Interference-Aware and Fault Tolerant Multipath Routing Protocols for Mobile Ad Hoc Networks
Er. Suhail Ahmad Ganie1, Mrs. Nidhi Sharma2
Department of Computer Science Engineering
Swami Devi Dyal Institute of Engineering and Technology, Golpura, Barwala, Panchkula, India

Abstract:
Routing in MANETs is interesting and challenging problem studied by the community due to the dynamic nature of the infrastructure present in MANETs and due to nodes joining and leaving the network. In routing, the transmission of data from one node to another is direct only if the source and destination nodes are neighbors and if they are within the wireless range of each other. On the same, the transmission is indirect in case of the source and destination nodes are not in the range of operation to each other and that are not neighbors. In case of indirect transmission, routing is achieved only through multiple hops, with the help of intermediate nodes that comes as neighbors to the source and the destination nodes which serves the purpose of routers for relaying the information in between these source and sink nodes. In multipath routing, a number of redundant packets are sent along different paths between a pair of source-destination nodes. This redundancy will increase the reliability in the transmission of the information, which implies that there is a much greater chance (than in unipath routing) that at least one of the paths are able to deliver the packet successfully to the destination. The multipath routing will further ensures the success as a fault-tolerant routing algorithm which provides route resilience when there are route failures in the network by sending the redundant packets. However, the major disadvantage of multipath routing is that when redundant packets are sent through different routes, it will introduce an unnecessary overhead in the network’s bandwidth requirement which will consume more battery power for transmission of redundant packets. This disadvantageous is considered when we take into account the fact that energy-efficiency is an important concern in wireless ad hoc networks, because most mobile nodes in such environments works based on battery power and resource constraint.

Keywords: MANET, AODV, Node Disjoint Path, LS-AOMDV

I. INTRODUCTION
Wireless network refers to any computer network that is not connected by any type of physical links. The IEEE 802.11 standard specifies two operating modes of wireless network: infrastructure mode and ad hoc mode. Infrastructure mode is used to connect computers with wireless network adapters to an existing wired network with the help of wireless router or access point. Ad hoc mode is used to connect wireless clients in a peer-to-peer fashion [2]. The Ad-hoc On-demand Distance Vector (AODV) routing protocol is a reactive on-demand routing protocol. It consists of two phases: route discovery and route maintenance phases. However, it does not utilize multiple paths. When the route disconnects, the node which has detected the link failure will send a wrong message to the source node to restart the route discovery, or the routediscovery will restart by itself [3]. Communicating nodes in a Mobile Ad hoc Network usually seek the help of other intermediate nodes to establish communication channels. Thus, the communication may be via multiple intermediate nodes from source to destination. High level routing protocols are implemented over a suitable topology. All nodes connected in a network must act as routers to have accurate delivery of data packets. Routes contain links which is the connection between two nodes. The route quality is influenced by change in link quality. A varying link route does not produce good results. The network layer has received a notice when working on Mobile Ad-hoc Network. Therefore plenty of routing protocols in such network with different objectives and with different specific needs have been proposed. As a matter of fact, the two vital operations at the network layer are data forwarding and routing. Data forwarding controls how packets are taken from one link and put on another. Routing finds out the path which the packet must follow to reach the destination from the source. Routing protocols can be divided into single path and multi-path based on the number of routes discovered [6]. However, backup routing protocols have to face the problems of transmission collision and contention, waste of node resources, which are caused by the additional traffic incurred by the backup strategy and node choice policy [3]. The traditional AODV protocol is vulnerable to the well known black hole attack. Traditional black-hole has little effect on multipath AODV. In case of multipath routing, when one path is affected by black-hole attack, then source node can choose another alternative path to send the data packets. So, in this paper we will introduce a new type of black-hole attack mainly for multipath AODV. To the best of our knowledge, we have not found any black-hole attack which is specifically, targeted for multipath AODV. Usually black-hole attack has been developed for single path AODV and the same concept is used for multipath routing. In our proposed attack, the attacker does not damage a single route; rather it waits for a number of alternate routes to be established and then attempts to damage all these routes in a single attempt [1].
II. LITERATURE REVIEWS

ChaitaliBiswasDutta et al in [1] proposed blackhole attack, the attacker looks for nodes through which many alternative paths of multipath AODV passes through. Such nodes are selected and blackhole attack is launched targeting them, thereby damaging more number of paths in a single attempt. Further, the attacker selects only those genuine nodes through which many alternative paths of multipath AODV passes through. Such nodes are selected and blackhole attack is launched targeting them, thereby damaging more number of paths in a single attempt. Further, the attacker selects only those genuine nodes through which many alternative paths pass through, thereby facilitating the attacker to use less number of nodes. So the attack scheme is power aware. Finally we also propose IDS to detect the proposed energy aware blackhole attack. NS2 experimental results show the validity of the proposed attack.

ChaitaliBiswasDutta et al in [2] proposed a new type blackhole attack mainly targeting multipath AODV. To the best of our knowledge there is no blackhole attack which specifically targets multipath AODV. Broadly speaking, in the proposed blackhole attack, the attacker looks for nodes through which many alternative paths of multipath AODV passes through. Such nodes are selected and blackhole attack is launched targeting them, thereby damaging more number of paths in a single attempt. Further, the attacker selects only those genuine nodes through more than a threshold number of alternative paths pass through, thereby facilitating the attacker to use less number of nodes. So the attack scheme is power aware. NS2 experimental results show the validity of the proposed attack.

Liu Yujun et al in [3] proposed a new improved protocol AODV-BRL to increase the adaptation of routing protocols to topology changes by modifying AODV-BR. In AODV-BRL, the alternate routes are created by the Extended Hello Message as well as RREP packets. Then the Extended Routing Table and the least hop count first (LHF) are proposed to determine the optimal alternative route that significantly reduces the distance between the repair node and the destination. Finally, the performance improvement is evaluated by simulations. According to simulation results it is evident that compared with AODV-BR and AODV, AODV-BRL has a higher packet delivery ratio and lower routing overhead.

Faizalqbalet al in [4] investigated a variety of existing single and multi-radio routing metrics to analyze their limitations in finding multiple reliable paths around interfering neighborhood. The paper thus proposes a Diversity based Multipath Routing Metric (DMRM) which basis its calculation on diverse wireless network conditions. The routing metric not only captures interfering traffic load on the link but also considers link loss ratio, inter and intra-flow interference, multiple data rates of nodes and channel diversity during multipath selection. DMRM integrates multiple routing conditions to overcome the limitations of existing metrics. The proposed metric is integrated with Diversity-based Multipath Routing Protocol (DMRP). DMRP is designed to select optimal path in terms of packet delivery ratio, lower level of interference, fewer congested links and multipath load balancing to achieve higher throughput and reduced end-to-end packet delay.

ChannabasayyaMathad et al in [5] designed a new fault tolerant routing algorithm called Fault Tolerant Multipath Routing Protocol (FTMRP), which adds the fault handling ability to the multipath routing protocol. The result of this algorithm is simulated using NS2 and compared with existing Ad hoc on-demand multipath distance vector routing (AOMDV) protocol to show the enhancement in performance.

Hrishabha Raj Jainet al in [6] proposed approach contains an adaptive technique in which the proposed scheme is more energy efficient. The filtering forwarding scheme slows down the spread of excessive RREQs originated by a node per unit time and with success prevents Denial of service attacks. This paper planned multipath extensions of AODV routing protocol and a security improvement against We compared results of AODV routing protocols in attacked condition and after applied our algorithm and enhance the results exploitation multipath scheme for AODV. We used ns-2 to simulate. Simulation results show that the energy consumption of network is less after applying our proposed algorithm and our Network gets more stable and that proposed technique has better packet delivery ratio and improved throughput.

Eman S. Alwadiyehet al in[7]proposed routing protocols have a higher delivery rate and higher throughput compared with the ones in Split multipath routing protocol (SMR). The significant improvement in packet delivery ratio resulted mainly from reducing the impact of hidden terminal problem. While, increasing the number of available channels between the selected disjoint routes is the main reason for the dramatic improvement in throughput. The efficiency of the proposed protocols and SMR protocol is evaluated by GloMoSim simulator.

III. DESIGN OF NEW FAULT TOLERANT MULTIPATH ROUTING PROTOCOL FOR MOBILE AD HOC NETWORKS

Mobile Ad Hoc Network (MANET) is a type of wireless network which are formed by a mobile nodes that work on the principle of cooperative agreement of mobile nodes. The characteristics of MANET are continuously changing infrastructures, no centralized network managers, no dedicated access points, no fixed base stations, not having a backbone network for controlling the network management functions, and there is a absence of designated routers for making routing decisions. All the nodes in MANETs are treated as equal in the environment and participate in the routing process by acting as routers for one another. During the transmission of data from one node to another, MANET requires several hops because of the limited wireless transmission range associated with the operation of the mobile nodes. The above described characteristics of MANETs, particularly those listed due to the mobility of the nodes in MANET environment, and the continuously-changing of the network infrastructure, influences several challenges in to this research area. Due to the continuously changing infrastructure, the routes that were highlighted as “best” will no longer remain as the “best” at a later time. Therefore, it needs to re-compute the routes continuously, implying that in such networks, there is no permanent convergence to a fixed set of routes. For the reason, any routing protocol operating on MANET environments should consider these research issues and challenges during the design of a new protocol for the system.
IV. INTERFERENCE-AWARE MULTIPATH ROUTING PROTOCOLS FOR MOBILE AD HOC NETWORKS

Mobile ad hoc networks (MANETs) are a multi-hop temporary autonomous system of mobile nodes with wireless transmitters and receivers without the aid of pre-established network infrastructure. Due to the dynamic nature of the network structure as well as limited resources, the efficiency of the existing routing protocols has become a critical and challenging issue and their performance might have a great impact on the network's overall performance. As found in literature, there were several attempts to handle different routing scenarios that focused on developing multipath routing protocols to distribute the traffic load on multiple node-disjoint routes. These researches aimed to enhance the existing routing protocols. Such protocols vary in their enhancements criteria such as load balancing, power saving or increasing the delivery ratio and throughput such as LS-AOMDV and NDM_AODV. However, the existence of interference between the multiple node-disjoint paths remarkably affects overall performance of MANETs by all means such as data loss, conflict, retransmission, channel share etc. Hence, it has been discovered that interference is one of the most important factors that have to be taken into consideration in developing such a multiple path disjoint scheme.

Carrier sensing range for any node is the range in which a node can receive signals but cannot appropriately decode them. For instance, when a node gets an access to the channel and start to transmit data, all other nodes that are located within its carrier sensing range will be interfered as shown in fig.2.

V. CONCLUSION

A wireless mobile ad hoc network is a research area with many difficult challenges in the design of routing and multipath identification. Mobility, constraint bandwidth, limited power and finally faulty operation of the path nodes. We focused mainly on increasing the delivery ratio and throughput in multipath routing schemes which used the concept of multipath routing in distributing the traffic load on multiple node-disjoint routes. We achieved it by reducing the impact of interference between the selected nodedisjoint routes. Single channel share and hidden terminal problem are the main consequences of interference that are discussed in this paper and are considered in the developed routing protocols. The developed routing protocols reduced the impacts of interference by detecting single channel sharing and hidden terminal problems between the selected disjoint routes, and thus avoiding the routes that cause them as much as can.

VI. REFERENCES


