Computer System Engineering

Design Project 2 Executive Summary

Ad-Hoc Wireless Network

Author:
Bo Song 11302010003
TianHao Wang 11302010005
XiaoBin Xu 11302010008

June 8, 2013

1 Introduction

2 Design Description

The design is partitioned into two parts, since the link layer is simple, we give the algorithm part in the network layer, and the protocol part in the end-to-end layer.

2.1 Routing Algorithm

In this section, we give our routing algorithm in the network layer. We first describe the data structure, that is, what we add in the header and tailer of the packet. Then we describe how the algorithm works.

2.1.0 Some Terms

We define the base station as node D, the handheld device which is about to send information as the node S. As mentioned in DP description, every handheld device has the location information of base station. Then we define a predefined constant P.

2.1.1 Data Structure

message meta data:
origin source time ok node list path node list id
message content: image(optional) and origin source location information

2.1.2 Adaptive Effective Zone Algorithm

In order to let messages reach the base station and maximize the throughput, we adopt a location based algorithm instead of brute force algorithm to broadcast messages.

The description mentioned below only focus on the whole process of routing and ignore the detail of other things such as reliability, security issues etc.

1. S invoke the predefined scan() function to get a list of tuples (node, loss_prob), for the sake of improving effectivity, then S chooses those nodes whose loss_prob is lower than P, and who is not in the origin path.

2. S broadcasts a message which has an unique ID to nearby nodes. The message contains the location information of S, a list which contains nodes chosen in Step1, the content information which contains location information of origin source node(here is S) or image information.

3. If node A receives the message sent by S, the first thing is to check whether the message has been sent from A, and discard it if it has. Then, check whether S wants A to broadcast the message by checking the node list. If not, discard it, too.

4. Then A calculates whether A is in the effective zone calculated using the location information of the sender and the base station, if A is not in the effective zone, discard it. Otherwise it rebroadcast the content message along with updated mete data as S does and invokes receive().

5. If all things go well, after the iterative processes of Step 1 to 5, the message will reach D with relative small number of hops.

2.2 Transfer Protocol

2.3 Different Reliability

2.3.1 Basic Lost Handling

In our location based algorithm, many nodes discard the packet for the sake of improving throughput. As a result, there will be a problem that S can not reach D through the nodes in the effective zone. Therefore, we need a basic mechanism to handle such problem along with the lost problem in send or receive process.

If the sender S does not receive confirm information carried by receive() function for a while, there are two possibilities:1. 2. (rebroadcast cast for first several times and then expand effective zone gradually)

2.3.2 Burst Mode

location information 5min, accelerate the frequency of rebroadcast

2.3.3 Image Reliability

try to send most recent image to base station

2.4 Malicious Nodes Handling

Nodes in the system should distinguish malicious nodes by some strange behavior, so we classify different kinds of malicious nodes and handle it separately.

Type One

the malicious node hear a legitimate message, then broadcasts many copy(such as one million) of this message pretending it received it from the source.

How to handle We add a counter to every node. When a node receive abnormal number of messages of one sender, the node can mark sender as a malicious node and discard message from it.
In this situation, we effectively prevent the millions copies of message from propagating forward to the whole system. However, nodes around the malicious node will suffer millions of connections till the malicious node stop sending, so these nodes will lose the ability to receive other messages. The only thing we can do to handle this relative small problem is send warning message to the base station or the other people to handle the malicious node in physical way.

Type TWO

The malicious node A receive a message, send the receive() function to the sender but stop forward the message and the sender will consider A will do its job as usual.

How to handle Under most situation, it is not a big problem since other nodes around sender will do their job as usual.
However, when all valid nodes(in effective zone and low lost probability) around sender are malicious node, the sender can not send message to the base station. We will disscuse it further in our report.

Type THREE

The malicious node change the message and send forward to the base station.

How to handle The method is easy that encrypt the message, but how to implement it correctly and prevent malicious node decrypt is a difficult theoretical problem and we will not discuss here.

3 Conclusion

Word Count:2483(exclude title page)