hence, it is necessary that node broadcasts its updated location information to all of its neighbors . These Location update packet are usually referred to as beacons. In most geographic routing protocols (e.g., GPSR),because are broadcast periodically for maintaining an accurate neighbor for a certain time interval, called neighbor time-out interval, the node consider this neighbor has moved out of the radio range and removes the outdated neighbor from its neighbor list. The neighbor time-out interval often is multiple times of the beacon interval.

Position is costly in many ways. Each update consumes node energy, wireless bandwidth, and increases the risk of packet collision at the medium access control (MAC) layer. Packet collisions cause packet loss which in turn affects the routing performance due to decreased accuracy in determining the correct local topology (a lost beacon broadcast is not retransmitted). A lost data packet does get retransmitted, but at the expense of increased end-to-end delay. Clearly, given the cost associated with transmitting beacons, it makes sense to adapt the frequency of beacon updates to the node mobility and the traffic condition within the network, rather than employing a static periodic update policy.

For example, if certain nodes are frequently changing the mobility characteristics (speed and/or heading), it makes sense to frequently changing their updated position. However, for nodes that do not exhibit significant dynamism, periodic broadcasting of beacons is wasteful. Further, if only a small percentage of the nodes are involved in forwarding packets, it is unnecessary for nodes which are located far away from the forwarding path to employ periodic beaconing because these updates are not useful for forwarding the current traffic. To overcome the drawbacks of periodic beacons the adaptive strategy is proposed in beacon transmission.

GEOGRAPHIC ROUTING

Geographic Routing (or position-based routing) uses location information for packet delivery in multi hop wireless networks. Neighbors locally exchange location determination techniques. Since node locally select next hop nodes based on this neighborhood information and the neither destination location, neither route established nor per-destination state is required in geographic routing. As large-scale sensor networks become more geographic routing increasingly more attractive. Also, location based services such as geo-casting can be best realized using geographic routing.

The most popular strategy for geographic routing is simply forwarding data packets to the neighbor geographically closest to the destination. Although this greedy method is effective in many cases, packet may get routed to where no neighbor is closer to the destination than the current node. Many recovery schemes have been proposed to route around such voids for guaranteed packet delivery as long as a path exists. These techniques typically exploit planar sub-graphs (i.e., Gabriel graph, Relative Neighborhood graph), and packets traverse faces on such graphs using the well-known right-hand rule. Most geographic routing protocols use one-hop information, but generalization to two-hop neighborhood is also possible.

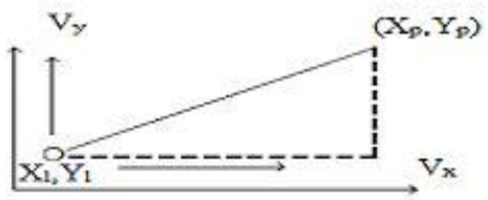


Figure 4.1 An Example of Mobility Predic 1

PROBLEM DEFINITION

In geographic routing protocol becomes the attractive choice for the mobile ad-hoc networks for that purpose many position system are involved. Position based routing protocol are mainly used in many networks due to dynamic change in the network topology and it is highly suitable for this present networks. But some of the protocol like Greedy Perimeter Stateless Routing Protocol and DSR protocol are also used. By using the GPS the nodes will create a local topology. However when nodes are switch off or on the local topology will not dynamic it will be a static. So it is necessary for each and every node in that network must send beacon packets to their neighboring nodes. Those beacon packets contain the nodes present location. In the geographic location nodes needs to send the beacon packet at equal interval of time for the accurate location of the nodes. But in this process it leads to consume more energy, increases in the wireless band width, and increase in the packet collision and this will lead to retransmit that packet again. The retransmitting the packet leads to decrease the routing performance. The lost packets are also not retransmitted. This will lead to increase in the update cost but we cannot use the static topology because of the inaccurate location in the nodes.

3 MODULES

The modules in Mobile Location Update Strategy are:

- System Model Module
- Mobility Prediction Module

- Mobile Location Update Module

System Model Module

In this module we have shown the creation of nodes which have been placed in different locations. And also have shown the movement of nodes with constant speed in a particular time interval.

3.2 Mobility Prediction Module

This module predicts the mobility of the nodes which are in the communication range. When the nodes are in moving state, the X-axis, Y-axis values, the distance between the two nodes, the velocity of the nodes are finding by this module. The previous position of the node and current position of the node are also calculated.

Mobile Location Update Module

In this module, the common positions are updated. While moving the nodes are in communication range, the common properties like location, velocity and node information are updated. These common information are updated frequently and maintained in a table. After find the one-hop neighbor, the packet has been forwarded by using the routing protocol GPSR (Greedy Perimeter Stateless Routing).

CONCEPT OF THE PROPOSED WORK

Mobility Prediction (MP) Rule

This rule adapts the beacon generation rate to the frequency with which the nodes change the characteristics that govern their motion (velocity and heading). The motion characteristics are included in the beacons broadcast to a node's neighbors. Nodes that frequently change their motion need to frequently update their neighbors, since their locations are changing dynamically. The goal of the MP rule is to send the next beacon update from node i when the error between the predicted location in the neighbors of i and node i's actual location is greater than an acceptable threshold. A simple location prediction scheme is used based on the physics of motion to estimate a node's current location. The nodes are assumed to be located in a two-dimensional coordinate system with the location ind1icated by the x and y coordinates. However, this scheme can be easily extended to a three dimensional coordinate system.

As shown in Figure 4.1, given the position of node i and its velocity along the x and y axes at time Tl, its neighbors can estimate the current position of i, by using the following equations:

$$Xpi = Xil + (Tc - Tl) * Vxi \quad (1)$$

$$Ypi = Yil + (Tc - Tl) * Vyi \quad (2)$$

Note that, here (Xil,Yil) and (Vix, Viy) refers to the location and velocity information that was broadcast in the previous beacon from node i. Node i uses the same prediction scheme to keep track of its predicted location among its neighbors.

Let (Xa, Ya), denote the actual location of node i, obtained via GPS or other localization techniques. Node i then computes the deviation Didevi as follows:

$$Di\ devi^2 = (Xai-Xpi)^2 + (Yai-Ypi)^2$$

Table 4.1 Notations for Mobility Prediction

VARIABLES	DEFINITION
(Xli,Yli)	The coordinate of node i at time Ti (included in the previous beacon)
(Vxi,Vyi)	The velocity of node I along the direction of the x and y axes at time Ti(included in the previous beacon)
Tl	The time of the last beacon broadcast
Tc	The current time
(Xpi,Ypi)	The predicted position of node I at the current time

If the deviation is greater than a certain threshold, known as the Acceptable Error Range (AER), it acts as a trigger for node i to broadcast its current location and velocity as a new beacon. The MP rule, thus, tries to maximize the effective duration of each beacon, by broadcasting a beacon only when the predicted position information based on the previous beacon becomes inaccurate.

This extends the effective duration of the beacon for nodes with low mobility, thus reducing the number of beacons. Further, highly mobile nodes can broadcast frequent beacons to ensure that their neighbors are aware of the rapidly changing topology.

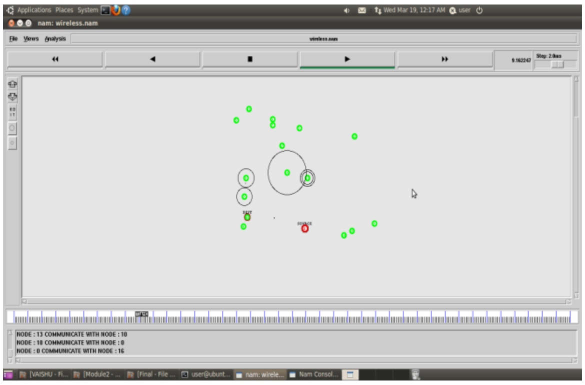
RDM (Random Direction Mobility) Model

This mobility model maintains a uniform distribution of nodes in the target region over the entire time interval under consideration. According to this model, a node's trajectory consists of multiple consecutive linear segments. In each segment, the node randomly selects a direction, a speed, and travel duration from certain predefined ranges. The node moves at the selected speed in the chosen direction until the selected travel duration expires. At the end of the segment, the node pauses for a random time interval and then randomly selects another set of values for the next segment and changes its motion accordingly.

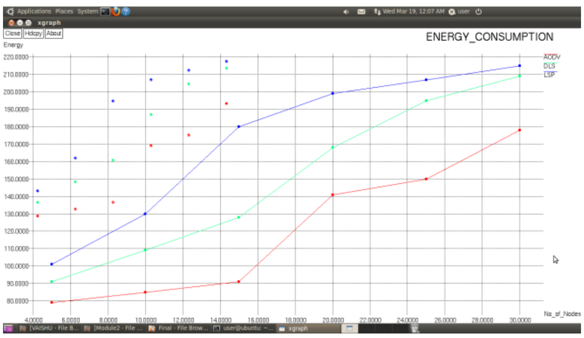
Greedy Perimeter Stateless Routing

The GPSR is a responsive and efficient protocol for mobile, wireless networks. GPSR can be applied to Sensor networks, Rooftop networks, Vehicular networks and ad-hoc networks. Assuming the wireless routers [nodes] know their own locations the Greedy forwarding algorithm will try to find the closest router which is also the closest to the final destination. If the network is dense enough that each interior node has a neighbor in every 2Π/3 angular sector, Greedy Forwarding will always succeed. However, the greedy forwarding algorithm can fail. When the Greedy Forwarding algorithm fails, the Perimeter Forwarding algorithm will be used. Apply the right-hand rule to traverse the edges of the void and find a path using the topology's perimeter. The Perimeter Forwarding Algorithm uses a longer path to the destination so the perimeter forwarding algorithm less efficient and cannot be used alone. Putting Greedy Forwarding and Perimeter Forwarding together makes the final GPSR which will use the necessary algorithm to find the best path in a given topology.

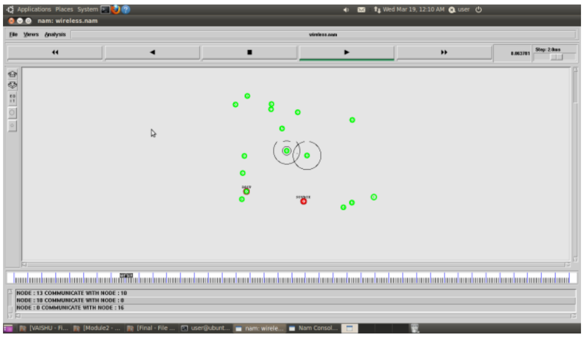
Mobility Prediction



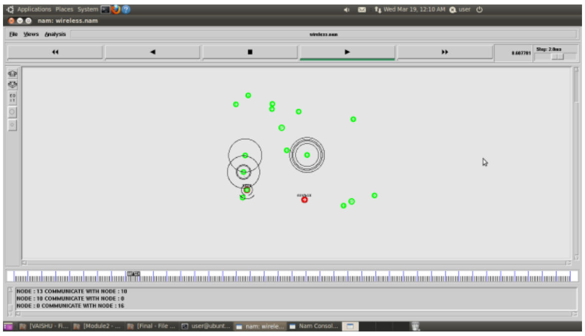
Transmission of Packets



Packet Dropping



Graph for Energy Consumption



CONCLUSION

In this paper we analysis the need of Location update of each node in the geographic routing protocol. So we propose this Mobile Location Update. In this Mobile Location Update it works on Mobility Prediction rule. This rule is to improve the accuracy of the node location. We embedded the Mobile Location Update with the GPSR and compared with the other beacon system by using the NS-2 Simulator. Our result indicates that we are using fewer beacons overhead and improve in the Energy Consumption, Packet Delivery Ratio and Average Delay. And alternate path when there is an occurrence of path failure is also found.

FUTURE ENHANCEMENTS

Future work includes utilizing the analytical model to find the optimal protocol parameters (e.g. the optimal radio range), studying how the proposed scheme can be used to achieve load balance and evaluating the performance of the proposed scheme on TCP connections in Mobile Ad-hoc Networks

REFERENCES

[1] Bettstetter, C. (2005) "Connectivity of wireless multihop networks in a shadow fading environment", in Wireless Network, vol. 11, no. 5, pp. 571-579.

[2] Blazevic, L. Giordano, L. and LeBoudec, J. (2004) "A Location Based Routing Method for Mobile Ad Hoc Networks", in IEEE Transaction on Mobile Computing, Vol. 3 No. 4.

[3] Chen, Q. Kanhere, S.S. and Hassan, M. (2010) "Mobility and Traffic Adaptive Position Update for Geographic Routing". CSE, UNSW, Sydney, Australia. UNSW-CSE-TR-1002.

[4] Chen, Q. Kanhere, S.S. Hassan, M. and Lan, L.C. (2006) "Adaptive Position Update in Geographic Routing", Proceedings of the International Conference on Communications (ICC 2006), pp. 4046-4051.

[5] Feeney, L.M and Nilsson, M. (2001) "Investigating the energy consumption of a wireless network interface in an ad hoc networking environment". in Proceedings of IEEE Infocom, pp. 1548-1557.

[6] Heissenbuttel, M. Braun, T. Bernoulli, T. et al (2004) "BLR: Beacon-Less Routing Algorithm for Mobile Ad-Hoc Networks", in Computer Communications, vol,27, pp. 1076-1086.