Routing Mechanism in Mobile Ad hoc Network with Improved Security and Channel Adaptivity under Fading

Jubin Sebastian E
Assistant Professor
Wireless Network Research Centre
Department of ECE
Vimal Jyothi Engineering College, Kerala, India

Anupriya Augustine
M Tech Scholar
Wireless Network Research Centre
Department of ECE
Vimal Jyothi Engineering College, Kerala, India

Joseena M Jose
Lecturer
Department of ECE
College of Engineering Trikaripur

ABSTRACT
Mobile Ad Hoc Network is a type of wireless network without a fixed topology consist a set of self organized nodes which are randomly, frequently and unpredictably mobile. In MANETs packet transmission is affected by radio link fluctuations. Hop count is a simple routing metric that calculate the distance between a source and destination on the number of routers in the path. Routing protocols for ad hoc networks have less channel fading. The minimum hop count is not enough for a routing protocol to achieve a good performance. MANET is an open environment and it is susceptible to many security attacks due to dynamic topology and lack of centralized monitoring authority. Anonymous routing protocols conceal the identities about the route, source and destination to provide security and privacy from intruder's attacks. So in this paper, channel adaptive protocol with improved node security, extensions to a multipath routing protocol to accommodate channel fading and node security is introduced. The resulting protocol is referred to as Channel Adaptive routing protocol with node security (CARNS). Using channel state information (CSI), a pre-emptive handoff strategy is applied to maintain reliable and stable connections. Paths are reusable, rather than simply regarding them as useless. In this paper we provide performance analysis of CARNS, as well as comparison between CARNS with AODV and AOMDV. The simulation results which confirms the improved network performance of CARNS, both in terms of node security and channel fading.

Keywords
Mobile Ad Hoc Networks, routing protocols, security, channel fading.

1. INTRODUCTION
Without fixed topology collection of mobile nodes forming an instant network is called ad hoc network. Ad hoc network does not have any base infrastructures such as in the conventional networks. MANET is very attractive in tactical and military applications because of rapidly deployable and self-organizing configurability. Like tactical communications in a battlefield, where the environment is unfavorable, but fast network establishment, self reconfiguration and security-sensitive operations are absolutely essential [1].

In MANETs, routing is done by using many numbers of protocols. Although routing design is greatly impacted by the fading mechanisms in the wireless channel, existing routing protocols for MANET consider typically only the path-loss effect as far as propagation impairment is concerned while ignoring the deleterious effects of channel fading and shadowing. Link breakages in wireless networks can severely deteriorate network throughput and routing performance. Another significant drawback of existing routing protocols for wireless ad hoc networks is that the considerable differences in the communication channels between nodes are rarely considered, which can directly impact the network lifetime.

Many MANET routing protocol exploit multi-hop paths to route packets, and the successful packet transmission on the paths depends on reliability of the wireless channel on each hop. Highly dynamic nature of nodes affect link stability, introducing large Doppler spread, resulting large channel variations [2]. Route outage probability metric, if used to select optimal route paths, is perhaps more appropriate MANETs than the conventional minimum hop-count metric because it is much more for desirable for a packet to reach its destination with a high success probability even if it involves a few additional hops than it be lost while transferring a route with fewer hop counts. To monitor instantaneous link conditions routing protocol can make use of prediction of channel state information (CSI) based on prior knowledge of channel characteristics. With the knowledge of channel behavior best link can be chosen to establish a new path, or hand over from failing connection to the one with more favorable channel conditions [3].

In this paper, we introduce an extended channel adaptive version of the AOMDV routing protocol, which uses average non fading duration as a routing metric along with hop count. The main parameter in the enhancement is that, we use channel quality information to work with ebb-and-flow of path availability. In this methodology, we can reuse the path which becomes unavailable for a time, rather than discarding them or regarding as useless .Here, we uses channel average non fading duration (ANFD) as a measure of link stability. This protocol uses the same information to predict signal fading and perform necessary handoff, so it can reduce unnecessary overhead on the path discovery phase. Orthogonal Frequency Division Multiplexing (OFDM) is used here to calculate ANFD and AFD. Using this, the handoff scheme will perform between the available narrow bands.

The average fading duration (AFD) is utilized to determine when to bring a path back into active state, allowing for varying nature of path usability instead of discarding at initial failure. This protocol provide a method for avoiding unnecessary route discoveries predicting path failure leading to handoff and then reuse the path when they are available again. Also, the same information is necessary to determine ANFD, AFD and predict path failure, and enhancing efficiency. Transmissions via unreliable wireless connection can result in large packet losses. So, it is important to consider a routing protocol which adapts to channel variations.

MANET is an open environment and it is susceptible to many security attacks due to dynamic topology and lack of centralized monitoring authority [4]. Secure routing protocols conceal the identities about the route, source and destination to provide security and privacy from intruder's attacks. Both active and passive attackers can affect the performance of the routing protocols and may leads to fatal effects in the communication. There are so many secure routing protocols are used to prevent the disastrous consequences by these attackers [5]. The scalability and energy efficiency of existing secure routing protocols are poor, while considering the delays and overhead introduced by the cryptographic methods, and also the cost of implementation is a major drawback to provide high security.

For providing high degree of security for the routing path and nodes in the network, we are introducing the extended form of GPSR which compensate all the security aware disputes in MANET. GPSR uses the greedy forwarding for route discovery. Because of this well defined routing algorithm the routs are immensely attacked by the intruders. The proposed protocol adopted the basics of GPSR for data transmission with great route and node security.

Region based partition is the main technique used in this protocol. The network is partitioned dynamically in to vertical and horizontal regions and one secondary destination position is selected from each regions. Then use the GPSR to send the data from the source node to the first secondary destination position. The nodes which are take part in the GPSR protocol form the routing path. The same procedure can continued till reaching the original destination. Selection of secondary positions is carried out randomly, so the route formed by this protocol is strictly secure from different attacks.

The routing protocol which adapts to channel variations and provide efficient security for routes is introduced in this paper. We call this protocol as Channel Adaptive routing protocol with node security (CARNS).

The rest of the paper organized as follows. In section 2 we review channel adaptive and node security protocols like AODV, AOMDV and GPSR. Proposed methodology is detailed in section 3. CARNS handoff scheme and node security techniques are described on Section 4. Simulation and discussion are presented in section 5 and section 6 is the conclusion.

2. LITRATURE REVIEW

The related works consider some of the well known security providing routing protocols [6]-[9] in Ad hoc networks. The protocols taken here for the literature study are AODV, AMODV and GPSR.

2.1. AODV

AODV [10] is a single-path, on-demand routing protocol. When a source node, Ns, generates a packet for a particular destination node, Nd, it broadcasts a route request (RREQ) packet. Here the source and destination IP addresses remain constant for the lifetime of the network, source sequence number is a monotonically increasing indicator of packet "freshness," destination sequence number is the last known sequence number for nd at ns and hop-count is initialized to zero and incremented at each intermediate node which processes the RREQ. A RREQ is identified by the source sequence number and broadcast ID. An intermediate node processes a RREQ if it has not received previously. If an intermediate node has a route to destination node with destination sequence number at least that in the RREQ, it returns a route reply (RREP) packet, updated with the information that it has. If not, it records :source IP address, source sequence number, broadcast ID, destination IP address and expiration time for reverse path route entry, and forwards the RREQ to its neighbors.

The route expiration time is the time after which the route is considered to have expired and a new route discovery process must be undertaken. Ns send packets via the first path it hears about. If it receives a later RREP which has either new information or a shorter hop-count, it discards the original route information. When a route becomes inactive, a route error (RERR) packet, with sequence number incremented from the corresponding RREP and hop-count of 1, is sent by the upstream node of the broken link to source node. While receiving a RERR, Ns initiates a new route discovery process if it still has packets to send to Nd. Nodes also periodically send "hello" messages to neighboring nodes to maintain knowledge of local connectivity.

2.2. AOMDV

AOMDV [11] extends AODV to provide multiple paths. In AOMDV each RREQ and RREP defines an alternative path to the source or destination. The routing entries contain a list of next-hops along with corresponding hop counts for each destination. To ensure loop-free paths AOMDV introduces the advertised hop count value at node i for destination d. This value represents the maximum hop-count for destination d available at node i. Consequently, alternate paths at node i for destination d are accepted only with lower hop count than the advertised hop count value. By suppressing duplicate RREQ at intermediate nodes node disjointness can be achieved. In both AODV and AOMDV, RREQ initiates a node route table entry in preparation for receipt of a returning RREP.

The time after which the entry is discarded, if a corresponding RREP has not been received, is called as Entry expiration time. In AOMDV, the routing table entry is slightly modified to allow for maintenance of multiple entries and multiple loop-free paths. First, hop-count is replaced by advertised hop-count and it is the maximum over all paths from the current node to Nd, so only one value is advertised from that node for a given destination sequence number. Second, next-hop IP address is replaced by a list of all next-hop nodes and corresponding hop-counts of the saved paths to Nd from that node.

2.3. GPSR

Greedy Perimeter Stateless Routing (GPSR) [12] is routing protocol that uses the positions of routers and destination to make packet forwarding decisions in wireless ad hoc networks. GPSR using only information about a router's immediate neighbors in the network topology for greedy forwarding decisions that are always gradually closer to the destination. If a packet reaches a region where greedy forwarding is impossible then the algorithm recovers by routing around the perimeter of the region. As the number of network destinations increases GPSR scales better in per-router state than shortest-path and ad-hoc routing protocols by keeping state only about the local topology. GPSR can use local topology information to find correct new routes quickly under mobility frequent topology changes.

The figure1 shows the route discovery in the GPSR. Here S is the source node and D is the destination node. R is the node which is the S's closest neighbor to node D. So the GPSR selects R as the relay node in the route path. The route establishing is continued till reaches to the destination node D.

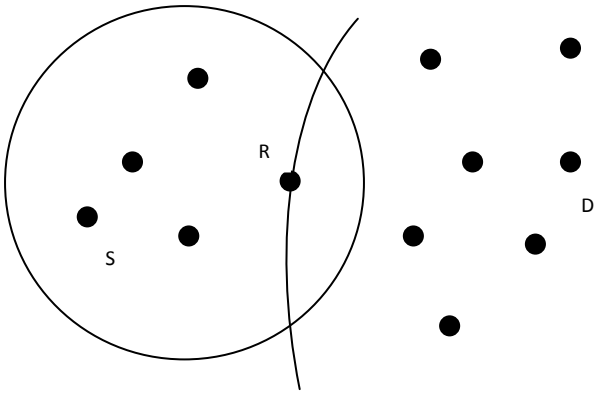

Fig 1: Route discovery in the GPSR.

Route discovery in AOMDV results in selection of link-disjoint, multiple loop-free paths between Ns and Nd, with alternative paths only utilized if the active path becomes unserviceable. One of the main drawbacks of AOMDV is that the path is selected only using the number of hops. Path stability is not taken into account. Thus, selected paths tend to have a small number of long hops .That means nodes are already close to the maximum possible communication distance apart, which will result in frequent link disconnections. Further, channel conditions are idealized with the path-loss or transmission range model, ignoring fading characteristics in all practical wireless communication systems.

In GPSR, greedy forwarding of the packets are taken place. That is the packets are always forward to nodes that are closer to the destination. It easy to reveal the source and destination and to analyze the traffic because of strict relay node selection. So an attacker can very easily find out the routing path, source and destination nodes [13].

The attacks to be faced by MANETs are very high those to be faced by the traditional wireless networks [14]. MANETs are susceptible to both passive eavesdrops as well as active malicious attacks due to the accessibility of the wireless channel to both the genuine user and attacker. The main problem in the implementation of complex security algorithms are the limited power backup and limited computational capability of the individual nodes. Frequent network reconfigurations because of the nodes mobility create more chances for attacks. Different types of attacks on MANET are passive and active attacks.

In passive attack the attacker listens and taps the communication between two nodes. Passive attacks are adverse for the security and privacy of communication. Operation of the communication channel is not disturbed by the passive attacker. But the attacker explores some valuable information about the communication channel. Topology of the network or the relationship between the nodes is used by the passive attacker to find out the network map. This can create some active attacks in the network.

Active attacker can inject unwanted information in the communication channel. It can also listen and modify the information in that channel. Active attackers can replay, modify or deletes some packets from the network. In a replay attack, the attacker resends a packet that was already transmitted. In a modify attack, the attacker can modify the active packets with unwanted information which causes incorrect updates of the routing table. So the packets are transmitted to wrong destinations. Active attacks create network congestion problems.

3. CHANNEL ADAPTIVE ROTING PROTOCOL WITH NODE SECURITY (CARNS)

CARNS considers channel fading to overcome the deficiency of AOMDV. The result of route discovery in AOMDV finds the selection of multiple loop- free, link-disjoint paths between source and destination node. In the route discovery phase, stability is measured using ANFD. These channel state information is determined by OFDM technique. The available frequency band information is always available at transceiver of each node. From this received signal OFDM can measure the average fading duration and average non fading duration of a particular channel. In the route maintenance phase, instead of waiting for the active path to fail, a channel prediction is used to determine the failure, and a handover is made to one of the remaining selected paths. Thus number of dropped packets and delay can be reduced.

3.1 Orthogonal Frequency-Division Multiplexing Technique (OFDM)

OFDM is a multicarrier system, and it divides the available bandwidth into many narrow bands. The main advantage of this system is that its ability to cope with channel fading, without complex equalization filters. In the proposed channel adaptive Multipath routing, OFDM technique utilizes the Channel State Information (CSI), and determine the available narrow bands in the system, when channel fading occurs. The handoff algorithm works based on the available non faded narrow band selected by OFDM. Here OFDM uses Fast Fourier Transform. OFDM is simple in concept, even though its implementation is complex. Mathematically, it can be implemented by using an Inverse Fast Fourier Transform (IFFT) in the transmitter and conversely an FFT in the receiver.

Table 1. Routing protocols comparisons

Protocol	Proactive/ Reactive	Routing Mechanism	Topology/ Geographic	Single/ Multiple route	Identity anonymity	Location anonymity	Route anonymity
AODV	Reactive	Hope by hope encryption	Geographic	Single	Source, Destination	Source, Destination	No
AOMDV	Reactive	Hope by hope encryption	Geographic	Single	Source, Destination	Source, Destination	No
AO2P	Reactive	Hope by hope encryption	Geographic	Single	Source, Destination	Source, Destination	No
ANODR	Reactive	Hope by hope encryption	Topology	Single	Source, Destination	No	Yes
ALARM	Proactive	Redundant traffic	Topology	Multiple	Source, Destination	Source	No
ALERT	Reactive	Randomize	Geographic	Multiple	Source, Destination	Source, Destination	Yes

3.2 Channel State Information (CSI)

The mobile Rayleigh or Rician radio channel is characterized by rapidly changing channel characteristics. As the amplitude of a signal received over such a channel also fluctuates, the receiver will experience periods during which the signal cannot be recovered reliably. If a certain minimum (threshold) signal level is needed for acceptable communication performance, the received signal will experience periods of sufficient signal strength or "non-fade intervals", during which the receiver can work reliably and at low bit error rate is called the average non fading duration.

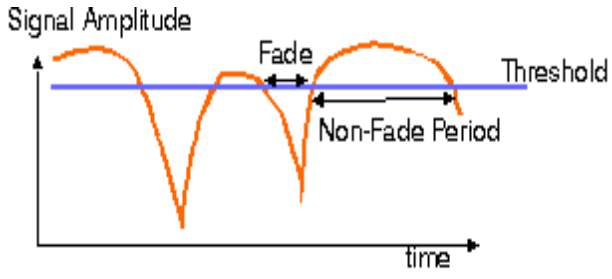

Fig 2: The two-state simplification of the wireless channel behavior.

Insufficient signal strength or "fades", during which the bit error rate is close to one half (randomly guessing ones and zeros) and the receiver may even fall out of lock. The average non fading duration is affected by two parameters such as the physical propagation environment and the node velocities.

The average fading duration ($\tilde{V}$), is the average length of time that the signal envelope spends below the threshold. The two wireless channel behaviors are depicted in figure 2.

3.3 Security in Routing

CARNS uses the underlying GPSR protocol finding the route in the network. The defects generated the malicious attackers in the network cannot be preventable by this GPSR, because of its well defined node selection procedure and the shortest path formations. So in CARNS we are using the extended version of GPSR [15] with alternative selection of relay nodes based on the partitioned regions, and is eligible for giving very secure protection to the routes and nodes. The CARNS having very efficient performance against active and passive attacks in the network by the attacker nodes. The CARNS protocols have better performance compared to the other existing secure routing protocols such as AODV, AOMDV and GPSR in terms of packet drop rate, packet delivery ratio and throughput and these will explained in the later sessions.

4. CARNS HANDOFF AND NODE SECURITY SCHEME

4.1 CARNS Handoff Scheme

Here, whenever the channel is getting faded, depending up on the average non fading duration, each node can switch from the fading channel to the better available channel in the network. This Handoff mechanism improves the connectivity in the network. An example of handoff in CARNS is shown in Figure 3. The handoff process is implemented via a handoff

request (HREQ) packet. For each received packet all the nodes maintain a table, which contain past signal strength, previous hop, and time of arrival. Typically, the required number of samples in the packet depends on the packet receipt times, compared with specified discrete time interval.

4.2 Handoff Trigger

Whenever the downstream node identify the probability of fade and send a HREQ to the uplink node, in this case route handoff triggered. The HREQ registers the following fields: source IP address, destination IP address, source sequence number, fade interval index, long term fading indicator, AFD, and vT max in the Handoff Table to Avoid Duplicate. At the same time if the probability of fading occurs, the receiver checks whether the link is at breaking point with respect to distance.

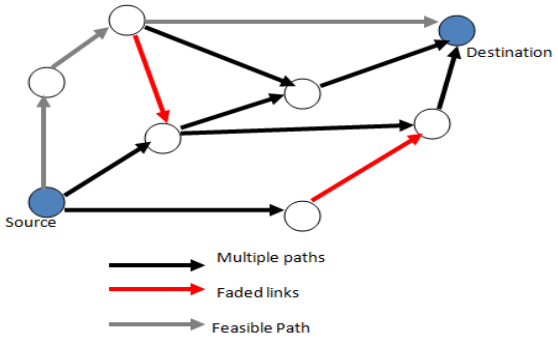

Fig 3: Handoff mechanism.

4.3 Handoff Table

In order to avoid duplicate HREQ, each node maintains a local handoff table. The fields in the handoff table are the source IP address, source sequence number, destination IP address, and expiration timeout. Expiration time out denote when the channel recover from fading and will be available again .It is calculated using the maximum average fading duration (AFD) of all currently faded links. If any unexpired entry is found for that Ns with the same or higher source sequence number, the HREQ is dropped.

4.4 Forwarding the HREQ

Any node receiving a non duplicate HREQ checks for alternative paths to Nd. If not, as for the case of node D, it propagates the HREQ. Otherwise, if it has one or more "good" alternative paths to the Nd, it marks the fading path indicated in the HREQ as dormant, setting the handoff dormant time in its routing table entry for that path to the AFD recorded in the HREQ. The HREQ is then dropped. If a fade is predicted on the active path, a non dormant alternative path to Nd is then adopted prior to the onset of link failure.

4.5 CARNS Node Security Scheme

The underlying protocol for CARNS is the GPSR. CARNS provides route, source and destination security. It uses randomized routing of one message copy to provide protection. CARNS provides more secure data transmission in mobile network [16] and also it can act as a resistant to certain types of attacks. The delay is reduced and results in the fastest data delivery across the networks.

CARNS is a region based routing protocol. In this the entire coverage area is divided in to different regions and selecting one secondary destination position from each region [17]. Then this protocol uses GPSR routing to forward data from one region to another. All the nodes in the protocol will create an untraceable path for the routing. So an outside attacker cannot easily find out this route due to the alternate manner of intermediate secondary destination position selection [18]. The route establishment of CARNS is shown in figure 4.

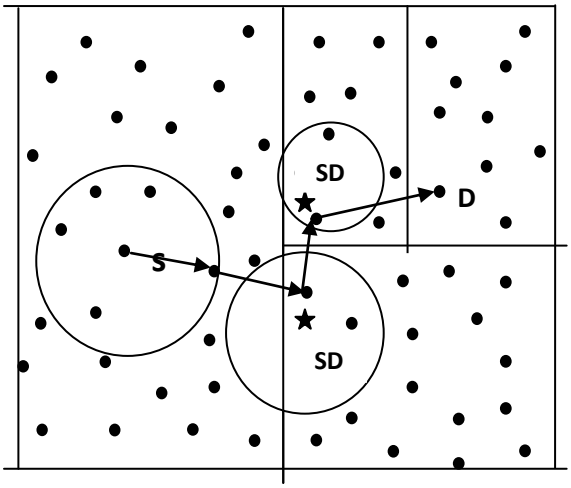

Fig 4: The route establishment of CARNS.

5. PERFORMANCE EVALUATION

Simulation is carried out to evaluate the performance [19] of CARNS protocol in terms of packet transmission and routing performance using ns 2.28. The results obtained are shown below. In this set of simulations, we vary the maximum node mobility in the Random Way Point mobility model, from 1*m/s* up to 5m/s, in the step of 1m/s. Higher mobility leads to more frequent changes in the network environment, and therefore to more difficult scenarios. Figure 5, 6 and 7 shows the packet delivery rate (PDR) and packet drop rate and throughput as the mobility of a node changes. The construction of multiple paths at route setup, and the search for eligible paths in the route establishment phase and ensures availability of alternative paths in case of channel fading and perform the route hand off, resulting in less packet loss. Hence throughput is comparatively high for CARNS than other routing protocols. For all algorithms the delivery ratio decreases with increasing node speeds. Compared to AODV and other routing algorithms gave a better delivery ratio in all scenarios. Since multiple routes are available between the source and destination the packet drop rate is reduced by the CARNS hand off scheme. Here we provide experimental evaluation of the CARNS protocol, which AOMDV, AODV and GPSR. The results exhibit the superior performance of CARNS in terms of packet delivery ratio, packet drop ratio and throughput.

The ratio of packets that are successfully delivered to a destination compared to the number of packets that have been sent out by the sender is the packet delivery ratio and the simulation results show that, it is higher in CARNS than the other protocols taken for the comparison. The improved packet delivery ratio of CARNS is set up because of the efficient handoff strategy used in this. We can send the packets successfully even in the situation of higher fading in the channel with selection of alternate channel. The channel

adaptive nature of the protocol improved the performance great with the packet delivery ratio. The route selection procedure followed by the CARNS also avoided the unwanted interactions from the attacker nodes and the packets are delivered to the destination with extreme security.

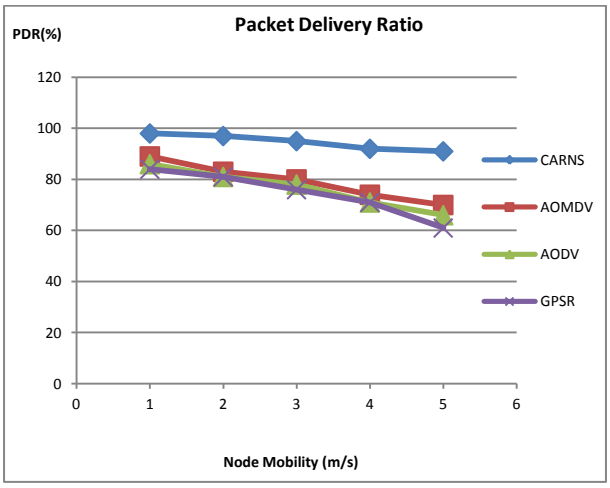

Fig 5: Comparison of Packet Delivery Ratio between CARNS, AOMDV,AODV and GPSR under different node moving speed.

The difference between the packets which are send the source and reached to the destination is the packet drop ratio or simply the total number of packets dropped during the transmission ratio. Improvement in the packet delivery ratio will reduce the packet drop ratio also. The key techniques of CARNS like handoff under fading channel scenarios and secure route selection are capable of establishing the low packet drop. The rate of successful packet delivery over a communication channel is defined as the throughput. Because of better performance in packet delivery and packet drop CARNS also shows superiority among other protocols in throughput also.

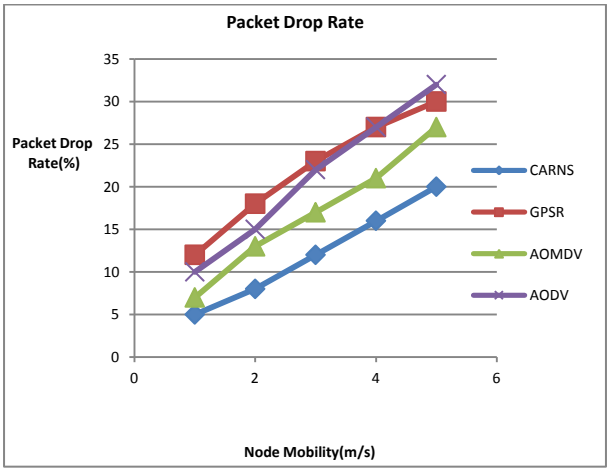

Fig 6: Comparison of Packet Drop Ratio between CARNS, AOMDV,AODV and GPSR under different node moving speed.

In summary, the experimental results exhibit the improved performance factors of CARNS compared with AOMDV, AODV and the baseline GPSR protocols. The favorable methods used for the channel selection under fading and the secure route discovery are capable of giving efficient performance for CARNS.

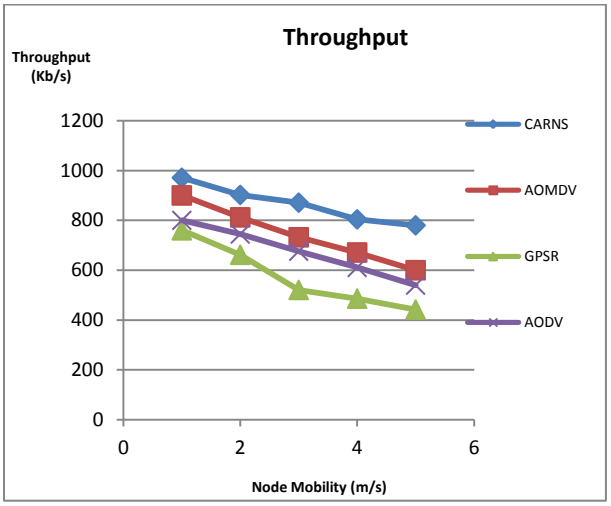

Fig7: Comparison of Throughput between CARNS, AOMDV,AODV and GPSR under different node moving speed.

6. CONCLUSION

MANET is a dynamic, infrastructure less and decentralizes network. The self configuration ability of MANET constitutes a wide variety of applications in tactical and common life. So the development of a routing protocol which satisfies all the performance enhancement features have great impact in networking fields.

The proposed CARNS considers channel fading to overcome the deficiency of AOMDV and it uses average non fading duration as a routing metric along with hop count. This protocol can reduce unnecessary overhead on the path discovery phase due to the utilization of the same information to predict signal fading and perform necessary handoff. ANFD and AFD calculated using the Orthogonal Frequency Division Multiplexing (OFDM) and the handoff scheme can perform between the available narrow bands.

Security is another major performance factor for reliable communication in MANET. The inherent features of MANET make it susceptible to many security attacks which may completely or partially destroys and changes the information contents. This will demands secure routing protocols to provide a very high level of security in MANET. Different techniques are used in secure protocols to achieve the goal of security. CARNS is the MANET protocol which provides higher security for the nodes and routing path. Performance of underlying GPSR routing can be improved by this new protocol and can avoid some adverse attacker effects. The main property of CARNS which provides security is its region partitioning and the alternate selection of secondary destination position from each partitioned regions.

In our paper we mainly deal with the passive attacks in the wireless networks. The future works mainly concentrates on the active attacks and related security issues in the networks. Also the proposed CARNS can be efficiently used for the IoT. Our future works and developments are for modifying this two tasks.

7. REFERENCES

[1] A. Pfitzmann, M. Hansen, "Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management - A Consolidated Proposal for Terminology," Tech. Rep., February 2008.

[2] Shweta Jain and Samir R. Das Computer Science Department State University of New York "Exploiting Path Diversity in the Link Layer in Wireless Ad Hoc Networks", Stony brook Stony Brook, NY 11794.

[3] Xiaoqin Chen, Haley M. Jones, and Dhammika Jayalath "Channel-Aware Routing in MANETs with Route Handoff", IEEE Transactions on Mobile Computing, vol. 10, NO. 1, Jan. 2011.

[4] S. Corson, J Marker," Mobile Ad Hoc Networking (MANET):Routing Protocol performance Issues and Evaluation Considerations", RFC 2501, January 1999.

[5] T. Camp, J. Boleng, and V. Davies, "A Survey of Mobility Models for Ad Ho Network Research", Wireless Communications and Mobile Computing, vol. 2,pp.483-502, 2002.

[6] Xiaoxin Wu and Bharat Bhargava, "A02P-Ad Hoc On-Demand Position-Based Private Routing Protocol", IEEE Transaction on mobile computing, VOL 4. NO. 3, May/June 2005.

[7] J Kong and X. Hong, "ANODR: Anonymous on Demand Routing with Untraceable Routes for Mobile Ad-Hoc Networks", Proc. Mobile Ad Hoc Networking, 2003.

[8] C.E. Perluns and P. Bhagwat, "Highly Dynamic Destination Sequenced Distance Vector Routing (DSDV) for Mobile Computers", Proc. ACM SIGCOMM, 1994.

[9] Z. J. Haas and M. R. Pearlman, "The Zone Routing Protocol (ZRP) for Ad Hoc Networks", Internet Draft, MANET Working Group, draft-ietf-manet-zonezrp-03.txt, March 2000.

[10] Perkins, E.M. Royer, "Ad-Hoc On-Demand Distance Vector Routing," Proc. IEEE Workshop Mobile Computing Systems & Applications, pp. 90-100, Feb. 1999.

[11] M.K. Marina, S.R. Das, "On-Demand Multipath Distance Vector Routing in Ad Hoc Networks," Proc. Ninth Int'l Conf. Network Protocols,pp. 14-23, Nov. 2001.

[12] Brad Karp, H.T.Kung, "GPSR: Greedy Perimeter Stateless Routing for Wireless Networks", Proceedings of 6th Annual International Conference on Mobile Computing & Networking, pp.243-254.

[13] T. Camp, J. Boleng, and V. Davies, "A Survey of Mobility Models for Ad Hoc Network Research", Wireless Communications and Mobile Computing, vol. 2,pp. 483-502, 2002.

[14] J. Raymond, "Traffic Analysis: Protocols, Attacks, Design Issues, and Open Problems," Proc. Int'l Workshop Designing Privacy Enhancing Technologies: Design Issues in Anonymity and Unobservability, pp. 10-29, 2001.

[15] L. Zhao and H. Shen, "ALERT-An Anonymous Location-Based Efficient Routing Protocol in MANETs", Proc. Int'l Conf. Parallel Processing (ICPP), 2011.

[16] J. Kong, X. Hong, M. Y. Sanadidi, and M. Gerla, "Mobility Changes Anonymity: Mobile Ad Hoc Networks Need Efficient Anonymous Routing", in ISCC, 2005, pp.57-62.

[17] M.F. Mokbel, C.-Y. Chow, and W.G. Aref, "The New Casper: Query Processing for Location Services without Compromising Privacy", Proc. 32nd Int'l Conf. Very Large Databases (VLDB), 2006.

[18] B. Zhu, Z. Wan, M. S. Kankanhalli, F. Bao, and R. H. Deng, "Anonymous Secure Routing in Mobile Ad-Hoc Networks", LCN '04' 2004.

[19] Jun Liu, Jiejun Kong, Xiaoyan Hong, and Mario Gerla, "Performance Evaluation of Anonymous Routing Protocols in MANETs", IEEE Wireless Communications and Networking Conference, 2006.