Analysis and Research of routing protocols DSR, AODV, and MIL-STD-188-220C

Huiming Wu [a], Xuan Wang, Hao Li, Chenglin Miao

Department of Information Engineering, Academy of Armored Forces Engineering, AAFE, Beijing, China

[a]whmwhmwhm@hotmail.com

Keywords: Ad hoc; DSR; AODV; MIL-STD-188-220C.

Abstract. We study and analyze the conception, theory, advantages and disadvantages of three wireless self-organization network routing protocols: DSR, AODV and MIL-STD-188-220C; emulate these three routing protocols on platform NS-2, and make conclusion concerning packet delivery ratio, throughput, End-To-End (ETE) delay and jitter.

Introduction

Wireless ad hoc networks, since its evolving to serve the military communications in the 1970s, after four decades of research and development, has developed the practical usages. Wireless ad-hoc network is a self-organizing no center network, which can enable the communication between nodes by self-organizing of network in the absence of fixed network infrastructure (such as base stations, switches). It has a very broad application prospect in various fields. In this paper, we simulate the performance parameter index of three routing protocols DSR, AODV, and MIL-STD-188-220C at the NS-2 simulation platform, including the success rate of routing protocols packet transmission under different network load, network throughput, end peer-end delay and end peer-end jitter.

DSR Routing Protocol

The basic concept. DSR protocol uses source routing algorithm, in the headers, each data packet of given line has a complete and ordered list of nodes by which this packet will go through. Using the source routing can guarantee the absence of loop, the nodes of forwarding or listening packet can cache the routing data in packet for the later use. As the data packets to be transferred already contain the necessary routing data, the intermediate nodes do not need to save the routing information.

Establishment of routing and maintenance of routing. DSR protocol consists of two processes: the route establishment and route maintenance. The works of these two processes are on-demand. Routing establishment: When a node is to transmit the data to the destination node, it first will check whether it caches the route to the destination node. If there is a valid route, it will be used to send data. Otherwise, the source node will start the process of establishing the route. It broadcasts a route request packet, which includes the destination node address, a source node address and an ID. To detect whether the route request packet is received repeatedly, each node maintains routing request form saves the <Sid, Request id> of recently received route request packet. When the node receives a route request packet, check if in the routing request table has a corresponding item. If it has, it will discard this route request packet; otherwise, the node will check the route record of route request packet if exist this node, if any, discard the packet; otherwise, if the destination node if the route request packet is the node itself or if this node has a route to the destination node, this node structure route will reply the packet and reverse the routing record in route request packet for the use of route reply packet. If it cannot reply the routing answer packet, the node will add its address to the route record of the route request packet, and forward this information.

Route Maintenance: In DSR protocol, the maintenance of routing is on-demand, no need to broadcast regularly. Once a route is in use, route maintenance program will monitor the operation and convey the error message to the source node. If there is an error at an intermediate node in the path of

data packet transmission, a route error packet will be returned. When the source node receives a routing error packet, a new route establishment process will be triggered.

Summary. Advantages: (1) only need to maintain the routes of nodes it communicates with, reducing the protocol overhead; (2) using the route caching techniques to reduce the routing establishment overhead; (3) support for multiple paths to the destination node; (4) can correctly calculate the routes of non-bidirectional link. Disadvantages: (1) header of each data packet needs to carry routing information so the additional overhead of data packet is bigger; (2) flooding mode for route request message, the route request message of neighboring nodes may have transmission conflict and repeated broadcasting; (3) as a result of the routing cache, expired route will affect the accuracy of routing.

AODV routing protocol

The basic concept. AODV protocol is an on-demand routing protocol. In order to find a route leading to the destination node, the source node will broadcast a route request packet (RREQ), and the intermediate node will establish "reverse route" to the source node according to the RREQ message. The item destination node of the reverse route is the source node of RREQ broadcast, the node of next hop is the neighbor node to send RREQ to this node. And then, it will broadcast this packet to surrounding nodes. If the destination node receives the RREQ, it will reply route reply packet (RREP) to the source node, and RREP will be transferred along the newly established reverse route to the source node.

Establishment of routing and maintenance of routing. Establishment of routing: When a node needs to communicate with a node but there is no valid path, it will start the route establishment process. Node has two counters: node number and broadcast ID. Route request (RREQ) packet of source node broadcasts includes: source node address, source node number, broadcast ID, destination node address, destination node number and the number of hops. Source node address and broadcast ID are unique to determine RREQ packets. When the source node sends another new RREQ packet, add 1 to ID. When the RREQ packet reaches the destination node or, saves an intermediate node of valid route to the destination node, the node will respond with a route reply (RREP) packet. When the RREP packet returns along the reverse path, each node in this path will built the front route items, record the latest serial number of the destination node, and the survival time of the routes reach the source node. The reverse routing which is established at the nodes not in return routing of RREP packet will be deleted because of a timeout. As the RREQ packet uses the route established with RREP packet, the AODV protocol only supports two-way link.

Route Maintenance: there are two ways of Route Maintenance for AODV routing protocol: reconstruction and local recovery of source node routing. The link interrupt between the node and a neighbor node will invalidate all routes using this link, so it's needed to notify all affected source node, by broadcasting the error message within one hop by the node detected interrupt. Node will first determine whether itself will be affected, set the corresponding item invalid, if the node has upstream node, continue to broadcast this message, otherwise, discard the packet. Another is the route recovery directly by intermediate node. When the intermediate node detects link interrupted, it will cache data streams and simultaneously send route request. When the destination node receives the request, it will answer the route reply and route recovery is successful; otherwise, if no route reply is received within a certain period of time, the route failure message will be reported to the source node, and the source node will take necessary actions.

Summary. When the network has less communication nodes, the control overhead and node memory overhead are smaller than that of the proactive routing protocol, and the response to the link break is more quickly, with certain extensibility. But the disadvantage is the bigger routing setup delay. AODV routing protocol uses route caching technology, any intermediate node can return the routing information to the source node; reporting link interruption information in time and rapid rebuilding the route can reduce the routing setup delay. In addition, AODV protocol only supports two-way link.

MIL-STD-188-220C routing protocol

The basic concept. MIL-STD-188-220C (hereinafter referred as 220C) , standard of US CNR (Combat Net Radio), which is designed to meet the needs of battle and tactical communication mobility, is a result of typical applications of the Ad hoc network in military communications.

220C protocol uses algorithm of source orientation relay routing based on the distance vector. Each node of the network, when enters the network, will maintain one list of distance vector between this node and all nodes of the entire network. Each item of the list contents of six-membered group (destination node, predecessor node of destination node, hops, overhead, and relay, silent). When the network topology changes, routing information only exchanges between the neighboring nodes of one hop. When to transmit data, the source node of the network will choose the most economical route according to the Intranet address of the destination node to and send data packets. The sent packet contains the complete route information needed to reach the destination node. In transit, the intermediate node will choose next relay node or destination node, according to the routing information at head of Intranet information in the received packet, and forward the packet. Between the internal nodes of 220C network, the topology information is exchanged by the topology updates and topology updates request message. When a node broadcasts topology update information to its adjacent nodes, its distance vector list will be copied to the topology update packet.

Sparse routing trees and topology updates. Sparse routing trees and sparse routing tables. Exchanging the entire routing trees table provides complete topology information, but will also make the data amount of routing trees very big. Therefore, that is transmitted between neighboring nodes should be a smaller copy of a complete routing tree (sparse routing tree). To reduce the number of branches of the routing tree, some paths leading to duplicate nodes in the routing tree should be deleted according to the following rules: keep only the shortest path from the root node to another node; keep no more than two paths with the same length from the root node to another node.

Conditional triggering for topology update process. Because of the obvious table-driven 220C protocol, the frequent exchanges of routing topology information would be a waste of valuable radio resources. At 220C protocol, conditional triggering is used to update the network topology and topology update requests.

Trigger condition of topology update: node I detects a link failure which is connected to a non-static node; node I detects a new or recovered link which is connected to a non-static node; node I detects link quality changes - only applicable in the link overhead; node I receives topology updates information from another node which modified its sparse routing tree; node I changes its silent mode and hopes to broadcast this change; node I modifies its relay capability state; node I receives a topology update request.

Trigger conditions of topology update request: ID of topology update does not match to the previously stored value; once data link transmission is detected from neighboring nodes previously unknown.

In order to prevent the frequent exchanges of network topology information in a network with dramatic topology changes, 220C states: topology update message cannot be sent more than once in each "MIN_UPDATE_PER". Topology update request message can be sent at most once in every "MIN_UPDATE_PER / 2". When some node is waiting for "MIN_UPDATE_PER" timer overflow, the allowed number of requests sent to this node is 2. "MIN_UPDATE_PER" is in minutes, and will be set by the network administrator when nodes configuration is finished. "MIN_UPDATE_PER" is 0 to disable the transmission of topology update message.

Simulation results

With simulation software NS-2, the following environment is configured to see the performances of AODV, DSR and 220C routing protocols at different network loads and different network topology change frequency: 36 nodes evenly spaced in 150m x 150m, MAC and physical layers use protocol

802.11, service CBR, 512 bytes per packet, transmission interval (0.001,0.01,0.1,1,10s), ideal channel with no fading.

Success rate of packet transmission. As can be seen from Figure 1, the success rate of packet transmission of three routing protocols will reduce with the increase of the network load. In the light load network, AODV has the highest packet transmission success rate, while 220C has the lowest; in the heavy load network, 220C has the better packet transmission success rate than AODV and DSR.

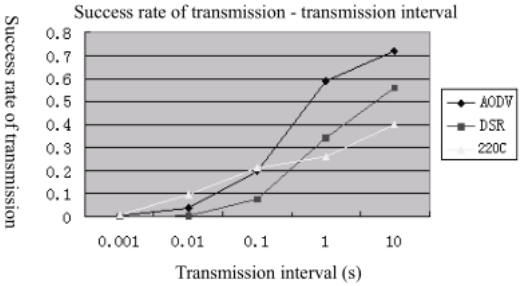

Figure 1 Comparison of packet transmission success rate

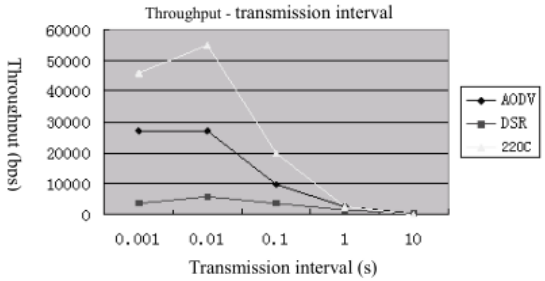

Figure 2 Comparison of Throughput

Throughput. It is apparent from Figure 2 that, the throughputs of three routing protocols are quite different, 220C has the biggest throughput, followed by AODV, and DSR has the smaller. Throughput differences in heavy load network are particularly evident.

End peer-end delay and jitter. For many multimedia applications, not only need the bearer network to provide error-free transparent transmission, but also need to meet user requirements for the subjective experience of multimedia applications such as delay and jitter of voice and video, the parameters of which are the smaller the better.

As can be seen from Figures 3 and 4, regardless of the heavy or light load of network, 220C protocol are able to guarantee lower latency and jitter. The performance of DSR is unsatisfactory with the delay of more than two seconds.

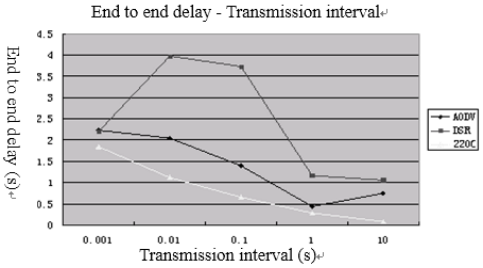

Figure 3 Comparison of end to end delay

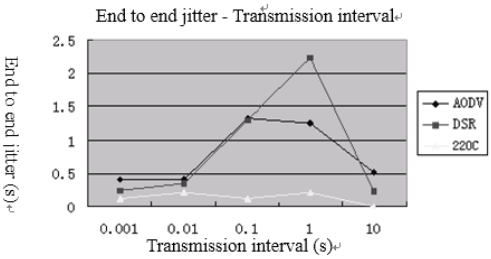

Figure 4 Comparison of end to end jitter

Conclusion

In this paper, we analyzed three kinds of routing protocols of wireless ad-hoc network, and realized simulation tests about 3 aspects: success rate of packet transmission, throughput and end to end delay and jitter. Through the analysis we can see the advantages of MIL-STD-188-220C.

References

[1] Standard of Interfaces for Subsystem of Digital Information Transmission Device (C version) MIL-STD-188-220C. Translated by Seventh Research Institute of China Electronics Technology Group Corporation. (2003)

[2] Practical Tutorial for Wireless Ad Hoc Network Technology. Tsinghua University Press, Beijing

[3] Xu Leiming, Pang Bo, Zhao Yao, NS and Network Simulation, Posts & Telecommunications Press, Beijing (2003)