STUDY OF ROUTING PROTOCOLS FOR JAMMING IN WIRELESS NETWORKS

Seemanaaz sharif khan
Dept.of E&TC, NBN Sinhgad school of engineering, Pune, India
seemanaazkhan150@gmail.com
Prof. Sharad Sawant
Assistant Professor, Dept. Of E&TC, NBN Sinhgad school of engineering, Pune, India
sharad.sawant@sinhgad.edu

ABSTRACT

In mobile wireless network routing protocol is important as per the performance is considered. In wireless networks nodes are self organize and acts as both system ends and as intermediate systems. Here basic problem is connectivity and nodes moving out of range from one another. Routing has received more attention from recent literature because dynamic behaviors of these networks have many technical challenges on the design of an effective routing scheme. In multiple paths routing total traffic is divided between available paths. In this article, we focus on the problem of jamming in wireless network where source nodes are used to perform traffic allocation on the basis of statistics of portfolio theory. Here we also study the different routing protocols used in wireless networks such as MPDSR, DSR, DSDV, AODV etc.

KEYWORDS: DSDV, DSR, MPSDR, AODV

INTRODUCTION

In data transport through the network jamming creates bad effects on point to point network or mesh type network. Out of six layers of TCPIP jamming is found at physical layer and its effects are found on all the layers. The simple solution to avoid jamming at physical layer is to spread the available spectrum due to which jammers need more resources to reach the destination node. Some jammers use cross layer protocol for jamming attacks which will target on link layer, error detection and correction protocol. Hence for higher layer protocols we have to build strong anti jamming techniques. Diversity is taken in to consideration while designing the anti jamming techniques. The main classes of routing protocols are Proactive, Reactive and Hybrid. A Reactive (on-demand) routing strategy is a popular routing category for wireless ad hoc routing. Using multiple-path variants of source routing protocols such as Dynamic Source Routing (DSR) or Ad-Hoc On- Demand Distance Vector (AODV), for example the MPDSR protocol, each source node can request several routing paths to the destination node for concurrent use to make effective use of this routing diversity. In this paper, we consider multiple path routing protocols based on anti-jamming diversity.

ROUTING PROTOCOLS

In this section we present background information about multiple path routing protocols and describe them such as DSDV,DSR ,MPDSR ,AODV.

A. DSDV

The Destination-Sequenced Distance Vector (DSDV) algorithm uses distance vector routing method which uses mobile nodes cooperate to form an ad-hoc network. It is a table driven proactive protocol which maintain a routing table with entries for all nodes in the network and not just a neighbors of nodes that is one for each destination within the ad-hoc network. One advantage of doing this is routes to any destinations are ready to use when needed.
DSDV is effective for creating ad-hoc networks for small populations of mobile nodes. The advantage here is that a smoothly functioning ad-hoc system with on-demand routes could largely eliminate the need for periodic broadcast of route advertisements. With the goals of minimizing broadcasts and transmission latency when new routes are needed.

B. DSR

The dynamic source routing protocol (DSR) is a simple and efficient routing protocol designed for wireless ad-hoc networks of mobile nodes. It is on demand source routing protocol based on concept of source routing. It is self organizing and self configuring protocol. Here the concept of route discovery and route maintenance is used.

In route discovery source node want to send packets to destination nodes and obtain a source route. When route is broken from source to destination it is indicated by route maintenance and then source try to attempt to use any other route to destination. This protocol first allows nodes to discover the path from source to destination and then try to maintain that path. Route discovery and route maintenance work entirely on demand. It is loop free protocol which avoids intermediate nodes to get up to date all the time. Number of intermediate nodes needs to reach any destination may change hence final network topology is rapidly changing and quit rich in number of nodes. In DSR source routes are dynamically discovered. It supports inter-networking between different types of wireless networks.

C. MP-DSR

Multiple path dynamic source routing protocol referred as MP-DSR. It provides soft Qo with respect to end-to-end reliability which is based on link availability and path reliability model. This protocol finds multiple disjoint paths for transmission of data. Disjoint path means when two paths say P1 and P2 consist of common source and destination nodes but they are having different intermediate nodes. In MPDSR data transmission fails only when all disjoint paths are fails at the same time. Hence here probability of failure of data transmission is less. In MPDSR during route discovery end to end reliability (P_u) is required. End to end reliability means probability of having successful data transmission between two mobile nodes. Its value lies between 0 & 1. In this protocol for route discovery we need two parameters which are number of paths to be discovered (m_0) and lowest path reliability (Π_{lower}) which satisfy the end to end reliability. When there are fewer paths available between sources a destination that is low m_0 at that time reliability of paths is more which means value of Π_{lower} is high, which means both the parameters are inversely proportional to each other. Source node sends route request message to all the available nodes to search all the available paths. When intermediate nodes receive this message it will check the path reliability requirements. If route request message does not meet this requirement node will reject this message. But when nodes fulfill the requirement then it will forward multiple copies of this message to neighboring nodes. Number of copies of messages is equal to number of neighboring nodes. When destination node receives this request message it will send route reply message to the source node and will create a path from source to destination.

D. AODV

Ad-hoc on demand distance vector routing uses collection of mobile nodes. Each mobile host works as a specialized router and routes are available on demand means only when needed. This protocol is suitable for dynamic self starting network which is loop free network. For route discovery AODV uses broadcast mechanism only when needed. It maintains route table entries for intermediate nodes which is dynamically varying. A node does not have to discover and maintain a route until the two nodes want to communicate where the previous node provide the services as a intermediate forwarding station to maintain connectivity between two other nodes. For path discovery each node has to maintain two separate counters a node sequence number and its broadcast id. Source node broadcast the route request message to its neighboring nodes. This request message contains source address, broadcast id, source sequence, destination address, destination sequence & hop counter. When any neighboring node satisfy route request it will send route reply message to the source node. When it will not satisfy then it will rebroadcast the request to neighboring nodes and will increase the hop counter. If node cannot satisfy route request message it keeps track of destination address, source address, broadcast id, expiration time for reverse path route entry, sequence number of source node so that it implement the reverse path setup. The purpose of route request expiration time is to separate the routing entries of reverse path from those who do not lie on source destination path. This time is depending on size of the network. Each routing table maintains the address of active neighbors. Neighbor is said to be active if it originate at least one packet for the destination. A mobile node maintains a route table entry for each destination of interest. Each entry of route table contains destination, next hope, number of hopes, destination sequence number, active neighbors and expiration time for route table entry. When new route is found it will compare the destination sequence number of previous path and new path and the route having greater sequence number is being selected.

JAMMING

It is an attack on wireless network which is related with radio frequencies. It disturbs the whole network by inserting some jamming nodes which are less than available nodes in the network. When network uses single frequency then this type of attack is simple. Constant jamming will not allow nodes to exchange data and they are not able to report the attack to remote monitoring network. Jamming is the attack on the physical layer of the network. Jammers are used to avoid enemy's wireless communication in battlefield whose purpose is to generate noise and bring down the other party's network.

A. SIMPLE PERIODIC JAMMING

In simple periodic jamming jam is created by creating periodic noise pulses. Its performance is better than other jamming techniques like intelligent jamming and trivial jamming. Simple periodic jamming is divided in different sections such as continuous low power jamming, burst high power jamming and busy jamming. To make network non operational simply insert periodic noise pulses at lower power levels. This jamming considers jamming power, pulse width and silence width. Total power is product of jamming power, number of pulses and pulse width. When there is no jammer then throughput decreases slightly.

B. INTELLIGENT JAMMING

This jamming will corrupt the control packets and reduces the throughput to the zero level. When control packets are corrupted no data is being transferred. This jamming is more power efficient. Control packets such as ACK, CTS, and DIFS are destroyed.

1) When medium is idle for DIFS duration then node have permission to access the medium once. When busy medium is found busy then nodes again have to wait for DIFS time and then it will select random time with in available window and it will add additional delays for the access of random amount of time.
2) When the idle channel is sensed by two stations then both these stations will send the data to that idle channel and because of this collision will occur at the receiver side. After waiting for DIFS time sender will get the RTs(Ready To Send) packets. RTS will include receiver data and time required for a data transmission. The node which receives the RTS packet will allot a NAV (Network Allocation Vector).
3) In CTS corruption jamming, jammer waits for RTS packets. After receiving this packet jammer will count down for SIFS duration and allot a short jamming pulse which will destroy the CTS packets.
4) In ACK corruption jamming, when jammer senses the DATA packets it will start to count down at the end of this packet for SIFS duration. After this it will send a jamming pulse of small duration which will corrupt the ACK packet. As ACK is not received by sender it will keep sending the data to the receiver node. And after a limit of TCP transmission is over sender will give up.
5) In DATA corruption jamming, when CTS packets are sensed it wait for SIFS time and insert a short duration of noise pulse and DATA packets are get corrupted.

ANTI JAMMING TECHNIQUES

Jamming strength is calculated by a jamming to signal ratio which is given by

$$\frac{J}{S} = \frac{P_j G_{jr} G_{rj} R_{tr}^{\ 2} L_r B_r}{P_t G_{tr} G_{rt} R_{jr}^{\ 2} L_j B_j}$$

Where P_j is power of the jammer, G_{jr} is antenna gain, Grj: antenna gain from receiver to jammer, Rtr: distance from transmitter to receiver, Lr: communication signal loss, Br: communications receiver bandwidth, Pt: transmitter power, Gtr: antenna gain from transmitter to receiver, Grt: antenna gain from receiver to transmitter, Rjr: distance from jammer to receiver, Lj: jammer signal loss and Bj: jamming transmitter bandwidth.

1) In transmission power level, jamming to signal ratio is reduced for that we have to increase transmission power level. This method is less efficient.
2) In spread spectrum method, jammer will spend more energy than the sender. For this we have to force the jammer to jam for large frequency bands than the receiver bandwidth. it spread a pseudo random sequence

over a frequency of band. To dispread the sequence we have to correlate the sequence with receiver signal.

3) In directional antenna technique, antenna gain is reduced from jammer to receiver. For this purpose we have to use sectored antenna or the antenna which will create a beam of reception on the transmitter.

REFERENCES

1] D. J. Thuente and M. Acharya, "Intelligent jamming in wireless networks with applications to 802.11b and other networks," in Proc. 25th IEEE Communications Society Military Communications Conference(MILCOM'06), Washington, DC, Oct. 2006, pp. 1–7.

2] A. D. Wood and J. A. Stankovic, "Denial of service in sensor networks," IEEE Computer, vol. 35, no. 10, pp. 54–62, Oct. 2002.

3] R. Leung, J. Liu, E. Poon, A.-L. C. Chan, and B. Li, "MP-DSR: A QoSaware multi-path dynamic source routing protocol for wireless ad-hoc networks," in Proc. 26th Annual IEEE Conference on Local Computer Networks (LCN'01), Tampa, FL, USA, Nov. 2001, pp. 132–141.

4] Patrick Tague, Sidharth Nabar, James A. Ritcey, and Radha Poovendran,"Jamming-Aware Traffic Allocation for Multiple-Path Routing Using Portfolio Selection," ieee/acm transactions on networking, vol. 19, no. 1, feb 2011.

5] I. F. Akyildiz, X. Wang, and W. Wang, "Wireless mesh networks: A survey," Computer Networks, vol. 47, no. 4, pp.445–487, Mar. 2005.