FILE TRANSFER PROTOCOL CONNECTION OVER A SINGLE –HOP BLUETOOTH RADIO LINK

P.N.V.Satyakonda#1, Dr.A.Srinivasa Rao#2

(CNS I/II M.Tech, KLUniversity)

E-Mail:satya539.puppala@gmail.com

Prof of KLUniversity

E-Mail:drsrinivas@kluniversity.in

Abstract- **TCP is the current dominant transport protocol, mainly used in fixed networks. It is well-known that TCP performance may degrade over paths that include wireless links, where packet losses are often not related to congestion, but to the unreliability of the transmission medium. In this paper, we examine this problem considering a wireless link based on Bluetooth radio equipment. Bluetooth (BT) is a low-cost system in the unlicensed 2.4GHz band. It provides a reliable data transmission using fast frequency hopping technique and Stop-and-Wait ARQ scheme. In our experiments, we have studied the performance of a heavy file transfer over a BT link, with different environmental conditions and BT radio packet formats. Results show that the best FTP performance in a wide range of radio channel conditions is obtained by using long non-FEC-protected radio packets. Nevertheless, in particularly hostile situations, the intermediate-length packet format appears more suitable. Furthermore, analysis has focused the possibility of inefficiency due to bad interaction between TCP and BT retransmission mechanisms.**

*Keywords:***packet,file transfer protocol,sliding window protocol,piconet.**

1. Introduction

The increasing popularity of wireless technologies and the continuing advancements in portable computing are flowing together in a raising demand for wireless networks. This consideration is forcing researchers to study the performance of the most common data applications over different radio equipment. In particular, much work has been made about the behaviour of Transmission Control Protocol (TCP) over wireless networks, thanks to its primary role in the Internet protocols stack. It is well know that TCP is tuned to work well in wired networks, where packet losses and unusual delay are primary due to congestion. Unfortunately, communication over wireless links suffers from sporadic high bit error rates that produce packet losses not related to congestion. These events may trigger the congestion reaction mechanisms on TCP throughput and hence, sub-optimal performance .A method proposed to alleviate these problems consists in hiding the unreliability of the wireless link from the TCP sender by using local retransmissions and forward error correction (FEC) schemes . In this way, the lossy link appears as are liable link with a reduced effective bandwidth. Unfortunately, the TCP sender may not be fully shielded from wireless losses. Indeed, the link layer retransmissions could generate sporadic long delay on segment delivery, causing the TCP sender timer to expire. These spurious timeouts trigger unnecessary segment retransmission and start the congestion control mechanisms, leading to a waste of available capacity in the wireless link and a significant degradation of end-to-end throughput. Besides, another problem is the low radio link capacity that could produce a buffer overflow at the interface between fixed and radio parts, resulting in a loss of performance. In spite of these problems, many proposals to support wireless Internet access are based on link layer approach. Some examples can be found in and where a radio connection based respectively on GSM and DECT technology is analysed. In this paper we consider a new link layer solution, based on the emerging Bluetooth technology.

2. Background

This section gives a brief overview of Bluetooth technology and of the TCP features of primary interest for our purposes.

2.1 The Bluetooth radio system

Bluetooth (BT) is a low-cost system for medium bit-rates wireless *ad-hoc* networks in the unlicensed 2.4 GHz ISM band. Two up to eight BT units sharing the same channel form a piconet. In each piconet, one unit acts as master, controlling the channel access in order to avoid collisions, based on a centralised polling scheme. The channel is represented by a pseudo-random hopping sequence 1-MHz RF channels.

The hopping sequence is unique for the Piconet and is determined by the Bluetooth (BT) device address of the master, whereas the BT clock of the master determines the phase of the hopping sequence. The time is divided into time slots where each slot corresponds to a RF hop frequency. The nominal hop rate is 1600 hops/s, corresponding to a slot duration of 625μs. Full duplex is obtained with a slot-based Time-Division Duplex (TDD) scheme.Both Synchronous Connection Oriented (SCO) and Asynchronous Connection Less (ACL) links can be established among BT terminals, respectively for coded voice and best-effort data traffic (symmetric and asymmetric), with an available bit rate of up to 721kb/s. The master maintains the SCO link by using reserved slots at regular intervals (circuit-switched connection). SCO packets are exclusively one slot long and they are never retransmitted. In the slots not reserved for SCO links, the master can exchange ACL packets with any slave on a per slot basis (packet-switched connection). A slave is permitted to return an ACL packet in the slave-to-master slot if and only if it has been addressed in the preceding master-to-slave slot, following the polling scheme mentioned above. A baseband packet can extend over **one**, **three** or **five** consecutive time slots. When a multiple slot packet is used, the transmitter frequency remains unchanged for the whole packet duration, thus reducing the efficiency loss due to the PLL settling time (~220μs), occurring each time a new frequency is used. Each packet starts with a 72-bit **access code** (AC), used for synchronisation and piconet identification. At the beginning of each reception slot, the BT unit correlates the sequence received to the expected AC. The incoming packet is accepted only if the correlator output exceeds a certain threshold, elsewhere it is discarded. The AC is followed by an 18-bit packet **header** field, coded with a 1/3 FEC code , resulting in a 54-bits header. A packet received with an unrecoverable header is immediately discarded. A **payload** field completes the baseband data packet. Payload is covered by a 16-bit CRC code, used by a simple Stop-and-Wait ARQ scheme to verify the integrity of received data.

2.2 TCP congestion recovery algorithms

Modern implementations of TCP include four intertwined algorithms for flow control: slow start, congestion avoidance, fast retransmit, and fast recovery.

Slow Start and Congestion Avoidance

The flow control scheme used by TCP is based on a "sliding window" concept. The allowed window (*awnd*) is the minimum of the sender's congestion window (*cwnd*) and the receiver's advertisement window (*rwnd*). During the *slow-start phase* the value of *cwnd* is increased by one segment for each received ACK, whereas, in congestion phase, the *cwnd* is incremented by 1 full-sized segment per round-trip time (RTT). Slow start phase ends when *cwnd* exceeds a specific threshold, called *ssthresh*, after that congestion avoidance phase is executed. When congestion is detected, the slow start phase is restarted with a *cwnd* set to one 1 full-sized segment and *ssthresh* set to half of the amount of outstanding data in the network.

Exponential Back off and Round Trip Estimation

TCP sender dynamically adapts the retransmission timeout (RTO) to the end-to-end delay, by using an estimation of mean (*SRTT*) and standard deviation (*D*) of theround-trip time (RTT). These values are adjusted each time an ACK is received, on the base of the following formulas

$SRTT=SRTT+0.125\cdot(RTT-SRTT)$

$D=D+0.25\cdot(|RTT-SRTT|-D)$

The retransmission timeout (RTO) is computed as

$RTO=SRTT+4\cdot D$

When a timer goes off before receiving the acknowledgement for the relative segment, the segment is retransmitted and the value of the timer is doubled.

Fast Retransmit and Fast Recovery

The TCP may generate a duplicate acknowledgement (DACK) when an out-of-order segment is received. If three or more duplicate ACKs are received in a row, it is a strong indication that a segment has been lost. TCP then performs a retransmission of what appears to be the missing segment, without waiting for a retransmission timer to expire (**fast retransmission**). After this retransmission, congestion avoidance, but not slow start is performed (**fast recovery**).

3. Methodology of analysis

The main focus of our analysis is to study the performance of different BT packet formats and the potential protocol interactions between TCP and radio link protocol(RLP).To converge from their initial values to a stable range operation. We have therefore performed a series of large bulk data transfers between a fixed FTP server and a nomadic FTP client. Experiments have been made in different real-world situations, obtained by moving the nomadic station around our research laboratory. Unfortunately, we have no method to precisely determine the signal strength in each situation. So, the environmental hostility has been classified on the basis of practical considerations, as the distance between BT devices, the presence or the absence of Line-of-sight (LOS), *etc*. This empirical classification is consistent with the measured packet drop probability (PDP), *i.e.* the probability that a packet is received with unrecoverable AC or Header fields.

Env1 2mt distance between terminals on different desks.

Env2 3mt distance on different desktops and microwave oven 4m away beneath a wall.

Env3 4mt distance, wall in the middle with metal whiteboards on both sides.

Env4 8mt distance on the same laboratory, with many obstacles between BT devices.

Env5 3mt distance on different desktops with microwave oven between them.

4. Measurements Platform and Tools

The architecture of the system that we have used for measurement collection. An FTP server is connected to a router through a 10Base-T Ethernet. The router interfaces fixed and radio parts establishing a BT piconet with an FTP client. The piconet has been configured with *master* on the router and *slave* on the client to maximizing the link capacity in the forward direction. Router and FTP client are running on two Pentium II notebooks, clocked to 200MHz and using the Windows 98 operating system. The radio interface runs a Bluetooth Digi Answer firmware, release , where BT baseband processing occurs. Winsock2 TCP/IPv4 Windows implementation has been used in tests. The "TCP Snooper" entity depicted Traces are collected also at the link layer exploiting the Digi Answer Bluetooth Application Programmer's Interface to collect statistics regarding an active Bluetooth link in terms of AC, FEC and CRC errors. Unfortunately, at this stage of our work, the tracing of radio link behaviour suffers of some drawbacks. For instance, the probing programs work independently on master and slave devices,then correlating master transmissions to slave receptions, and *vice versa*, is not easy. Furthermore, the probing time is not always constant and sporadically can assume very high values. The result is that we are able to determine only the trend of radio connection, and not its step-by-step history. Nevertheless, the information obtained permits to draw some interesting observation about the BT performance.

.

5. Measurement Results

In this section we present and analyse the results obtained by using different BT packet formats in our test environments. Note that the values obtained by measurements must be considered only as indicative, because even repeated stationary measurements in an identical location often yield different results.

5.1 Protected vs Un protected packet

Protecting payload with FEC produces two opposite effects: on one hand, the FEC theoretically improves the payload error probability and lowers the packet retransmission probability (PRP), on the other hand, the code overhead reduces the maximum bit rate achievable. Thus a trade-off between good put realised by DMn and DHn packets can be expected. In reality, we have found that unprotected overrun protected formats in almost all the situations considered. This fact can be partially explained by observing the two dashed curves depicted in

These curves represent respectively the AC error probability (PAC) and the Header Checksum error conditioned probability (PHEC), *i.e.* the probability of having an HEC failure given that the AC field is good.

We can note that, while the AC error probability grows rapidly passing from Env1 to Env5, the PHEC remains roughly of the same order of magnitude. This is due to the fact that the HEC is considered only when the packet has a good AC field and hence the signal strength is sufficiently high. Since the radio channel is slowly time-variant, with high probability it will remain good also during header reception. This consideration can be extended to the payload field. Indeed, if the AC and HEC fields are good, then with high probability the radio signal is strong enough to guarantee a low error probability in the payload field, and consequently the FEC results useless.

Measurements confirm this observation, at least for packets with short and medium length. Instead, long packets show an effective improvement of PRP due to FEC, especially in dynamic environment. The waste of capacity caused by FEC overhead is not compensated by the code benefit on PRP; thus, at least in the considered situations, unprotected packet format results preferable protected ones.

5.2 Short vs Long packet

In this subsection we compare the performance obtained by using packet of different length. On the basis of the results presented in the previous subsection, we consider only unprotected packet formats. During the transmission of a multi-slot packet, the carrier frequency remains unchanged for the whole packet duration, thus reducing the efficiency loss due to the PLL settling time. On the other hand, if an error occurs anywhere in the payload field, the entire packet must be retransmitted; thus in the same channel condition, long packets have higher retransmission probability than short ones. The combination of these two effects determines the effective link capacity as seen by the upper layer. Besides good put, the end-to-end performance is determined also by the link latency. than the estimated SST. Indeed, due to the low radio link capacity, segments could be buffered on the router and their delay consequently grows with the queue length.

5.3. TCP over BT link: Preliminary Res

An example of a trace of an FTP connection running on Bluetooth ispresented, for a mobile host that moves in areas characterized by different received signal quality. It can be noticed that, under normal operation, TCP Reno adapts to the latency variations due to the Bluetooth baseband retransmissions, as expected. However, under critical channel conditions, the TCP sender timeout istriggered,resulting in unnecessary retransmissions of TCP packets and in congestion control mechanisms being invoked, which reduce the connection throughput.

In the graphic, the black diamond's represent packets sent by the FTP server, while the lower and the upper lines show respectively the acknowledgement value and the transmission .window size advertised by the client. After a timeout occurs at ~62.3s, packets are retransmitted by the sender without the whole advertised window being exploited (slow-start phase) and the abnormal situation persists for about 1 second. In addition several duplicate acknowledgements are also generated In general, retransmissions often result in a cascade-effect whose negative impact extends for seconds.

6. Conclusions : In this paper we have presented the results of a set of measurements relative to an FTP connection over a single-hop BT radio link. Our measurement-based approach has given us the opportunity to observe the system behaviour in real-world situations and thus to analyse the performance obtained by using different Bluetooth packet formats.

From the collected bulk data, we can conclude that BT protected packet formats suffer from the inefficiency of FEC overhead that is not compensated by the improvement of packet retransmission probability. Furthermore, in almost all the considered situations, DH5 packets appear more suitable than DH3 in terms of good put and average SST; whereas in particularly hostile environments, the intermediate-length packet format seems better.

Finally in all the considered situations, the DH5 packet format is characterised by an estimated value of SST standard deviation greater than that obtained for DH3, due to the thick granularity of long packet transmission time. The effect of this delay variation on the end-to-end performance must be investigated in more details.

Future work will focus on analysing the possible impact of BT latency on end-to end performance, and on deriving models for the wireless link that capture the aggregate of real-world effects like noise, interference and fading.

References:

1.Department of Electronic Engineering, University of Padova,
Via Gradenigo 16/A, Padova (Italy),
Phone +39 049 8277662, Fax: +39 049 8277699
mailto: andrea.zanella@cnit.it

2. W. R. Stevens, «TCP/IP Illustrated, Volume 1: The Protocols,» Addison-Wesley, 1994.

3. G. R. Wright, W. R. Stevens, «TCP/IP Illustrated, Volume 2: The Implementation», Addison-Wesley, 1995.

4. W. Stevens, «TCP Slow Start, Congestion Avoidance, Fast Retransmit, and Fast Recovery Algorithms», RFC 2001 Jan.1997.

5. A. DeSimone, M. C. Chuah, and O. C. Yue. «Throughput Performance of Transport-Layer Protocols over Wireless LANs,» *Proc. Globecom '93*, December 1993.

6. A. Chockalingam, M. Zorzi and V. Tralli, «Wireless TCP Performance with Link Layer FEC/ARQ,» *Proc. of International Conference on Communications*, pp.1212-1216, Vancouver, Canada, June 1999.