ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 2, February 2014

An Efficient Call Control and Secure Mechanism for Routing Protocol

A.KEERTHIKA[1], A.SANTHIYA[2]

PG Student (M. TECH.,), Department of Computer Science and Engineering,

Manakula Vinayagar Institute of Technology, Pondicherry, India[1]

UG Student (B. TECH.,), Department Of Electronics and Communication Engineering,

Christ College of Engineering and Technology, Pondicherry, India[2]

Abstract: An efficient call control is a tedious task because of network traffic and intruders. In an Ad Hoc wireless network end to end communication for a long time results packet loss will occurs. In an existing mechanism invokes periodic beacon update scheme which consumes the network resources such as energy and bandwidth specifically when the network traffic is high it creates packet loss in the network leads to retransmission of data packet causing additional delay and energy consumption. The novel scheme of Adaptive Position Update (APU) including two rules named Mobility Prediction Rule (MP) and On demand Route Learning Rule (ODL). According to this scheme call control is inefficient because the load has not been balanced and the network security is low. To address these limitations, in this paper proposes Endpoint Admission Control (EAC) mechanism for efficient call control and also provide the security mechanism to prevent the call from the intruders. We present four new mechanisms as tools for securing distance vector and path vector routing protocols. For securing distance vector protocols, to provide authentication of a received routing update in bounded time. For securing path vector protocols, our cumulative authentication mechanism authenticates the list of routers on the path in a routing update, preventing removal or reordering of the router addresses in the list; the mechanism uses only a single authenticator in the routing update rather than one per router address. These mechanisms can be used as building blocks for securing routing protocols.

Keywords: Ad Hoc wireless network, Adaptive Position Update, Endpoint Admission Control, Security Mechanism for routing protocol.

I. INTRODUCTION

With the growing popularity of positioning devices (e.g., GPS) and other localization schemes [1], geographic routing protocols are becoming an attractive choice for use in mobile ad hoc networks [2], [3], [4]. The underlying principle used in these protocols involves selecting the next routing hop from among a node's neighbors, which is geographically closest to the destination. Since the forwarding decision is based entirely on local knowledge, it obviates the need to create and maintain routes for each destination. By virtue of these characteristics, position-based routing protocols are highly scalable and particularly robust to frequent changes in the network topology. The forwarding strategy employed in the aforementioned geographic routing protocols requires the following information: 1) the position of the final destination of the packet and 2) the position of a node's neighbors. Position updates are 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 conditions within the network, rather than employing a static periodic update policy. Adaptive Position Update scheme eliminates the drawbacks of periodic beaconing by adapting to the system variations. APU incorporates two rules for triggering the beacon update process. The first rule, referred as Mobility Prediction (MP), uses a simple mobility prediction scheme to estimate when the location information broadcast in the previous beacon becomes inaccurate. The next beacon is broadcast only if the predicted error in the location estimate is greater than a certain threshold, thus tuning the update frequency to the dynamism inherent in the node's motion. The second rule, referred as On-Demand Learning (ODL), aims at improving the accuracy of the topology along the routing paths between the communicating nodes. ODL uses an on-demand learning strategy, whereby a node broadcasts beacons when it overhears the transmission of a data packet from a new neighbor in its vicinity. This ensures that nodes involved in forwarding data packets maintain a more update view of the local topology. On the contrary, nodes that are not in the vicinity of the forwarding path are unaffected by this rule and do not broadcast beacons very frequently. In this paper we proposes Endpoint Admission Control (EAC) mechanism mainly used to balanced the load over the traffic in the network, by means of probing, marking and terminating the call. As our economy and critical infrastructure increasingly rely on the Internet, securing routing protocols becomes of critical importance. So that we present four new mechanisms as tools for securing distance vector and path vector routing protocols. For securing distance vector protocols, our hash tree chain mechanism forces a router to increase the distance (metric)

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 2, February 2014

when forwarding a routing table entry. To provide authentication of a received routing update in bounded time, we present a new mechanism, similar to hash chains, that we call tree-authenticated one-way chains. For cases in which the maximum metric is large, we present skip chains, which provides more efficient initial computation cost and more efficient element verification; this mechanism is based on a new cryptographic mechanism, called MW-chains, which we also present. For securing path vector protocols, our cumulative authentication mechanism authenticates the list of routers on the path in a routing update, preventing removal or reordering of the router addresses in the list; the mechanism uses only a single authenticator in the routing update rather than one per router address. We also present a simple mechanism to securely switch one-way chains, by authenticating the next one-way chain using the previous one. These mechanisms are all based on efficient symmetric cryptographic techniques and can be used as building blocks for securing routing protocols.

II. RELATED WORK

In this paper to reduce the retransmission of voice and data in the wireless Ad Hoc network and also maintains security of transferring the data from one end to another. In geographic routing (also known as position-based routing or geometric routing) is a technique to deliver a message to a node in a network over multiple hops by means of position information. Routing decisions are not based on network addresses and routing tables; instead, messages are routed towards a destination location. With knowledge of the neighbours' location, each node can select the next hop neighbour that is closer to the destination, and thus advance towards the destination in each step. Position updates are costly in many ways. Each up-date consumes node energy, wireless bandwidth, and increases the risk of packet collision at the medium ac-cess 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 conditions within the network, rather than employing static periodic update policy. When one more call is placed on the wireless network than can be supported, all calls start to suffer unacceptable call quality [2]. For this reason and taking into account the small number of VoIP connections possible, Call Admission Control (CAC) is a critical requirement so that a call which cannot be supported by the wireless network will not be admitted.

An approach to Admission Control (AC) that has emerged in recent years is Endpoint Admission Control (EAC), with all AC decisions taken by the endpoint devices. EAC usually consists of probing the end-to-end path, with probes resembling the traffic profile of the flow to be admitted.

The QOS of the probe flow is measured in terms of delay, loss, and jitter and some combination of these can be used to determine if the flow can be admitted [3]. Common thresholds for a voice connection include a maximum 150ms one-way end-to-end delay or 1% packet loss bound to provide high quality voice [4]. An EAC scheme is proposed in this paper that adapts this paradigm specifically to the characteristics of the VoIP system, and does not require modifications to network components such as APs and routers. All that is required is wireless VoIP handsets that implement the proposed Call Admission Control (CAC) scheme.

Symmetric cryptographic primitives are much more efficient than asymmetric primitives, but so far, few security mechanisms based on symmetric cryptography have been designed for the requirements of routing protocols. We now discuss the exceptions of which we are aware. Three mechanisms based on symmetric cryptography have been proposed to secure link state routing updates. Cheung [2] presents an efficient time-based authentication protocol to authenticate link state routing updates. The proposed authentication is optimistic, though, and routers use the routing update before it is authenticated. Our new mechanisms for building efficient and secure path vector routing protocols.

III. ANALYSIS

Mobile users now a day's receiving more than one call at a time frequently. So that we find out the position of the end user and check the network traffic because of packet loss. If the channel is free to establish the call otherwise use the EAC scheme to balance the load over the channel and establish the call connection.

EXISTING SYSTEM

Existing mechanisms invokes periodic beacon update scheme which consumes the network resources such as energy and bandwidth specifically when the network traffic is high it creates packet loss in the network leads to retransmission of data packet causing additional delay and energy consumption. The novel scheme of Adaptive Position Update (APU) including two rules named Mobility Prediction Rule (MP) and On demand Route Learning Rule (ODL).

ADAPTIVE POSITION UPDATE

We begin by listing the assumptions made in our work:

- All nodes are aware of their own position and velocity.
- All links are bidirectional.
- The beacon updates include the current location and velocity of the nodes.
- Data packets can piggyback position and velocity.

Updates and all one-hop neighbours operate in the promiscuous mode and hence can overhear the data packets. Upon initialization, each node broadcasts a beacon informing its neighbours about its presence and its current location and velocity. Following this, in most geographic routing protocols such as GPSR, each node periodically broadcasts its current location information.

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 2, February 2014

The position information received from neighbouring beacons is stored at each node. The APU strategy proposed in this project dynamically adjusts the beacon update intervals based on the mobility dynamics of the nodes and the forwarding patterns in the network. APU employs two schemes based on the mobility dynamics of the nodes and the forwarding patterns in the network.

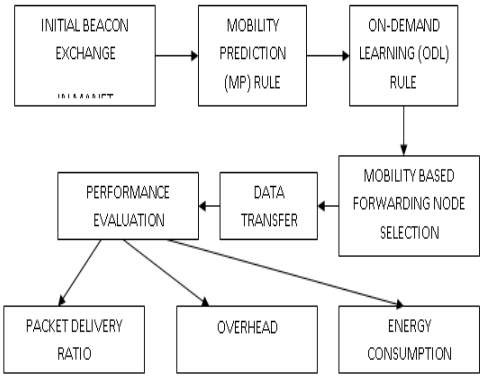

Fig 1. Block diagram for APU

A. MOBILITY PREDICTION 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 neighbours. The neighbours can then track the node's motion using simple linear motion equations. Nodes that frequently change their motion need to frequently update their neighbours, since their locations are changing dynamically. The beacons transmitted by the nodes contain their current position and speed. Nodes estimate their positions periodically by employing linear kinematic equations based on the parameters announced in the last announced beacon. If the predicted location is different from the actual location, a new beacon is broadcast to inform the neighbours about changes in the node's mobility characteristics.

On the contrary, nodes which move slowly do not need to send frequent updates. A periodic beacon update policy cannot satisfy both these requirements simultaneously, since a small update interval will be wasteful for slow nodes, whereas a larger update interval will lead to inaccurate position information for the highly mobile nodes.

B. ON-DEMAND LEARNING RULE

The MP rule solely may not be sufficient for maintaining an accurate local topology. It is necessary to devise a mechanism, which will maintain a more accurate local topology in those regions of the network where significant data forwarding activities are on-going. This is precisely what the On-Demand Learning rule aims to achieve. As the name suggests, a node broadcasts beacons on-demand, i.e., in response to data forwarding activities that occur in the vicinity of that node. According to this rule, whenever a node overhears a data transmission from a new neighbor, it broadcasts a beacon as a response. By a new neighbor, we imply a neighbor who is not contained in the neighbor list of this node. In reality, a node waits for a small random time interval before responding with the beacon to prevent collisions with other beacons.

Recall that, we have assumed that the location updates are piggybacked on the data packets and that all nodes operate in the promiscuous mode, which allows them to overhear all data packets transmitted in their vicinity. In addition, since the data packet contains the location of the final destination, any node that overhears a data packet also checks its current location and determines if the destination is within its transmission range. If so, the destination node is added to the list of neighboring nodes, if it is not already present. Note that, this particular check incurs zero cost, i.e., no beacons need to be transmitted. Load imbalance and packet retransmission will occur.

PROPOSED SYSTEM

An existing system finds only the location of the neighbor nodes but in proposed system provides the call control mechanism by using EAC and also provides the security from the intruders throughout the end of the call.

A. ENDPOINT ADMISSION CONTROL (EAC)

The EAC procedure consists of a type of "local path" probing of the route to the VoIP server, which focuses on congestion in the *access network*, as opposed to "end-to-end" probing. The assumption here is that the *most significant* delays are commonly in the access network as opposed to the backbone. The reason that ICMP Echo messages are used for probing is to ensure that *different types* of VoIP servers can respond to the probes without the need for any modifications. There are two possible call admission scenarios. The first scenario is where a call originates and terminates on the WLAN phone system. The second scenario is where a call is between wired and wireless counterparts. Fig. 2 illustrates the call setup procedure including the EAC probing phases, where SIP is used as the signaling protocol. SIP is used to establish and tear down call connections, and is used as is, i.e. *no modifications* are required to the signaling protocol used.

When the WLAN handset, A, receives a call setup request from the user, it first sends probing packets to the VoIP server to verify the originating cell is capable of supporting the quality required for the call. If the decision is to admit the call, then SIP messages are sent to initiate call setup. Upon receiving a call setup request (SIP .INVITE. message) from the VoIP server, the caller's handset, B, also sends probing packets to the VoIP server to verify the terminating cell is also capable of supporting the call. If the call can be admitted, SIP is used to complete the call setup procedure and the voice session begins *with acceptable call quality*. If on the other hand it is deemed that the quality of either the originating or terminating cell *is not sufficient* to support the call, a *busy tone* (SIP .BUSY HERE. message is sent by B if its cell cannot support the call) is sent to the user who initiated the call. The main reason for *splitting* the probing path into two parts is the fact that the call initiator is not aware of the IP address of the receiver at the beginning of the call setup request. If the initiator waits for the delivery of the caller's IP address from the VoIP server, which resolves

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 2, February 2014

the caller's phone number to an IP address, this would add an *undesirable delay* to the call setup time. Thus splitting of the probing path is *a compromise between call setup time and realistic probing of the voice path*. A short probing duration is also desirable to minimize the call setup delay, which is very noticeable to the user.

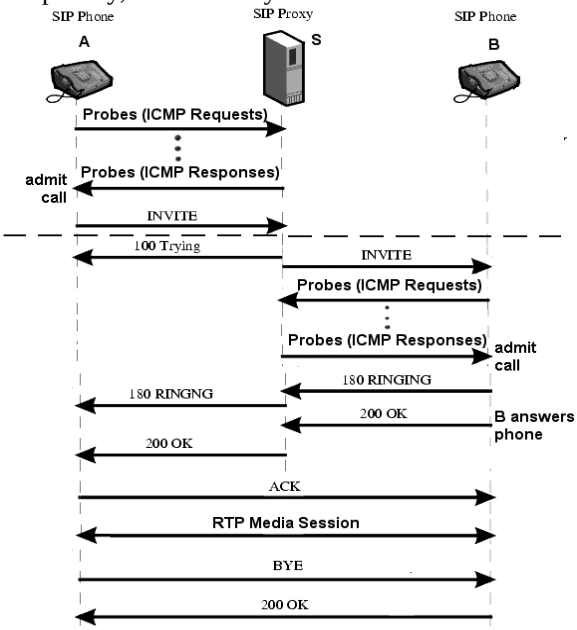

Fig. 2. Call setup sequence showing probing and signaling traffic.

B. EFFICIENT SECURITY MECHANISMS FOR ROUTING PROTOCOLS

In distance vector routing, each router maintains a routing table listing all possible destinations within the network. Each entry in a node's routing table contains the address identity) of some destination, this node's shortest known distance (usually in number of hops) to that destination, and the address of this node's neighbor router that is the _rest hop on this shortest route to that destination; the distance to the destination is known as the *metric* in that table entry. When routing a packet to some destination, the node transmits the packet to the indicated neighbor router for that destination, and each router in turn uses its own routing table to forward the packet along its next hop toward the destination. To maintain the routing tables, each node periodically transmits a routing update to each of its neighbor routers, containing the information from its own routing table. Each node uses this information advertised by its neighbors to update its own table, so that its route for each destination uses as a next hop the neighbor that claimed the shortest distance to that destination; the node sets the metric in its table entry or that destination to 1 (hop) more than the metric in that neighbor's update.

Path vector protocols are similar to distance vector protocols, except that in place of the metric, each routing update includes a list of routers (or, in the case of BGP, a list of Autonomous Systems) on the route. By default, a path vector protocol will choose a route with the shortest recorded path; policies may also specify specific routers to prefer or to avoid. As a result, a node may wish to authenticate each hop that the routing update has traversed as recorded in the path, and to assure that no hops were removed from that recorded path. A traditional way to perform this authentication is to have each node insert an authenticator in the packet, and to have the recipient individually verify each authenticator when the packet is received. This approach requires the network overhead of carrying a message authentication code (MAC) for each node in the path. In this section, we present a *cumulative authentication* mechanism that has the property that the message can be authenticated with only a single MAC, together with an ordered list of nodes traversed by the packet.

V. SYSTEM DESIGN

In the first set of simulations, we evaluate the impact of varying the mobility dynamics and traffic load on the performance of APU and also compare it with periodic beaconing and two recently proposed updating schemes: distance-based and speed-based beaconing Nevertheless, the second part of the cost also plays a very important role in practice, especially when the content is large (e.g., in the order of gigabytes), and it has a significant impact on the choice of parameters. In some previous work it is proposed to divide the content to be distributed into smaller trunks (sometimes referred to as generations), and random linear network coding is applied to each trunk of content independently. This paper consists of five modules are

- Network Creation Module
- Beaconing Information
- Mobility Prediction Rule
- On-Demand Learning Rule
- Graph Analysis

A. NETWORK CREATION MODULE

Mobile Ad hoc network is created with the total number of 48 wireless nodes. Nodes are configured with simulation parameters listed in the simulation model table. Nodes are deployed in the initial location. After the deployment, each node identifies its neighbours by sending beacon. Nodes which are located within the communication range are known as neighbours. Each node broadcast the beacon to its neighbours.

In this module first we create the network environment for adaptive position update for Geographic routing system. The network creation module will be as follows:

So, first we create network module with Source node, intermediate nodes and sink node. In this

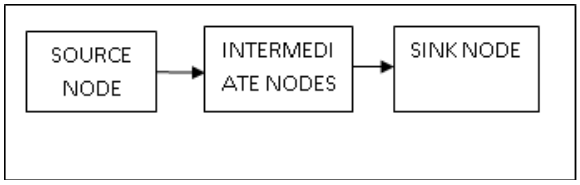

Fig 3. Network creation

Network environment we are going to perform our technique of Adaptive position update (APU). In the router node, we design as the network nodes perform the operations of Beaconing information, mobility prediction

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 2, February 2014

rule and On-demand Learning Rule. The Source node perform the operation of triggering router node by sending the data using Socket technique by giving the IP address from one node to another node. The destination node performs the operation of receiving data and acknowledging the details.

B. BEACONING INFORMATION

In this module, the after triggering the router node, the node initialization process is carried out.

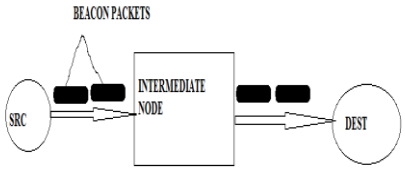

Fig 4. Beaconing information transmission

Then, the beacon packets are transmitted to all the nodes in the network. In this module, we check the nodes distance between previous position and current position. The node distance greater than acceptable threshold update their position to its neighbours through beacon packets.

C. MOBILITY PREDICTION RULE

The beacons transmitted by the nodes contain their current position and speed. Nodes estimate their positions periodically by employing linear kinematic equations based on the parameters announced in the last announced beacon. If the predicted location is different from the actual location, a new beacon is broadcast to inform the neighbours about changes in the node's mobility characteristics The Node Prediction rule is triggered when there is change in the location of the node. The change in the location of the node is cannot be predicated because it moves in the random. The computation overhead involved in the content distribution consists of two parts.

The first part is the cost due to the verification of the packets, and the second part is the cost due to the need to compute random combinations of the data blocks. The preceding sections of this paper focus on the first part of the cost, which can be reduced through the use of more efficient hash functions and batch verification techniques as we have discussed.

Nevertheless, the second part of the cost also plays a very important role in practice, especially when the content is large (e.g., in the order of gigabytes), and it has a significant impact on the choice of parameters. In some previous work it is proposed to divide the content to be distributed into smaller trunks (sometimes referred to as generations), and random linear network coding is applied to each trunk of content independently.

Although this method works in certain application scenarios, it does not address the problem directly but instead avoids high computation overhead by applying random linear network coding to smaller problem instances. Hence, this strategy may lose certain benefits from network coding.

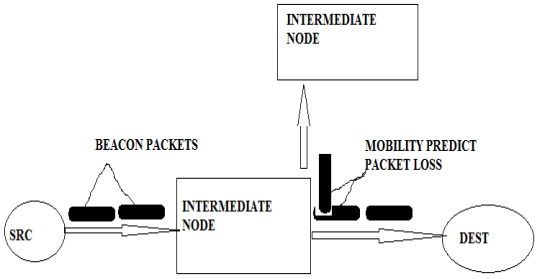

Fig 5. Mobility prediction module

D. ON-DEMAND LEARNING RULE

An accurate representation of the local topology is particularly desired at those nodes that are responsible for forwarding packets. Hence, APU seeks to increase the frequency of beacon updates at those nodes that overhear data packet transmissions.

As a result, nodes involved in forwarding packets can build an enriched view of the local topology. As the name suggests, a node broadcasts beacons on-demand, i.e., in response to data forwarding activities that occur in the vicinity of that node. According to this rule, whenever a node overhears a data transmission from a new neighbor, it broadcasts a beacon as a response. By a new neighbor, we imply a neighbor who is not contained in the neighbor list of this node.

In reality, a node waits for a small random time interval before responding with the beacon to prevent collisions with other beacons.

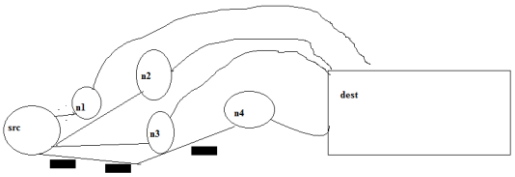

Fig 6. Finding the shortest path by using ODL

E. GRAPH ANALYSIS AND PERFORMANCE EVALUTION

In this module, we analyse our and we evaluate the impact of varying the mobility dynamics and traffic load on the performance of APU and also compare it with periodic beaconing and two recently proposed updating schemes: distance-based and speed-based beaconing (SB). The simulation results show that APU can adapt to mobility and traffic load well. For each dynamic case, APU generates less or similar amount of beacon overhead as other beaconing schemes but achieve better performance in terms of packet delivery ratio, average end-to-end delay and energy consumption.

- **PDR**

PDR is the proportion to the total amount of packets reached the receiver and amount of packet sent by source. If the amount of malicious node increases, PDR decreases. The higher mobility of nodes causes PDR to decrease.

- **ENERGY CONSUMPTION**

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 2, February 2014

It is the amount of energy consumed by the sensors for the data transmission over the network.
Energy Consumption = Sum of energy consumed by each sensor.

- **OVERHEAD**

Overhead = Number of messages involved in beacon update process.

From the trace obtained from the data transmission from source to destination, performance metrics such as energy consumption, overhead, and packet delivery ratio are obtained using the awk script. Awk script processes the trace file and produces the result. Using the results obtained from awk script graph is plotted for performance metrics using graph tool available in ns-2. The computation overhead involved in the content distribution consists of two parts. The first part is the cost due to the verification of the packets, and the second part is the cost due to the need to compute random combinations of the data blocks. The preceding sections of this paper focus on the first part of the cost, which can be reduced through the use of more efficient hash functions and batch verification techniques as we have discussed.

VI. EXPRIMENT

In this section, we present a comprehensive simulation based evaluation of APU using the popular NS-2 simulator. We compare the performance of APU with other beaconing schemes. These include PB and two other recently proposed adaptive beaconing schemes in [13]: (i) Distance-based Beaconing and (ii) Speed-based Beaconing.

We conduct three sets of experiments. In the first set of simulations, we demonstrate that APU can effectively adapt the beacon transmissions to the node mobility dynamics and traffic load. In addition, we also evaluate the validity of the analytical results derived in Section 4, by comparing the same with the results from the simulations. In the second set of experiments, we consider the impact of real-world factors such as localization errors, realistic radio propagation, and sparse density of the network on the performance of APU. In the third set of experiments, we evaluate the impact of parameter AER (which is from MP component) on the overall performance of APU. This enables us to investigate which component (MP or ODL) contributes to the performance more significantly.

SCREEN SHOTS

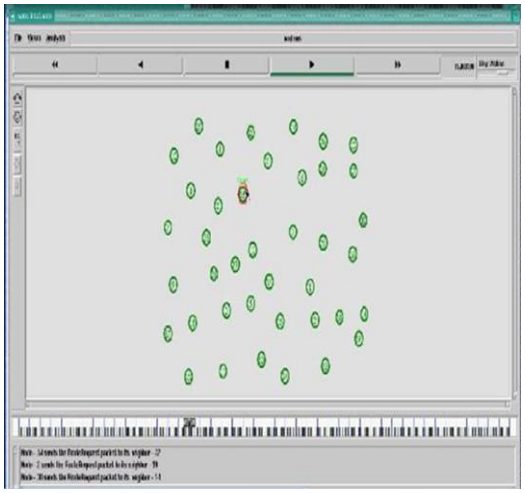

Fig 7. Probing Strategy Output

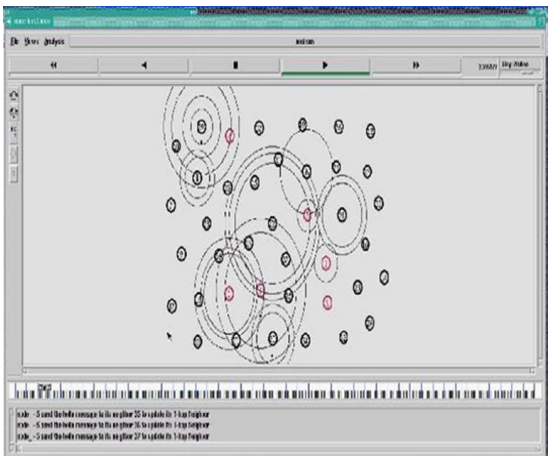

Fig 8. Marking Strategy Output

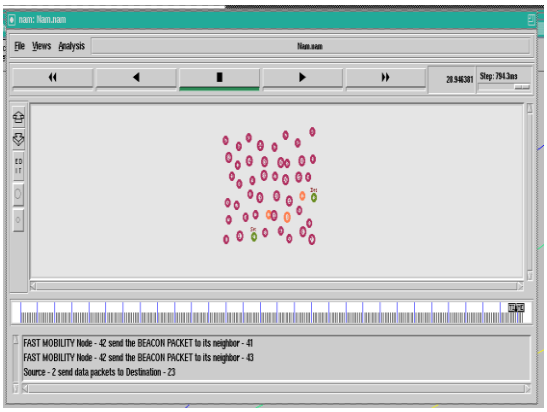

Fig 9. Decision Strategy Output

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 2, February 2014

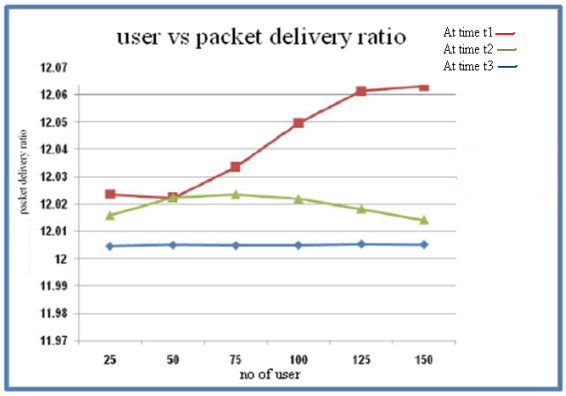

Fig 10. User Vs Packet Delivery Ratio

VII. CONCLUSION

In this project, the need to adapt the beacon update is identified and the corresponding policy is employed in geographic routing protocols to the node mobility dynamics and the traffic load. The Adaptive Position Update (APU) strategy is proposed to address these problems. The APU scheme employs two mutually exclusive rules. The MP rule uses mobility prediction to estimate the accuracy of the location estimate and adapts the beacon update interval accordingly, instead of using periodic beaconing. The ODL rule allows nodes along the data forwarding path to maintain an accurate view of the local topology by exchanging beacons in response to data packets that are overheard from new neighbours. Performance of APU is evaluated using extensive NS-2 simulations for varying node speeds and traffic load. Results indicate that the APU strategy generates less or similar amount of beacon overhead as other beaconing schemes but achieve better packet delivery ratio, less overhead and energy consumption. By using EAC mechanism to control the admission calls over the channel and also provides the security for routing protocol based on distance vector and path vector routing mechanisms.

ACKNOWLEDGMENT

We would like to thank god, our family members and friends for their cooperation and continued support in my career ventures.

REFERENCES

[1] S. Garg and M. Kappes, .An experimental study of throughput for UDP and VoIP traffic in IEEE 802.11b networks,. Proc. IEEE WCNC 2003.
[2] S. Garg and M. Kappes, .Can I add a VoIP call?,. IEEE ICC 2003.
[3] K. Mase, .Toward Scalable Admission Control for VoIP Networks, IEEE Communications Magazine, Vol. 42, No. 7 July 2004.
[4] J.H. James, B. Chen & L. Garrison, .Implementing VoIP: A Voice Transmission Performance Progress Report,. IEEE Communications Magazine, Vol. 42, No. 7 July 2004.
[5] D. Gao and J. Cai, .Admission Control in IEEE 802.11e Wireless LANs,. IEEE Network Magazine, Vol 19, No 4 July/August 2005.
[6] M. Barry, A. T. Campbell, A. Veres, .Distributed Control Algorithms for Service Differentiation in Wireless Packet Networks,. Proc. IEEE Infocom .01, 2001.
[7] C. Perkins, E. Belding-Royer, and S. Das, Ad Hoc On-Demand Distance Vector (AODV) Routing, IETF RFC 3561, July 2003.
[8] J. Li, J. Jannotti, D.S.J.D. Couto, D.R. Karger, and R. Morris, "A Scalable Location Service for Geographic Ad Hoc Routing," Proc. ACM MobiCom, pp. 120-130, Aug. 2000.
[9] Z.J. Haas and B. Liang, "Ad Hoc Mobility Management with Uniform Quorum Systems," IEEE/ACM Trans. Networking, vol. 7, no. 2, pp. 228-240, Apr. 1999.
[10] A. Rao, S. Ratnasamy, C. Papadimitriou, S. Shenker, and I. Stoica, "Geographic Routing without Location Information," Proc. ACM MobiCom, pp. 96-108, Sept. 2003.
[11] S. Lee, B. Bhattacharjee, and S. Banerjee, "Efficient Geographic Routing in Multihop Wireless Networks," Proc. ACM MobiHoc, pp. 230-241, May 2005.
[12] Q. Chen, S.S. Kanhere, M. Hassan, and K.C. Lan, "Adaptive Position Update in Geographic Routing," Proc. Int'l Conf. Comm. (ICC '06), pp. 4046-4051, June 2006.
[13] M. Heissenbuttel, T. Braun, M. Walchli, and T. Bernoulli, "Evaluating of the Limitations and Alternatives in Beaconing," Ad Hoc Networks, vol. 5, no. 5, pp. 558-578, 2007.
[14] Y. Kim, R. Govindan, B. Karp, and S. Shenker, "Geographic Routing Made Practical," Proc. Second Conf. Symp. Networked Systems Design and Implementation, pp. 217-230, May 2005.
[15] F. Kuhn, R. Wattenhofer, and A. Zollinger, "Worst-Case Optimal and Average-Case Efficient Geometric Ad-Hoc Routing," Proc. ACM MobiHoc, pp. 267-278, June 2003.
[16] B. Blum, T. He, S. Son, and J. Stankovic, "IGF: A State-Free Robust Communication Protocol for Wireless Sensor Networks," technical report, Dept. of Computer Science, Univ. of Virginia, 2003.
[17] M. Zorzi and R. Rao, "Geographic Random Forwarding (GeRaF) for Ad Hoc and Sensor Networks: Energy and Latency Performance," IEEE Trans. Mobile Computing, vol. 2, no. 4, pp. 349-365, Oct.-Dec. 2003.
[18] M. Heissenbuttel et al., "BLR: Beacon-Less Routing Algorithm for Mobile Ad-Hoc Networks," Computer Comm., vol. 27, pp. 1076-1086, July 2004.
[19] J. Hightower and G. Borriello,"Location Systems for Ubiquitous Computing," Computer, vol. 34, no. 8, pp. 57-66, Aug. 2001.

BIOGRAPHIES

A. **KEERTHIKA**, PG Student, Department Of CSE, MIT, Pondicherry, India

A. SANTHIYA, UG Student, Department Of ECE, CCET, Pondicherry, India