Development of Reliable Multihomed Scatternet Network

R.Dhaya, Dr.V.Sadasivam, Dr.R.Kanthavel

Lecturer, National Engineering College, Kovilpatti, Tamilnadu ,India.

Professor, M.S.University, Tirunelveli, Tamilnadu, India.

Teaching Research Associate, Govt. College of Engineering, Tirunelveli, Tamilnadu, India.

***Abstract*— Since wireless networks are movable and flexible, the conventional protocols are standing behind fault tolerance problems. A new Stream control transmission protocol (SCTP) is a transport layer protocol which is reliable, message-oriented data transport protocol that supports multiple streams to prevent head-of-line blocking and multihoming for end-to-end network fault-tolerance. A host is multihomed if it can be addressed by multiple IP addresses. SCTP multihoming allows connections, or associations to remain alive even when an endpoint's IP address become unreachable. In a multihomed host there will be at least two IP addresses. SCTP uses one IP for a primary path and the other IP for secondary path. Initially, SCTP uses the primary path for transmission of data. If the primary path fails then the secondary path is chosen for further transmission. Similarly if the secondary path fails then the primary path is chosen for further transmission. On the other hand Bluetooth Scatternet refers to a collection of Bluetooth piconets. The proposed Bluetooth Scatternet system uses the multihoming concept of SCTP for effective fault tolerance during data transmission.**

Keywords: Multihoming, Scatternets, Piconets,Bluetooth.

I. INTRODUCTION

Bluetooth is a wireless protocol for exchanging data over short distances from fixed and mobile devices, creating personal area networks (PANs). It can connect several devices, overcoming problems of synchronization. Bluetooth uses a radio technology called frequency-hopping spread spectrum, which chops up the data being sent and transmits chunks of it on up to 79 frequencies. It can achieve a gross data rate of 1 Mb/s [2]. Bluetooth provides a way to connect and exchange information between devices such as mobile phones, telephones, laptops, personal computers, printers, Global Positioning System (GPS) receivers and digital cameras.

Bluetooth protocols assume that a small number of units will participate in communications at any given time. These small groups are called piconets, and they consist of one master unit and up to seven active slave units. The master is the unit that initiates transmissions, and the slaves are the responding units[13].

As with piconets, where multiple Bluetooth devices are able to connect with each other in an ad-hoc manner, so too can multiple piconets join together to form a larger network known as a scatternet [12]. Bluetooth devices must have point-to-multipoint capability in order to engage in scatternet communication, and several piconets can be connected to each other through one scatternet [4]. Furthermore, a single Bluetooth device may participate as a slave in several piconets, but can only be a master in one piconet.

II. PROPOSED SOLUTION

The main objective of this paper is to perform the simulation of SCTP in Bluetooth Scatternets which of course, is a wireless network. A Bluetooth Scatternet consisting of two piconets is established. Each piconet has one master and one slave. The slave called "Slave-bridge" connects the two piconets. "Connects" here means that this slave-bridge acts as the medium through which data transmission will take place between the two Masters. This suggests that whenever there is a path breakage, SCTP will automatically detect the path

failure and an alternate path can be used by means of heartbeat signals.

A. DEVICE DETECTION

In mobile ad hoc environments, devices initially have no information about their surrounding environment or the devices that operate within their range. There is no centralized instance to query about the environment. Therefore, a protocol must exist that provides means for detecting devices and enables devices to set up a connection, Bluetooth uses the Base band protocol for this task . Two procedures are used in the device discovery procedure; inquiry and page.

B. PROXIMITY PROCESS

In order to set up a connection, a device must detect what other devices are in range. This is the goal of the inquiry procedure. The process is initiated by the unit that wishes to collect device information or create a connection. To conserve power and coexist with other link activity, inquiry is always initiated by higher level control protocols. The inquiry procedure must overcome the initial frequency discrepancy between devices. Therefore, inquiry only uses 32 of the 79 hop frequencies [3]. Typically a device enters inquiry mode periodically. Similarly, a device that wishes to be visible to inquiring units enters inquiry scan in certain intervals. In order to find each other, one device must be in Inquiry state and one (or more) device must be in Inquiry Scan sub-state simultaneously.

C. CONNECTION ESTABLISHMENT

In Bluetooth the connection establishment is handled by the page process. The page process requires knowledge of the BD_ADDR of the device with which the connection is to be established. Furthermore the device being paged must be in Page Scan sub-state, i.e. listening for page messages. At the end of the page process a connection has been set up, the paging device becomes the master and the paged device becomes the slave. As with inquiry a device typically enters Page state periodically and a device that wishes to be able to connect to paging units enters page scan in certain intervals.

D. SCATTERNET USERCASE

In this scenario the mobile phone functions as both a master and a slave . In order for this to work, regardless of data speed, an effective scatternet implementation is required.

E. PICONET VS SCATTERNET:

A piconet is the type of connection that is formed between two or more Bluetooth-enabled devices. However, when a piconet is formed between two or more devices, one device is dynamically elected to take the role of 'master', and all other devices assume a 'slave' role for synchronization reasons. Piconets have a 3-bit address space, which limits the maximum size of a piconet to 8 devices ($2^3 = 8$), i.e. 1 master and 7 slaves [3]. A piconet allows one *master* device to interconnect with up to seven active *slave* devices (because a three-bit MAC address is used). Up to 255 further slave devices can be inactive, which the master device can bring into active status at any time. A piconet typically has a range of about 10 m and a transfer rate between about 400 and 700 kbit/s depending on whether synchronous or asynchronous connection is used.

A scatternet is a type of ad-hoc computer network consisting of two or more piconets. A scatternet is a number of interconnected piconets that supports communication between more than 8 devices . Scatternets can be formed when a member of one piconet (either the master or one of the slaves) elects to participate as a slave in a second, separate piconet. The device participating in both piconets is known as slave-bridge which can relay data between members of both ad-hoc networks. Using this approach, it is possible to join together numerous piconets into a large scatternet, and to expand the physical size of the network beyond Bluetooth's limited range.

III. EXISTING PROBLEM

Besides all the explanations mentioned above, SCTP still has some existing shortfalls. The existing problem is, however not involved with fixed network with

fixed hosts i.e., the normal connections that involves connections using cables. The existing problem is mainly with the manipulation of data transmission in fixed network with mobile hosts and with wireless networks [10].

Presently TCP is mainly used in wireless networks. But TCP does not support multihoming. It supports only one IP per host that greatly reduces the fault tolerance level of the connection. Also there is a great possibility for congestion to occur[11]. The same problem occurs when we use UDP as the transmission protocol.

Introduction

IV. STREAM CONTROL TRANSMISSION PROTOCOL

Stream Control Transmission Protocol (SCTP) is an end-to-end transport protocol that provides services heretofore unavailable from either of the workhorse transport protocols[9].

A. NEED FOR SCTP

TCP has performed immense service as the primary means of reliable data transfer in IP networks. However, an increasing number of recent applications have found TCP too limiting, and have incorporated their own reliable data transfer protocol on top of UDP [8]. The limitations which users have wished to bypass include the following:

- TCP provides both reliable data transfer and strict order-of transmission delivery of data. Some applications need reliable transfer without sequence maintenance, while others would be satisfied with partial ordering of the data [5]. In both of these cases the head-of-line blocking offered by TCP causes unnecessary delay.
- The stream-oriented nature of TCP is often an inconvenience. Applications must add their own record marking to delineate their messages, and must make explicit use of the push facility to ensure that a complete message is transferred in a reasonable time.
- The limited scope of TCP sockets complicates the task of providing highly-available data transfer capability using multihomed hosts.
- TCP is relatively vulnerable to denial of service attacks, such as SYN attacks. Transport of PSTN signalling across the IP network is an application for which all of these limitations of TCP are relevant[6] .

Two key problems surfaced in the use of TCP:

- **Head-of-line blocking** - a problem where sending independent messages over an order-preserving TCP connection causes delivery of messages sent later to be delayed within a receiver's transport layer buffers until an earlier lost message is retransmitted and arrives thus resulting in undesirable call setup failure[5].
- **Multihoming** - where a host with multiple points for redundancy purposes, does not want to wait for a routing convergence to communicate critical messages to its peer communication endpoint. For call control signalling, such delay is unacceptable when an alternate available path exists[1]. A TCP connection only binds a single point of attachment at either end point.

TABLE 1: COMPARISON OF SCTP SERVICES AND FEATURES WITH THOSE OF TCP AND UDP.

SERVICES/FEATURES	SCTP	TCP	UDP
Connection – oriented	Yes	Yes	No
Full Duplex	Yes	Yes	Yes
Reliable Data Transfer	Yes	Yes	No
Partial Reliable Data Transfer	Optional	No	No

Flow control	Yes	Yes	No
TCP Friendly Congestion Control	Yes	Yes	No
ECN Capable	Yes	Yes	No
Ordered data delivery	Yes	Yes	No
Unordered data delivery	Yes	No	Yes
Path MTU discovery	Yes	Yes	No
Message fragmentation	Yes	Yes	No
Message bundling	Yes	Yes	No
Multistreaming	Yes	No	No
Multihoming	Yes	No	No
Reachability check	Yes	Yes	No

SCTP monitors the paths of the association using a built-in heartbeat [7] as shown in Table 1; upon detecting a path failure, the protocol sends traffic over the alternate path. It's not even necessary for the applications to know that a failover recovery occurred.

V. EXPERIMENTAL WORKS :BASIC STRUCTURE OF THE PROPOSED SYSTEM

The experiment consists of:-

- Two Piconets, each with a Master and a Slave
- First Piconet consists of Master1 with two IP addresses: IP 0.1 and IP 0.2
- Second Piconet consists of Master2 with two IP addresses: IP 6.1 and IP 6.2
- Slave Bridge connects both the Piconets
- Primary path is (if node 1 is to be failed)
  - Master1 → IP 0.1 → Slave Bridge → IP 6.1 → Master2
- Alternate path is
  - Master1 → IP 0.2 → Slave Bridge → IP 6.1 → Master2
- Path for acknowledgement is
  - Master2 → IP 6.2 → Slave Bridge → IP 0.2 → Master1

A. WORKING OF THE PROPOSED SYSTEM

The main working of this paper is as stated above. According to the node selected, the primary path is assigned. For example, if we select node 1 to fail, the path 0→1→3→4→6 will be selected as the primary path. If we select node 5 to fail, the path 0→2→3→5→6 will be selected as the primary path. Similarly, the heartbeat also depends on the node to be failed. When we select the node to be failed, the heartbeat will start flowing through its complementary IP address of the corresponding host. For example, if node 1 is selected then heartbeat signals will flow through 3→2 and 2→0 (Node 2 is the complementary IP address for node 1).

Example 1:If node 1 fails, then the Primary path (0→1→3→4→6) will fail. This means that no data transmission can occur through the primary path. Now stop the heartbeat signals through 3→2 and 2→0. As soon as the heartbeat signals stop, data transmission will continue through the secondary path (0→2→3→4→6). Note here that only the IP address of the failure node is replaced with its complementary IP address (1 is replaced with 2), but not necessarily for the other host (4 is not replaced with 5). After all data transmissions are over, acknowledgement signals will be started from the Receiver (Master2) to the Sender (Master1) via Slave-bridge (6→5→3→2→0).

Example 2:If node 2 fails, then the Primary path (0→2→3→5→6) will fail. This means that no data transmission can occur through the primary path. Now stop the heartbeat signals through 3→1 and 1→0. As soon as the heartbeat signals stop, data transmission will continue through the secondary path (0→1→3→5→6). Note here also that only the IP address of the host that fails is replaced with its complementary IP address (2 is replaced with 1), but not necessarily for the other host (5 is not replaced with 5). After all data transmissions are over, acknowledgement signals will be sent from the Receiver (Master2) to the Sender (Master1) via Slave-bridge (6→5→3→2→0).

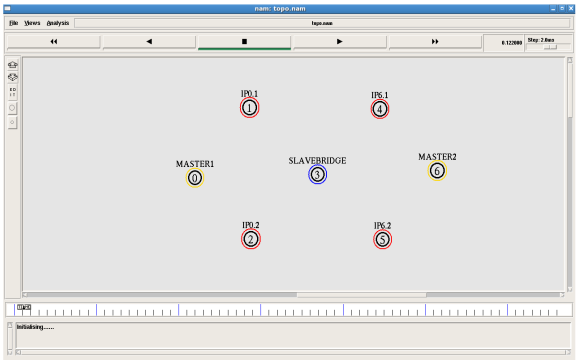

Fig 1: Proposed Bluetooth Scatternet with two piconets

Figure 1 shows our proposed network having two piconets. Node-0 and node-6 are the masters in each piconet. As we can see, the slave-bridge lies in the intersection of the two piconets. This means that it lies within the data transmission range of Master1 as well as Master 2. Note that from the piconets, Master1 and Master 2 are not in each others range for data transmission.Node-1 and node-2 are the IP addresses of Master1, node-4 and node-5 are the IP addresses of Master 2. Thus we have justified that both Master1 and Master 2 are multihomed. Data transmission takes place through one of the IP addresses of Master1, passes through the slave-bridge, and then reaches Master2 through one of its IP addresses. This is referred to as the "Primary path". When path breakage occurs, data transmission will take place by replacing the failed IP address with its complementary IP address of the corresponding host.

This is illustrated in the following algorithm proposed in figure 2:-

Step 1: Initialize the Bluetooth Scatternet.

Step 2: Start Data transfer through Primary Path.

Step 3: Start Heartbeat signals through alternate path.

Step 4: If Primary path fails-

- Stop Data transfer through Primary path.
- Search for alternate path using

Fig 2: Proposed algorithm

V. EXPERIMENTAL RESULTS

A. INITIALIZATION

Node 0 checks for other nodes which are within its range and is illustrated in Fig 3. Here Node 1, Node 2 and Node 3 are within the range of Node 0. So Node 0 can transmit data to these three nodes.

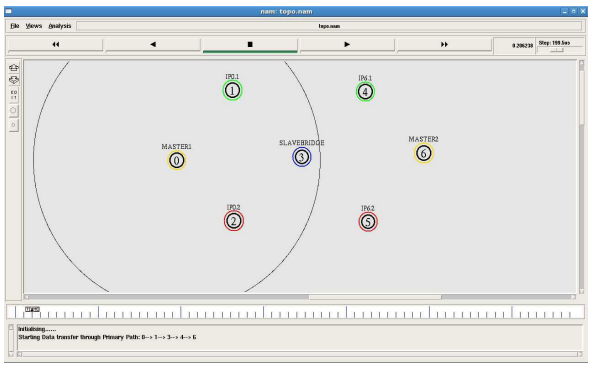

Fig 3: Node 0 inquires its neighbouring nodes

B. DATA TRANSFER THROUGH PRIMARY PATH

After initialisation the data starts transferring from the sender to the receiver through the Primary Path. Here the Primary Path is 0→1→3→4→6 as shown in the Figure 4. Here the Primary Path is 0→1→3→4→6 because the node to be failed is selected as Node 1.

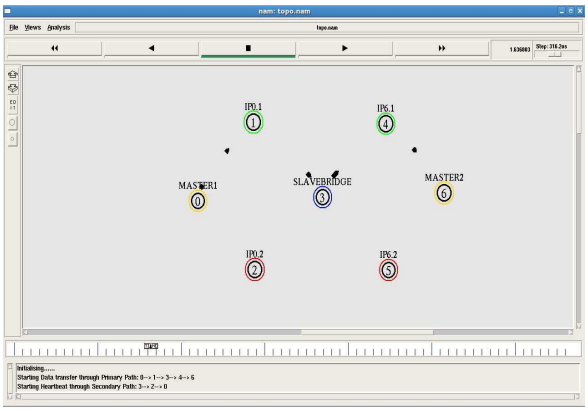

Fig 4: Data transfer through Primary Path

C. HEARTBEAT SIGNALS THROUGH 3→2 AND 2→0

After data starts transferring through the Primary Path the Heartbeat signals are sent through the paths 3→2 and 2→0 which is shown in Figure 5. The heartbeats check whether these two paths are alive or not. This is done because when the Primary Path fails these two paths will serve as the alternate path.

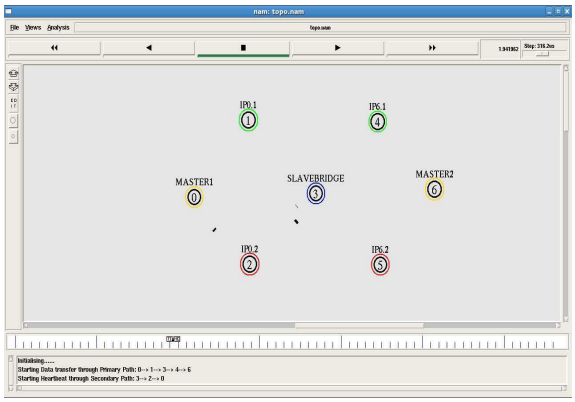

Fig 5: Heartbeat signals through alternate path

D. PATH FAILURE DUE TO NODE 1 (PACKET LOSS)

When data transfers through the Primary Path, there occurs a path failure due to Node 1 which results in Packet Loss in Node 1 and which is shown in Figure 6. Data can no longer transfer through the Primary Path.

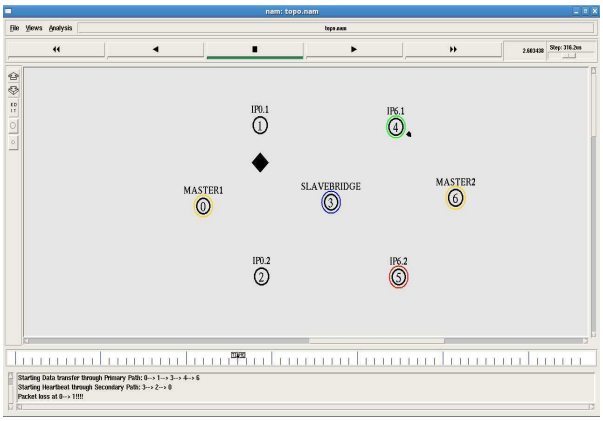

Fig 6: Path failure due to node 1

E. DATA TRANSFER THROUGH SECONDARY PATH

Due to the Primary Path failure, we cannot transfer any data through it. So we use the Secondary Path as shown in Figure 7 for transferring the remaining data.The Secondary Path transfers all the remaining data from the sender to the receiver. Here the Secondary path is taken as 0→2→3→4→6.

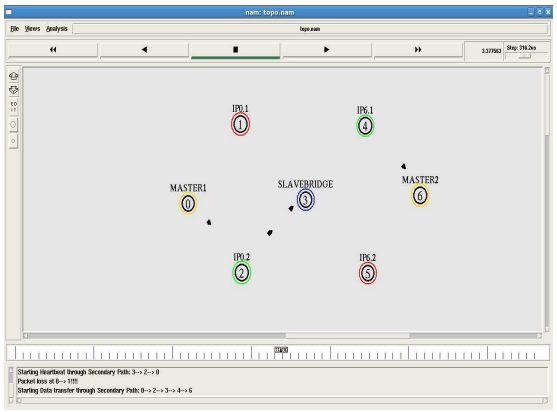

Fig 7: Data transfer through Secondary Path

F. ACKNOWLEDGEMENT FROM RECEIVER TO SENDER

After all the data transmissions are over, we send the acknowledgements through a separate path**.** This is illustrated in Figure 8. Here the path 6→5→3→2→0 is used for transferring acknowledgements from receiver to sender.

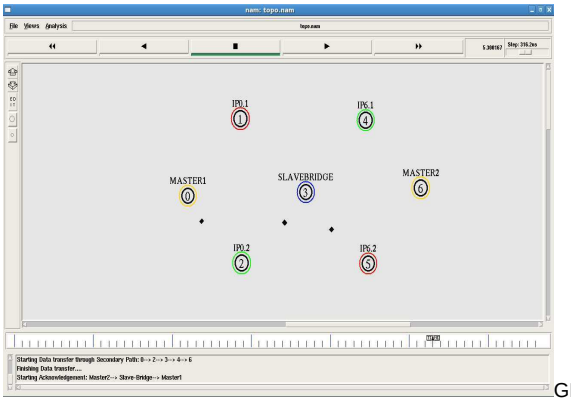

Fig 8: Acknowledgement from Receiver to Sender

IV. GE

G. X-GRAPH : NODE VS TRANSMISSION TIME (PRIMARY AND SECONDARY PATH)

The Figure 9 graph compares the efficiency of

data transfer through Primary and Secondary path.

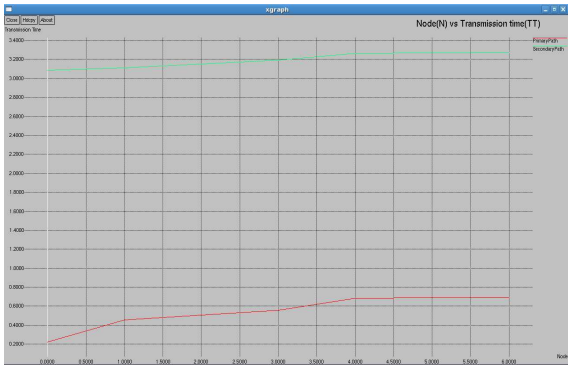

Fig 9 : Node Vs Transmission Time (Primary and Secondary path)

TABLE 2: NODE VS TRANSMISSION TIME (PRIMARY PATH)

X-AXIS (NODE)	Y-AXIS (TRANSMISSION TIME)
0	0.221539
1	0.456455
3	0.556162
4	0.682935
6	0.691748

In Table 2, Node(N) is taken in X-axis and Transmission Time is taken in the Y-axis. Node(N) specifies the nodes forming the Primary Path. Transmission time specifies the time at which every node receives a particular packet that is sent from sender to receiver. Here the time taken by Primary Path to send a single packet from sender to receiver is around 0.46.

TABLE 3: NODE VS TRANSMISSION TIME (SECONDARY PATH)

X-AXIS (NODE)	Y-AXIS (TRANSMISSION TIME)
0	3.086787
2	3.111769
3	3.190826
4	3.262293
6	3.273045

In the above Table 3, Node(N) is taken in X-axis and Transmission Time is taken in the Y-axis. Node(N) specifies the nodes forming the Secondary Path. Transmission time specifies the time at which every node receives a particular packet that is sent from sender to receiver. Here the time taken by Secondary Path to send a single packet from sender to receiver is

around 0.20. So from the tables we can find that Secondary Path is more efficient than Primary Path.

H. 5.8.2 NODE VS TRANSMISSION TIME (PATH FAILURE)

This Figure 10 shows the path failure due to node 4. In x-axis we take the nodes forming the primary path. In y-axis, we take the transmission time from sender to receiver. As we can see from the graph, when node 4 fails the transmission through the Primary path is ended.

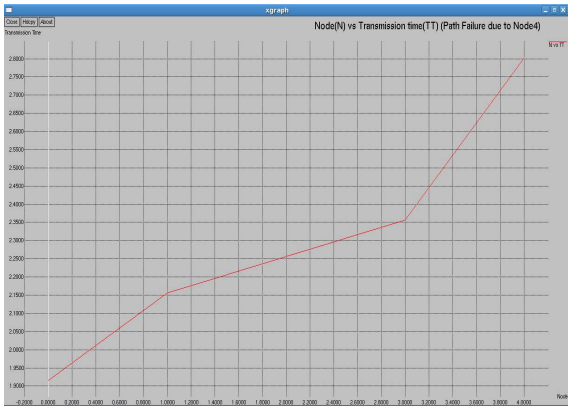

Fig 10: Node Vs Transmission Time (Path failure)

TABLE 4: NODE VS TRANSMISSION TIME (PATH FAILURE)

X-AXIS (NODE)	Y-AXIS (TRANSMISSION TIME)
0	1.91539
1	2.156455
3	2.356162
4	2.8023
6	---------

In the above Table 4, we take Node (N) in X-axis and Transmission Time is taken in the Y-axis. Node (N) specifies the nodes forming the Primary Path 0→1→3→4→6. Data starts transferring through the Primary path. It reaches Node 4 at the time 2.8023. At the meantime, Node 4 fails due to packet loss. So no more data can be transferred through Node 4.Hence the data does not reaches Node 6. This is the reason why Node 6 has no transmission time.

VI. CONCLUSION

A Bluetooth Scatternet has been established. Multi-homing facility of SCTP has been implemented in the established Bluetooth Scatternet. Hence congestion is avoided in our Proposed System. From the experimental result it is seen that secondary path is more efficient than Primary path. Secondary path transfers data two times faster than the Primary path. So even if Primary path fails, data transmission through Secondary path will be very efficient and reliable. SCTP thus increases the fault tolerance level during data transmission in Bluetooth Scatternets. Increased ACK traffic due to large amount of data transmission can be avoided by providing separate path for ACK. In our Proposed System, we provided a separate path for ACK. Hence ACK traffic has been avoided.

In our proposed system we have two IP addresses per host. But we can increase the number of IP addresses more than two for each host so as to obtain more than two paths for data transmission in order to increase the fault tolerance level.

REFERENCES

[1] Abd El AI ,Saadawi, and M. Lee., LS_SCTP: A Bandwidth Aggregation Technique For Stream Control Transmission Protocol. Computer Communication, Vol 27, No 10, pp 1012-1024,2004.

[2] Baatz, M. Frank, C. Kühl, P. Martini and C. Scholz, "Bluetooth Scatternets: An Enhanced Adaptive Scheduling Scheme", Proc. IEEE INFOCOM'02,pp 789-790, 2005.

[3] Basagni, Bruno and Petrioli, A Performance Comparison of Scatternet Formation Protocols for Networks of Bluetooth Devices, *Proc. IEEE International Conference on Pervasive Computing and Communications (PerCom)* Texas, pp 93-103, 2005.

[4] Bhagwat and Segall A, A routing vector (RVM) for routing in Bluetooth scatternets, *Proc. IEEE Int. Workshop on Mobile Multimedia Communications MoMuC*,pp 375-379, 1999.

[5] caro A, Amer P ,Iyengar J and R Stewart, Retransmission policies with transport layer multihoming In IEEE ICON 2003, pp 255-260, 2003.

[6] Daoud K. , Guillouard, K., Herbelin, P. and Crespi, N, A Network-Controlled Architecture for SCTP Hard Handover,IEEE Conference on Vehicular Technology, pp 1-5,2010.

[7] Iyengar J , shah K,Amer P, and Stewart Concurrent multipath transfer using SCTP multihoming. In SPECTS 2004, San Jose.Califonia,pp 74-81, 2004.

8] Iyengar J, Amer P and Stewart R, Concurrent multipath transfer using transport layer multihoming: performance under varying band width proportions. In Milcom Vol 1,pp 238-244, 2003.

9] Jinsuk Baek Fisher, P.S. Minho Jo and Hsiao-Hwa Chen, A Lightweight SCTP for Partially Reliable Overlay Video Multicast Service for Mobile Terminals , IEEE Transactions on Multimedia, Vol 12,No 7,pp 754 - 766 ,2010.

[10] Riccione, RG-SCTP: Using the relay gateway approach for applying SCTP in vehicular networks,The IEEE symposium on Computers and Communications, pp 234-239,2010.

[11] UC Berkeley, LBL,USC/ISI, AND Xerox parc.ns2 documentation and software, version 21b8,2001,

[12] Wang Y , Stojmenovic I and LI X Y, Bluetooth Scatternet Formation for Single-hop Ad Hoc Networks Based on Virtual Positions, in Proc. 9th IEEE Symposium on Computers and Communications ISCC'2004,pp 1-17 , 2006.

[13] Wang Y , Stojmenovic I and LI X Y, Partial Delaunay, Triangulation and Degree Limited Localized Bluetooth Multihop, Scatternet Formation, *IEEE Transactions on Parallel and Distributed, Systems, Vol 15, No 4, pp 350-361, 2006.*