ISSN:0975-9646
Himansu Sekhar Pattanayak et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 2 (4) , 2011, 1559-1563

Gray Zone Effect in MANETs on Proactive and Reactive Routing Protocols

Himansu Sekhar Pattanayak[1], H. S Bindra [2], A. L Sangal [3]
[1-3] *Computer Science and Engineering, Dr. B. R. Ambedkar, NIT Jalandhar, India*

Abstract— **There has been much research work done on the improvement of adhoc routing protocols to enhance network performances. But in these networks, performance is very much dependent on wireless physical layer where communication is quite complex. The effect of the combination of different routing strategies (protocols) and physical channel properties can vary the network performance up to a great extend. Gray zone effect is one of such effects, which results in high data loss and degradation of performance. Generally, in adhoc networks, broadcast control packets have lower data rate and user packets have same or higher data rates. Low data rate packets can travel longer distance than high data rate packets. Packet sizes of control packets are smaller compared to data packets, so control packets can cover greater distance than other packets. Due to these reasons, communicating nodes find valid paths which data packet cannot cover. This is known as gray zone effect. In our proposed work, we have selected OLSR (proactive), AODV (reactive) routing protocol for analyzing the phenomena. We also propose a simple approach to reduce the performance degradation by limiting the size of application data packets.**

Keywords— **Gray Zone, AODV, OLSR, Lower hop count, Broadcast rate and Unicast rate, Control packets and Data packets, Adhoc Network.**

I. Introduction

Mobile adhoc networks (MANETs) [1] are infrastructure-less networks, where mobile nodes in the network dynamically establish route among themselves to form their own network while moving. It is formed instantaneously, and uses multi-hop routing to transmit information. MANET technology can provide an extremely flexible method of establishing communications in situations where geographical or terrestrial constraints demand a totally distributed network system without any fixed base station.

Routing is a difficult problem in a MANETs. In the absence of dedicated routers nodes have to act as routers. MANET routing protocols have been classified into two major categories [2].

A. Proactive Routing Protocol

Proactive protocols rely on the periodic exchange of routing information between nodes, and are triggered by network topology changes. Subsequently, when a node has to forward data packets, it performs a table lookup. **Eg:** Optimized Link State Routing (OLSR), Fish-eye State Routing (FSR), Destination Sequenced Distance Vector (DSDV).

Optimized Link State Routing (OLSR): OLSR [4] is a proactive IP routing protocol for mobile ad hoc networks. It can be implemented in any ad hoc network. Lately, it is also used in WiMAX Mesh. OLSR is classified as proactive due to its nature. Nodes in the network use topology information derived from HELLO packets and Topology Control (TC) messages to discover their neighbours. Not all nodes in the network route broadcast packets. Only Multipoint Relay (MPR) nodes route broadcast packets. Routes from the source to the intended destination are built before use. Each node in the network keeps a routing table. This makes the routing overhead for OLSR higher than any other reactive routing protocol such as AODV or DSR. However, the routing overhead does not increase with the number of routes in use since there is no need to build a new route when needed. This reduces the route discovery delay. In OLSR, nodes send HELLO messages to their neighbours at a predetermined interval. These messages are periodically sent to determine the status of the links. This protocol maintains bi-directional links for communications.

B. Reactive Routing Protocol

Reactive protocols perform route discovery only when there is data to forward and then cache the discovered routes. Subsequently, if a source sends additional packets to a destination, it can use the cached route information. **Eg:** Ad hoc On Demand Distance Vector (AODV), Dynamic Source routing protocol (DSR), Temporally ordered routing algorithm (TORA).

Ad Hoc On-Demand Distance Vector Routing (AODV): AODV [3] discovers routes, when needed via route discovery process. It uses traditional routing tables, one entry per destination. AODV relies on routing table entries to propagate an RREP back to the source and, subsequently, to route data packets to the destination. AODV uses sequence numbers maintained at each destination to determine freshness of routing information and to prevent routing loops. A routing table entry is expired if not used recently. A set of predecessor nodes is maintained for each routing table entry, indicating the set of neighbouring nodes which use that entry to route data packets. These nodes are notified with RERR packets when the next-hop link breaks. Each predecessor node, in turn, forwards the RERR to its own set of predecessors, thus effectively erasing all routes using the broken link. RERR packets in AODV are intended to inform all sources using a link when a failure occurs.

C. Communication Gray Zone

Due to small-scale and large-scale channel variation, the channel quality changes within milliseconds depending on the nodes location and mobility. The routing protocol cannot select a route simply based on a single route request message [5]. Most of the wired networks rely on the symmetric links which are always fixed. But in case of wireless networks, the nodes are mobile and constantly changing their position within network. Again, the physical medium usually chosen i,e; 802.11 is not bidirectional rather, it sometimes display unidirectional properties. Thus, communication in wireless networks is more complex than wired networks. Another characteristic of wireless channel, which has an effect on performance of ad hoc routing protocols, is communication gray zone [6]. Communication gray zone is the area where link is quite fragile and data loss is high. For better performance we need to avoid such links in our path. A single link of such type in the path can have drastic effect on data delivery. In larger network the situation get worse. The gray zone effect can happen, when broadcasting control packets can find connectivity between two nodes but data packets cannot travel that distance. In this case, nodes are able to find valid routes but some data packets may not reach the destination.

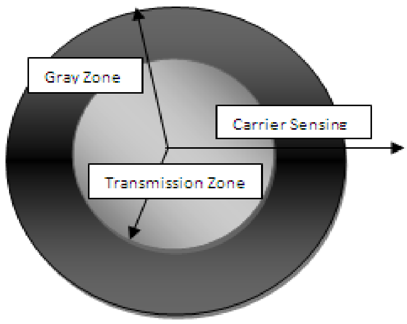

Fig 1 Communication gray zone

As shown in Fig 1, the inner most region is known as transmission region in which transmission is smooth and good. The outer most region is called physical carrier sensing zone, in which the neighbour node can sense the signal but cannot receive all. The middle one is known as gray zone in which links are fragile and high error rate is there in receiving packets. Again these regions can expand or sink according to different physical parameters.

There are some factors contribute to gray zone effect in ad hoc networks which are given below:

- *Different Transmission Rate:* In IEEE 802.11a/b/g, broadcast packets are always transmitted at a base bit rate while data packets can be sent at higher rate. Then the broadcasted packets can reach further than data packets. This is the main reason causing a gray zone.
- *Control Packet Size:* Generally control message are of small size than data packets. It means control packets can cover more distance than the data packets. It results in longer links which the data packets cannot cover. Moreover, bit error rates are high in case of bigger packets.
- *Fluctuating Links and Hello Message:* At the edge of the transmission range, the link quality is poor and unsteady. If the HELLO messages are received successfully, this link becomes an unreliable link in a route. Ad hoc protocols use broadcast messages to discover routes and periodically broadcast HELLO beacons to detect neighboring nodes so that it can update routes in the routing table. The HELLO messages are small in size in comparison to data packets.They are sent at default broadcast rate, which is lower than the data packets. So, they can travel greater distance and detect distant node as neighbor. Thus, The HELLO messages have special properties contributing to the gray zone creation [6]:

Let's take an example to explain the gray zone effect. In the Fig 2 ,source S is communicating with destination D. Suppose AODV is the routing protocol. Node A and B are both in the radio range of source S. So, S detects both A and B as its neighbours. When a path between S to D will establish; it will be S->B->D (shown in dark links) instead of S->A->B->D (shown in dashed links), due to lesser hop count. But the large user packets cannot reach to node B, which is at the edge of the link between S and B. This will degrade the network performance. But, if the path S->A->B->D would have been, chosen then there would have been fewer drops of packets.

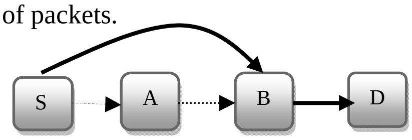

Fig 2 Problem of selecting lower hop count path

Thus, the hop count based protocols like OLSR, AODV are sensitive to gray zone effect. OLSR maintains link state of the paths and communication is only through bi-directional links. So, these links are comparatively stable. But, AODV select path based only on hop count. AODV chooses the path with lesser hop count resulting in fragile links. So, AODV is more sensitive to gray zone effect than OLSR.

The rest of the paper is organized as follow. Section II describes previous research on the communication gray zone problem in wireless network. Section III describes our work, Section IV discusses about simulation set up and results. The last section is for conclusion and future work.

II. Related Work

In work [7] the author used mote devices with hardware technology as mica2 and mica2dot. Mica2 nodes show a quite irregular behaviour immediately beyond the communication distance of 55 m and 65 m and the packet reception probability has a large variance. This is referred as "gray-zone phenomenon". Increasing in the distance resulted in higher packet reception. The authors in paper [8] observed spurious performance degradations with the AODV-UU implementation. The reason they gave is presence of communication gray zones in the network, which were several meters wide. In these zones, the routing protocol would report a valid route to the destination node, but virtually no data packets would pass through. Further experiments revealed that these gray zones are caused by the difference in transmission range for different packet types. In IEEE 802.11b, broadcast packets are sent at 2 Mbit/s while unicast packets can be sent at data rate up to 11 Mbit/s. As a result, broadcast packets can reach greater distance than unicast packets, which is the main cause of gray zone.

Author in paper [6] says that OLSR and LUNAR [9] are less sensitive than AODV to communication gray zones. OLSR uses strong bi-directional links for communication, which is not the case in AODV. LUNAR does not rely on a broadcast neighbour sensing algorithm. Instead, it re-discovers delivery paths after a predefined time interval, irrespective of the time when the old path was used to transmit data packet. Thus, the creation of new routing table entries is solely based on unicast route replies, which mitigates the gray zone problem for LUNAR.

Note that, AODV too creates routing table entries based on unicast RREP messages. However, when using HELLO messages (instead of link layer notification), original AODV also adds routing table entries based on broadcasts. Every time a data packet is transmitted, life time for the path is renewed and no new path is discovered. Researchers in paper [10] confirmed the existence of gray zone contributing to the negative effect in the secure routing protocol of mobile ad hoc network. By testing the hardware indoor and doing the simulation, they compare AODV and SAODV (Secure AODV) routing protocol.

The work in paper [11] is focused on the wireless network with the bidirectional links. After receiving the RREQ (Route Request) message, the node creates RREQ ACK (Acknowledgment) and returns to the sent node. They confirmed that, they can use strong link instead of fragile link as opposed to the original AODV protocol. By adding the function, that prevents the omnidirectional links cases, they tried to reduce gray zone effect. But, this method may introduce high complexity in the network. Work in [6] shows that artificially limiting the range of AODV HELLO packets by filtering on the SNR (signal to noise ratio) value eliminates the gray zone effect. In fact, setting the SNR acceptance level such that, HELLO packets have slightly shorter transmission range than the data packets, will force AODV to pick a more robust link than earlier; and it will increase the overall performance. But this method is complicated, as it necessary to implement the function at MAC layer.

The authors of work [12] did the experiment with QualNet 3.7 commercial network simulator. QualNet provides a 'closer to reality' propagation and path loss model. Under the 'two-ray ground reflection' propagation model and using 802.11b radio they notice that the gray zone for longer packet is wider than shorter packet. To solve the asymmetry between the control packet and the data packet they propose to dynamically determine the size of the control packets in conformance to the application data packet size for which a route is sought for. AODV protocol is taken for study. In this proposal, the source resizes the RREQ packets to make it the same length as of the data packet by using dummy bytes, so that RREQ packets that reach the destination indeed show the routes that will be physically able to deliver the same length of data packet on an end-to-end basis. But, this scheme has its demerits as it introduces additional complexity and large overhead due to addition of dummy byte.

The authors in [13] propose a new technique by setting data rate for unicast and broadcast to different values. Broadcast rate is set higher than unicast data rate. When the distance between nodes is approximately 200 m apart (in presence of gray zone) the throughput for high broadcast rate is more than that of low broadcast rate. The experiment is done on OLSR routing protocol.

III. PROPOSED WORK

Our work is divided in to three parts. In first part we examine the distance at which gray zone effect occurs. By simulation, we determine the distance at which links are fragile. We perform simulation on each specified data rate for IEEE 802.11, i.e., 1, 2, 5.5, 11 Mbps. For the next part of the work we select AODV and OLSR as routing protocols. From result of first part of our experiment, we set the distance between the nodes more than gray zone distance and compare the result with the scenario that do not have gray zone effect. Then we compare the degradation of performances for OLSR and AODV protocols. In our experiment, we here show that AODV is more sensitive to gray zone. In the third part we change the application data packet to different sizes and compare their result. With increase in packet size of user data packets; throughput increases due to lesser overhead. But increasing beyond certain limit throughput decreases due to gray zone effect. In this work we propose that, by limiting application data packets length we can restrict the gray zone effect and increase throughput. It simpler than the work [12] in which, control packets are added with dummy bits to make them same length as user data packets. It increase overhead of control packets and performance may decrease due to congestion.

IV. SIMULATION AND RESULTS

We use Qualnet 5.0.2 network simulator for our work. Qualnet [14] network simulator is commercial network simulation environment for network modelling and simulation. It resembles very closely with real world implementation. We have selected average number of packet received and average throughput (number of bits processed / difference of time between first and last received packet in seconds) as the parameters for our study. First we have taken two nodes on work space. We employ AODV protocol as routing protocol. 802.11b is chosen as physical layer. The simulation parameters are given in Table I.

TABLE I
PARAMETERS-EFFECT ON PERFORMANCE DUE TO CHANGING DISTANCE BETWEEN THE NODES

Parameters	**values**
No Of Nodes	2
Terrain Size	1000 m *1000 m
Traffic type	CBR
Distance between nodes	100,200,300,400,500,600 meters
Application Data rate	5 kbps
Routing Protocol	AODV
Simulation Time	100 seconds
Physical Layer Data Rate	1,2,5.5,11 Mbps

Fig 3 shows the simulation results of the performances of communicating nodes based on the distance between them. The distance between the nodes varies from 100 to 600 meters. We have different data rates for the physical layer according with IEEE 802.11b standards. In this result we wanted to reveal the relationship between distance (between neighbouring nodes) and throughput. It can be clearly seen in the graph that, at a distance of 100 and 200 meters throughput of four different physical data rates is nearly same. As the distance increases throughput decreases in all four cases. At about 300 meter, throughput of 11 Mbps data rate decrease more rapidly than the others. At about 400 meters, throughput for 11 mbps data rate decreases to zero. We can see that, throughputs decrease more rapidly in higher data rates. It can be seen that, after 200 meters there is steady decrease in throughput for each data rate. It re-affirm the theory that with lower data rate data packets can travel more distance and can be received successfully. We have clearly seen the gray zone effect after distance 200 meters.

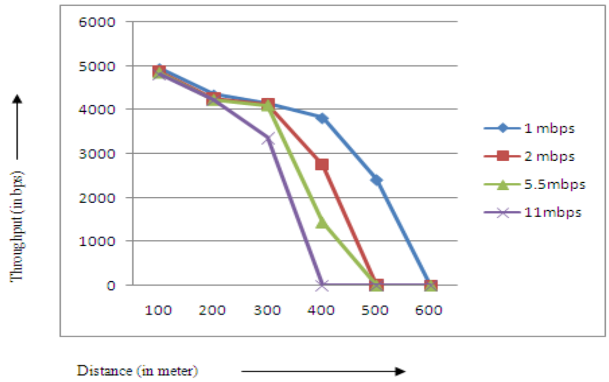

Fig 3 Change in throughput due to change in distance

In the next simulation we have taken 16 nodes on work space. Two different terrain sizes are selected to have different average distance between nodes. In first case we take 200 * 200 m terrain size. The work space is of square size. The average distance becomes 50 meters. At this distance there is less chance of communication gray zone as we have seen in the previous experiment. The gray zone effect starts after 200 meters distance between nodes. The second terrain size is 1200 * 1200 m so that the average distance between the nodes will be 300 meters. In this case we ensure that there is presence of gray zone. Traffic type CBR is chosen for all cases. Application data rate is varied as 0.5, 1, 1.5, 2, 2.5 Mbps. All other parameters are given in Table-2.

TABLE III
PARAMETERS-GRAY ZONE EFFECT ON AODV & OLSR PROTOCOLS

Parameters	values
No Of Nodes	16
Terrain Size	200 m *200 m, 1200m *1200m
Application type	CBR
Application rate	0.5,1,1.5,2,2.5 Mbps
Mobility	0-10 m/s
Routing Protocol	AODV, OLSR
Simulation Time	100 seconds
Physical Layer Data Rate	2 Mbps

In above two figures OLSR-50, AODV-50 denotes average distances between nodes are 50 meters in 200 * 200 meters terrain size. In this case, gray zone effect is negligible. OLSR-300, AODV-300 denotes average distances between nodes are 300 meters in 1200 * 1200 meters terrain size. In this case, gray zone effect is there. The performances of OLSR and AODV are nearly similar, at distance 50 meters between nodes, in both average packets, and throughput. But when the distance becomes 300 meters then performance decreases significantly. As it can be seen in Fig 4 and Fig 5 OLSR performs better than AODV. This proves that AODV is more sensitive to gray zone effect. AODV only compares hop-count metric for selection of path which makes the paths fragile and more sensitive to gray zones.

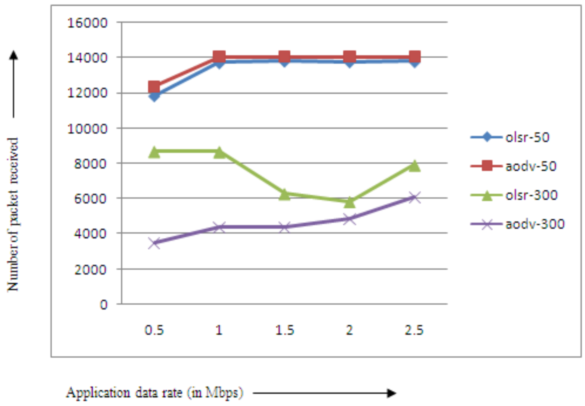

Fig 4 Gray zone effect on average number of packets received

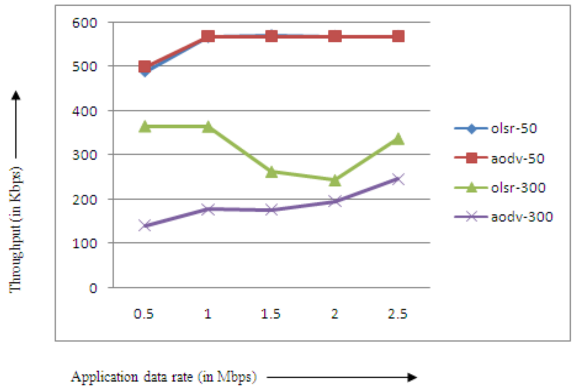

Fig 5 Gray zone effect on average throughput

In the next simulation we take 50 nodes on work space. In order to some randomness we place them with random placement model available in Qualnet software. We take 1500 * 1500 m terrain size. The work space is of square size. The average distance becomes 200 meters. In this distance there is more chance of communication gray zone as we have seen in previous experiment. We take CBR application for the experiments. For all simulations IEEE 802.11b is taken as physical layer. We vary the size of application data packet as 0.5, 1, 1.5, 2, 2.5 Kilo bytes. Other parameters are given in Table III.

TABLE IIIII
PARAMETERS-EFFECT OF PACKET SIZE ON GRAY ZONE

Parameters	values
No of Nodes	50
Terrain Size	1500m *1500m
Traffic type	CBR
Application data rate	4 Mbps
Size of data packet	0.5,1,1.5,2,2.5 kilo bytes
Mobility	0-10 m/s
Routing Protocol	AODV, OLSR
Simulation Time	100 seconds
Physical Layer Data Rate	2 Mbps

As it can be seen in the Fig 6, as packet size increase from 0.5 kilo bytes throughput increases and attains maximum at 1.5

kilo byte packet size for both AODV and OLSR protocols. This is because lesser overhead for per user data packet. But, if we increase the user data packet size beyond 1.5 kilo bytes throughput decreases rapidly. It is because bigger data packets are more affected by gray zone effect than smaller data packets. We can also see that throughput of OLSR is more sensitive to size of data packets.

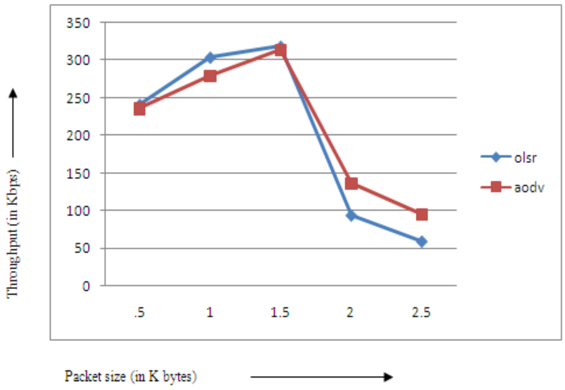

Fig 6 Sensitivity of AODV & OLSR for change in size of data packets

V. Conclusion And Future work

From the research we can conclude that, the presence of gray zone decreases the network performances up to a great extend. Gray zone effect is more on higher data rates than lower data rates. Low data rate packets can travel more distance then higher data rate packets. We also conclude that AODV is more affected, by the presence of gray zone, than OLSR. By doing simulations we realize that; we can increase the network performance by reducing the gray zone effect if we limit our application packet size. It is better and easier than adding dummy bits to control packets. The experiments also reveal that OLSR is more affected by change in packet size than AODV protocol.

There is further scope to reduce gray zone effect by setting data rates for unicast and broadcast to appropriate values for different application rates. By selecting optimum packet size and data rate, we will try to minimize gray zone effect in our future work.

References

[1] Ning Zhang . Alagan Anpalagan, “Sensitivity of SWAN QoS model in MANETs with proactive and reactive routing: a simulation study”, Telecommun Syst, © Springer Science, 2009.

[2] Loay Abusalah, Ashfaq Khokhar, and Mohsen Guizani, “A Survey of Secure Mobile Ad Hoc Routing Protocols”, IEEE Communications Surveys & Tutorials, vol. 10, no. 4, 2008..

[3] Ian D. Chakeres and Elizabeth M. Belding-Royer, “AODV Routing Protocol Implementation Design”.

[4] T.H. Clausen and P. Jacquet, “Optimized Link State Routing (OLSR)”, RFC 3626, October 2003.

[5] S.Shakkottai, T.S.Rappaport and P.C.Karlsso, “Cross-layer Design for Wireless Networks", IEEE Communications Magazine, October 2003.

[6] H.Lundgren, E.Nordström, C. Tschudin , “Coping with communication gray zones in IEEE 802.11b based ad hoc networks”, 5th ACM international workshop on Wireless mobile multimedia ,2002.

[7] Giuseppe Anastasia, Eleonora Borgiaa, Marco Contiac, Enrico Gregoria, Andrea Passarellaa, “Understanding the real behavior of Mote and 802.11 ad hoc networks: an experimental approach”, Pervasive and Mobile Computing, 2005 , www.sciencedirect.com.

[8] Christian Tschudin, Per Gunningberg, HenrikLundgren, ErikNordstrom, Computer Science Department, University of Basel, “Lessons from experimental MANET research” Ad Hoc Networks 3 (2005), www.sciencedirect.com

[9] C. Tschudin, “Lightweight Underlay Network Ad Hoc Routing (LUNAR) Protocol”, IETF Internet draft, drafttschudin- manet-lunar-00.txt, March 2004.

[10] Yuxia Lin, A.H.M. Rad, Vincent W.S. Wong, “Experimental Comparisons between SAODV and AODV”, Modeling and Simulation, AICMS, May 2008.

[11] Kazuhiro Mizoguchi, Teruaki Kitasuka, Tsuneo Nakanishi and Akita Fukuda, “A Consideration of Communication Gray zone Problem in Ad hoc Networks using Wireless LAN”, IPSJ SIG Technical Report, 2004.

[12] Ashiq Khan, Toshihiro Suzuki, Motonari Kobayashi and Masanori Morita Research Laboratories, NTT DoCoMo, Inc, Japan, “Packet Size based Routing for Route Stability in Mobile Ad-hoc Networks” The 18th Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, 2007.

[13] Nhy Nguyen Tu PHAM, Yiyuan DIAO, Yusuke KATO, Kenichiro YAGURA, Yumi TAKAKI and Chikara OHTA Faculty of Engineering, Kobe University, Kobe City, Japan , “A Simple Approach on Mitigating the Gray Zone Effect to Improve Throughput in IEEE802.11 based Ad-hoc Network” Second International Conference on Advances, 2009

[14] Scalable network Inc.
http://www.scalable- newtwork.com/