Design of GPS-GPRS Delivering Data System Using UDP Protocol

Mahdi Oliaei and Mohammad Hossein Noranian

***Abstract*—Packet data will become a significant portion of emerging and future wireless/Internet traffic. However, network congestion and wireless channel error yields tremendous packet loss and degraded data quality. In this paper, we propose an empirical design for interfacing between GPS and GPRS delivering data systems by employing user datagram protocol (UDP). It can be employed by the third-generation (3G) and higher generations of wireless networks usefully. The utilized program is MATLAB software which has a significant role of controlling between miscellaneous partitions effectively real-time.**

***Index Terms*—Global Packet Radio Service (GPRS); Global Positioning System (GPS); User Datagram Protocol (UDP); Transmission Control Protocol (TCP); Internet Protocol (IP)**

I. Introduction

INTERACTIVE and network-based multimedia and data applications such as video, image, and audio are being used increasingly both in the internet and over wireless channels. In an internet-to-mobile traffic flow scenario, the multimedia services employ user datagram protocol (UDP) as their transport protocol [1]. Compared to transmission control protocol (TCP) [2], UDP does not yield retransmission delay, which makes it attractive to delay sensitive applications. A UDP packet includes a header and payload. UDP employs a cyclic redundancy check (CRC) to verify the integrity of packets; therefore, it can detect any error in the packet header or payload. If an error is detected, the packet is declared lost and discarded. UDP packet transmission in internet is best effort in which case network congestion yields packet loss. At the receiving host, packets are either perfect or completely lost.

A. GPRS based UDP

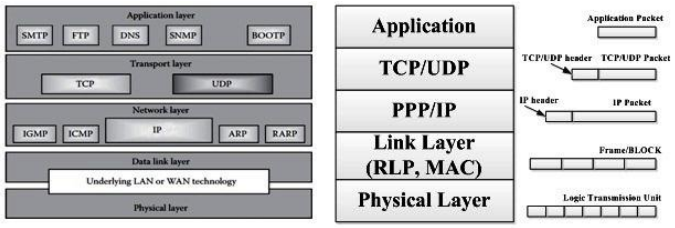
Fig. 1 (a) illustrates a general wireless protocol stack and data unit associated with each layer. After attaching UDP (TCP)/IP/PPP related headers, the application packets are deemed as a continuous bit stream at the link layer. To accomplish physical transmissions that are burst by burst, the link layer partitions the packets into multiple units. The unit size depends on the configuration of radio link protocol (RLP), medium access control (MAC), and physical (PHY) layer, as well as the current channel status, but is usually small compared to the packet length. In third-generation (3G) wireless systems [3] and [4], for applications that require low and medium data rates, each physical layer frame corresponds to a transmission unit. To support high data rate services, MAC protocol specifies that RLP can subdivide each physical layer frame into smaller logical frames named logical transmission units (LTUs), each associated with a 16 bits of CRC [5]. Typical LTU size can vary from 300 to 600 bits (4080 bytes), while IP packets are typically 6001500 bytes long. In the remainder, we simply use frame to represent both frame and LTU. At the MAC/PHY layer, channel coding is applied to each frame to protect the information data. While at the receiver, residue error after channel decoding can be detected using CRC. This frame error information is available at the RLP layer. It should be noted that in a time-varying channel, the transmitter could adjust the format of channel coding and modulation in each frame, i.e., apply link adaptation to maintain quality of service (QoS) requirements. It is possible to combine link adaptation with FEC coding at the packet level to achieve maximum flexibility. However, this approach suffers from a significant level of signaling, delay and complexity. In the remainder, we assume that packet FEC coding at application layer is performed for a given bandwidth and channel frame error rate (FER) requirement. And link adaptation is employed to maintain such requirement. The relation between these two designs is absorbed in the definition of data rate and channel FER. While satisfying the delay requirement, the RLP layer at the receiving host can specify a limited number of retransmissions to compensate for frame losses. However, such an error handling procedure cannot guarantee error free delivery so some frames would still be corrupted. We assume that the benefit of retransmissions is embedded in the FER and thus is irrelevant to our protocol and FEC coding design. The RLP forward the received frames to the point-to-point protocol (PPP) [6] for packet reconstruction. In current wireless systems, the erroneous frames are not forwarded to PPP or its equivalent layer and there is no indication of missing frames. This consequents to packet loss. When TCP is employed, packet loss can be recovered through congestion control. The performance of TCP/RLP has been

Manuscript received December 13, 2013.

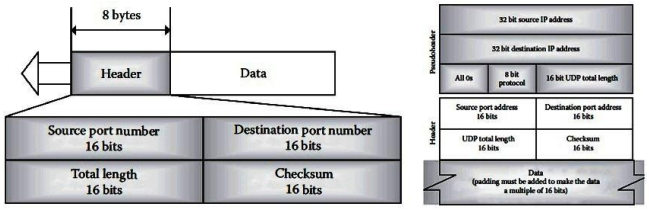
Mahdi Oliaei is with the Electrical and Computer Engineering Department, K. N. Toosi University of Technology, Seyed khandan, Dr. Shariati Ave., Tehran, Islamic Republic of Iran. P.O BOX: 16315-1355 (e-mail: m.oliaei90@ee.kntu.ac.ir)

Mohammad Hossein Noranian is R & D manager, AZM Electronics Co. (e-mail: m.h.noranian@azmco.net)

studied in [7] and [8]. User datagram protocol (UDP) is a part of TCP/IP suite. It provides full transport layer services to applications. It belongs to the transport layer services to applications. It belongs to the transport layer in the TCP/IP suite model, as shown in Fig. 1 (a). UDP provides a connection between two processes at both ends of transmission [9], as shown in Fig. 2 (b). This connection is provided with minimal overhead, without flow control or acknowledgment of received data. The minimal error control is provided by ignoring (dropping) received packets that fail the checksum test.



(a)



(b)

Fig. 1. (a) UDP and TCP/IP in the TCP/IP suite model, (b) User datagram format and Pseudoheader added to the UDP datagram [1]

Fig. 2 shows the comparison between IP and UDP addressing process which defines each domain of its protocol.

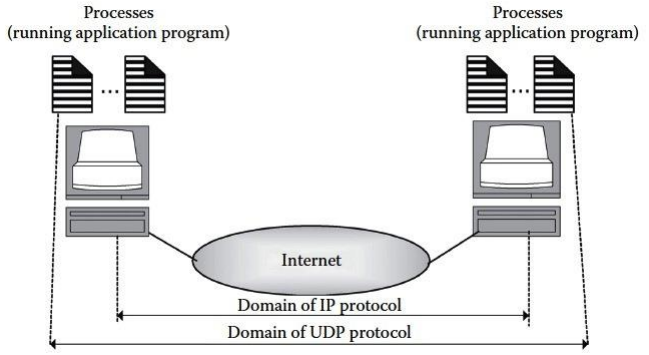


Fig. 2. Comparison of IP and UDP addressing [1]

B. GPS System

The Navigation System with Timing and Ranging (NAVSTAR) Global Positioning System (GPS) was conceived as a ranging system from known positions of satellite in space to unknown positions on land, sea, in air and space. The GPS constellation consists of 24 satellites in 6 orbital planes with 4 satellites in each plane. The ascending nodes of the orbital planes are separated by 60 degrees and the planes are inclined 55 degrees. Each GPS satellite is in an approximately circular, semi synchronous (20,200 km altitude) orbit. The orbits of the GPS satellites are available by broadcast superimposed on the GPS pseudorandom noise codes (PRN), or after post-processing to get precise ephemerides, they are available from organizations such as the Jet Propulsion Lab (JPL) or the International Geodetic Service (IGS) among others. The GPS receivers convert the satellite's signals into position, velocity, and time estimates for navigation, positioning, time dissemination, or Geodesy. Each GPS satellite transmits data on two frequencies, L1 (1575.42 MHz) and L2 (1227.60 MHz). The atomic clocks aboard the satellite produce the fundamental L-band frequency, 10.23 MHz. The L1 and L2 carrier frequencies are generated by multiplying the fundamental frequency by 154 and 120, respectively. Two pseudorandom noise (PRN) codes, along with satellite ephemerides (Broad-cast Ephemerides), ionospheric modeling coefficients, status information, system time, and satellite clock corrections are superimposed onto the carrier frequencies, L1 and L2 (Fig. 3). The measured travel times of the signals from the satellites to the receivers are used to compute the pseudoranges. The Course Acquisition (C/A) code, sometimes called the Standard Positioning Service (SPS), is a pseudorandom noise code that is modulated onto the L1 carrier. Because initial point positioning tests using the C/A code resulted in better than expected positions, the Department of Defense (DoD) directed "Selective availability" (SA) in order to deny full system accuracy to unauthorized users. SA is the intentional corruption of the GPS satellite clocks and the Broadcast Ephemerides. Errors are introduced into the fundamental frequency of the GPS clocks. This clock "dithering" affects the satellite clock corrections, as well as the pseudorange observables. Errors are introduced into the Broadcast Ephemerides by truncating the orbital information in the navigation message. The precision (P) code, sometimes called the Precise Positioning Service (PPS), is modulated onto the L1 and L2 carriers allowing for the removal of the first order effects of the ionosphere. The P code is referred to as the Y code if encrypted. Y code is actually the combination of the P code and a W encryption code and requires a DoD authorized receiver to use it. Originally the encryption was intended as a means to safe-guard the signal from being corrupted by interference, jamming, or falsified signals with the GPS signature. Because of the intent to protect against "spoofing" the encryption is referred to as "Anti-spoofing" (A-S). A-S is either "on" or it's "off"; there is no variable effect of A-S as there is with SA. Nowadays, GPS is one of most common tools using for AVL systems for helping to both public and private transportations. One of advantages of GPS system is its conformal application that it can work in any climate properly without considering for GPS application type. In this paper, we propose an empirical design by employing user datagram protocol (UDP), which delivers packet data into GPS system in the safe mode.

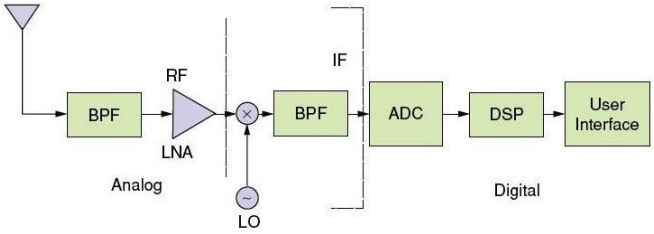


Fig. 3. Block diagram of a heterodyne GPS receiver system [11]

II. THEORY

The structure used for delivering data in UDP mode is SIM900 TCP/IP application. There are two modes: Single connection and multi-connection. In single connection mode, SIM900 can work at both transparent and non-transparent modes where under these two transmission modes, SIM900 can be configured as either TCP/UDP client or TCP server. In multi connection mode, SIM900 only can work at non-transparent mode where SIM900 can work as an absolute TCP/UDP client that can establish 8 connections totally [10]. The structure of this TCP/IP application is given as below. The transparent mode is also known as Bridge mode. The device in transparent mode can act as a bridge and also filter/inspect packets. It has all the interfaces belonging to the same LAN segment do not have to change other network settings when you add a transparent device to the network. In a word, a transparent mode, all AT commands are not available. Methods are provided to switch back and forth between data mode and command mode. Once switched to command mode, all AT commands can be used again.

In the single connection, command AT+CIPMUX=<n> used for selecting TCP/IP connection mode, when n=0, it is a single connection; n=1, it is multi connection. The default configuration is single connection.

Command AT+CIPMODE=<n> is used for selecting TCP/IP application mode, when n=0, it is non-transparent mode (normal mode); n=1, it is transparent mode. The default configuration is non-transparent mode. There are three working modes for SIM900 under this mode: TCP client, UDP client and TCP server [10].

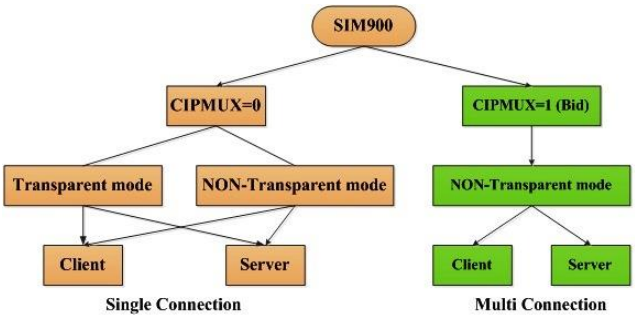
UDP has a constant size 8 byte header prepended to the transmitted data, as shown in Fig. 1 (b). The meaning of each header field is described below:

A. Source port address

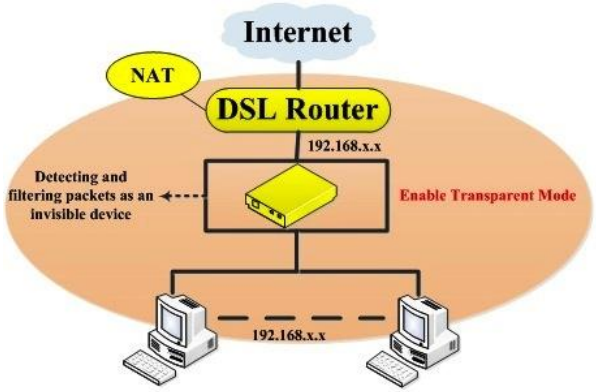
This is a 16 bit field that contains a port number of the process that sends options or data in this segment.

B. Destination port address

This is a 16 bit field that contains a port number of the process that is supported to receive options or data carried by this segment.



(a)



(b)

Fig. 4. (a) SIM900 TCP/IP Structure, (b) Typical transparent mode structure datagram [10]

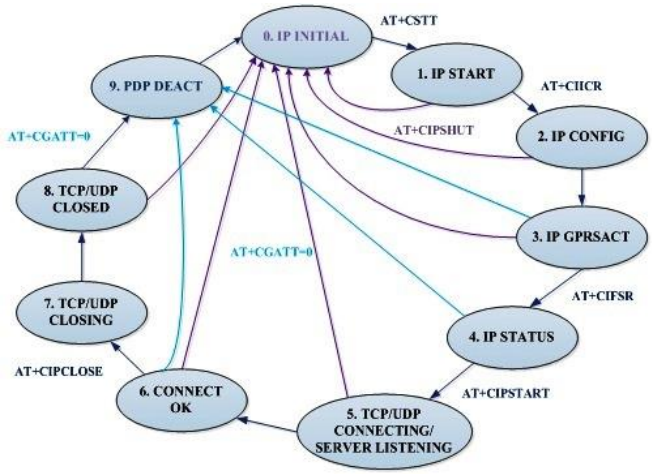


Fig.5. GPRS states diagram for single connection [10]

C. Total length

This is a 16 bit field that contains the total length of the packet. Although the number could be in the range from 0 to 65535, the minimum length is 8 bytes that correspond to the packet with header and no data. The maximum length is 65507 because 20 bytes are used by the IP header and 8 bytes by the UDP header. Thus, this information is redundant to the packet length stored in the IP header. An extension to UDP that allows for transmission of larger datagrams over IPv6 packets has been standardized. In such a case, the UDP header

specified total length is ignored.

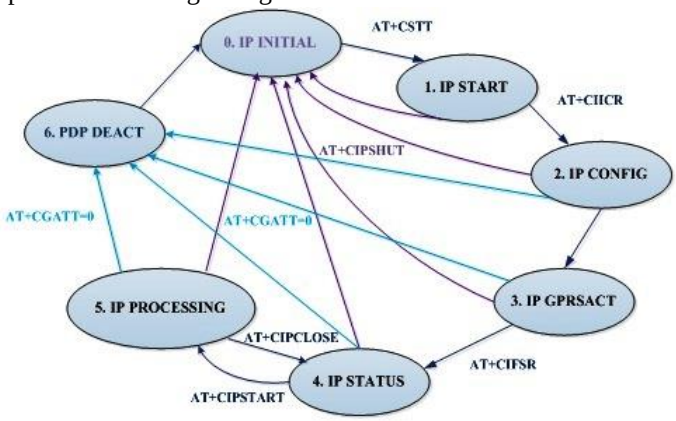


Fig. 6. GPRS states diagram for multi connection [10]

D. Checksum

This 16 bit field contains the checksum. The checksum is calculated by

- Initially filling it with 0s
- Adding a pseudoheader with information prepended as a stream of 16 bit numbers. If the number of bytes is odd, 0 is appended at the end
- Adding all 16 bit numbers using 1s complement binary arithmetic.
- Complementing the result. This complemented result is inserted into the checksum field.

E. Checksum verification

The receiver calculates the new checksum for the received packet that includes the original checksum, after adding the so-called pseudoheader. If the new checksum is nonzero, then the datagram is corrupted and is discarded. In case of UDP, the use of checksum is optional. If it is not calculated then the field is filled with 0s. The receiver can determine whether checksum was calculated by inspecting the field. Even in case the checksum is 0 the field does not contain 0 as the calculated checksum is complemented at the end of the process and negative 0 (the field filled with 1s) is stored.

F. Port Number Assignments

In order to provide platform for an independent process addressing on a host, each connection of the process to the network is assigned a 16 bit number. There are three categories of port numbers: well-known (0-1023), registered (1024-49151) and ephemeral (49152-6553). Well-known ports have been historically assigned to common services. Some operating systems (OS) require that the process which utilizes these ports must have administrative privileges. This requirement was historically created to avoid hackers running server imposters on multiuser systems. Well-known ports are registered and controlled by Internet Assigned Numbers Authority (IANA). Registered ports are also registered by IANA to avoid possible conflicts among different applications attempting to use the same port for listening to incoming connections that are typically assigned to the first available port above 49151. Some operating systems may not follow IANA recommendations and treat the registered ports range as ephemeral. For example, BSD uses ports 1024 through 4999 as ephemeral ports, many Linux kernels use 32768-61000, Windows use 1025-5000, while Free BSD follows IANA port range. As it was already outlined, UDP provides connectionless communication. Each datagram is not related to another datagrams coming earlier or later from the same source. The datagrams are not numbered. There is no need for establishing or tearing down the connection. In the extreme case, just one datagram might be sent in the process of data exchange between the two processes. UDP does not provide any flow control. The receiving side may be overflowed with incoming data. Unlike in TCP, which has a windowing mechanism, there is no way to control the sender. There is no other error control than the checksum discussed above. The sender cannot be requested to resend any datagram. However, an upper level protocol that utilizes UDP may implement some kind of control. In that case, unlike in TCP, no data is repeated by resending the same datagram. Instead, the communication process sends a request to send some information again. Trivial file transfer protocol (TFTP) is a very good example of that situation. Since it has its own higher level flow and error control, it can use UDP as a transport layer protocol instead of TCP. Other examples of UDP utilization are simple network management protocol (SNMP) or any other protocol that requires only simple short request-response communication [10].

III. Application

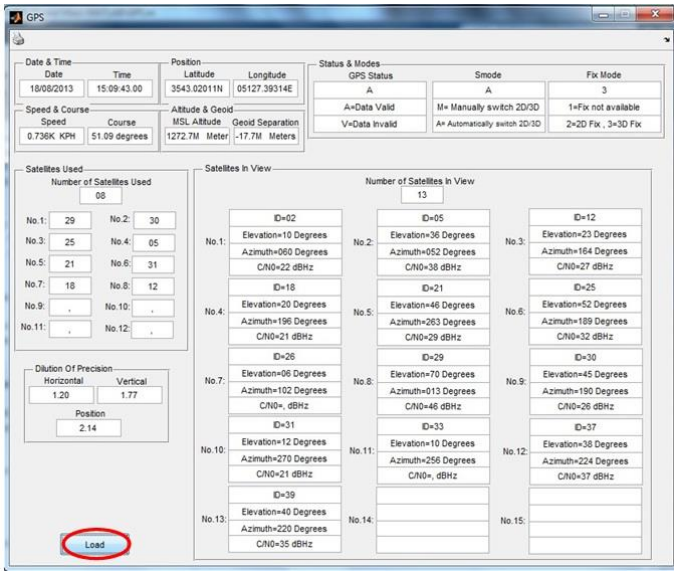
A GUI MATLAB code has been utilized for connection between GPRS and GPS systems. The GPS module used for these applications TC35i, Siemens product, which the interface is created by applying the Serial Communication Port (SCP) with a PC (LAPTOP or DESKTOP) as control server. Also, this design was applied in a microcontroller for central processor between integrated GPRS-GPS system [11]. The schematic view of this MATLAB program has been shown in Fig. 7.

AT commands are useful for connecting the modules with each other, then by taking advantage of these commands, the GPS data can be extracted as shown in Fig. 7 (a). The exploited data from GPS module is sent to the one of GPRS node modules and afterwards, the data will be sent into other GPRS nodes by UDP protocol every time. The AT commands block diagram (flowchart) used for interfacing between two nodes have been mentioned below (Fig.7 (b) and Fig. 8):

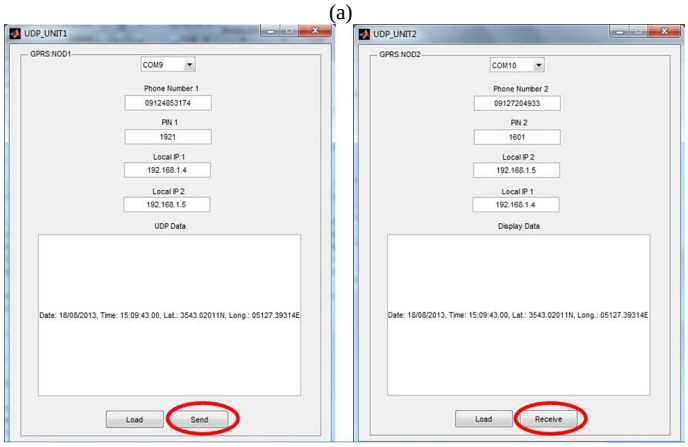
A. Network Initialization

First, the two nodes of UDP protocol interface system are established by their pin codes. The AT+CGATT command is used for enabling the GPRS network system. The AT+CSTT command enters the under covered network of GPRS (here:

Mcinet network). AT+CIIR creates the wireless network connection and AT+CIFSR gets a dynamic IP address.



(a)



(b)

Fig. 7. Schematic view of (a) GPS MATLAB Window, (b) GPRS (UDP interface) MATLAB Window

B. *Connection Appointment*

Of course the dynamic IP address can be changed to fixed IP address by AT+CLPORT command. This command determines the interface protocol type and gets its connection port. The AT+CIPSRIP displays the mentioned IP address. The AT+CIPHEAD command delivers the protocol header as mentioned in Fig. 1 (b). The aforementioned procedure is done for the second node. With setting the AT+CIPUDPMODE=1 an establishment of a network is obtained in broad connection type. By employing the AT+CIPSTART for every node and appearing the CONNECT OK message, the connection requirement can be applied. AT+CIPSTART initializes a connection between two nodes by their defined IP addresses. Afterwards, AT+CIPSEND sends the data packets by determined protocol. After the packet data writing finished, the Ctrl+Z shortcut key ends the packet data and then sending stage is accomplished by this command.

C. *Connection Shut-down*

Two commands are exploited for shutting down the network connection. These commands are named AT+CIPCLOSE and AT+CIPSHUT. The AT+CIPCLOSE disconnects the interconnection between two connected nodes while the AT+CIPSHUT closes the GPRS network.

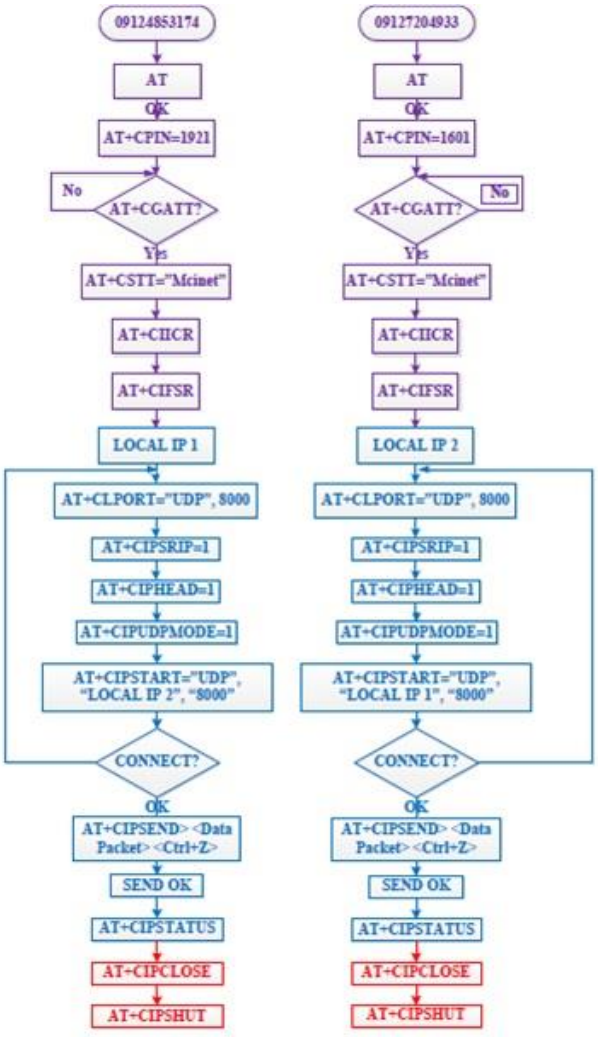


Fig. 8. UDP interface block diagram

IV. Conclusion

In this paper, a proposed empirical design for interfacing between GPS and GPRS delivering data systems by employing user datagram protocol (UDP) packet data was introduced which could be employed by the third-generation (3G) and higher generations of wireless networks usefully.

This procedure had three stages: Network Initialization, Connection Appointment, and Connection Shut-down. The AT commands were used for interfacing between the available nodes in each section.

The utilized program in this letter was MATLAB software which had a significant role of controlling between miscellaneous partitions effectively real-time.

ACKNOWLEDGMENT

The authors would like to thank AZM Electronics Co. as technical support company for providing the equipments.

REFERENCES

[1] J. Postel, "User datagram protocol", *Request for Comments*, RFC 768, ISI, Aug. 1980.
[2] W. Stevens, "TCP/IP Illustrated Reading", *MA: Addison-Wesly*, 1994, vol. 1.
[3] K. Buchanan, R. Fudge, D. Mcfarlane, T. Phillps, A. Sasaki, and H. Xia, IMT-2000: Service providers perspective, *IEEE personal communication*, Aug. 1997.
[4] R. Pandya, D. Grillo, E. Lycksell, P. Meiybegue, H. Okinaka, and M. Yabusaki, "IMT-2000 standard: Network aspects", *IEEE personal communication*, Aug. 1997.
[5] "Medium Access Control (MAC) standard for cdma2000 spread spectrum systems", *TIA/EIA/IS-2000.3*, Mar. 1999.
[6] "Point to point protocol", *Request for Comments*, RFC 1661.
[7] A. Chockalingam and G. Bao, "Performance of TCP/RLP protocol stack on correlated fading DS-CDMA wireless links", *IEEE Trans. Veh. Technol.*, vol. 49, pp. 2833, Jan. 2000.
[8] R. Van Nobelen, N. Seshadri, J. Whitehead, and S. Timiri, "An adaptive radio link protocol with enhanced data rates for GSM evolution", *IEEE Personal communication*, Feb. 1999.
[9] Aleksander Malinowski, Bogdan M. Wilamowski, "User Datagram Protocol-UDP", 2010.
[10] "TCP/IP APPLICATION NOTE V. 1.01", *A Company of SIM Tech (SIMcom)*, 2010.
[11] Olyaei, M., Kazerooni, M., Cheldavi, A., "Design and construction of automobile anti-thief multi-purpose system using GPS data", The 2nd Annual International Conference on Automotive Electronics Industry, by Research Institute of New Technologies in Automotive Industry, Accepted, 4-5 Feb. 2009. (Paper ID: AEC2009 1232).

Mahdi Oliaei was born in Dubai, UAE, on March 26, 1988. He received the B.Sc. and M.Sc. degrees in electrical and electronic engineering from Iran University of Science and Technology (IUST), and electrical and computer science engineering from Khaje Nasir Toosi University of Technology (KNTU), Tehran, Iran, in 2011 and 2013, respectively.
His current research interests are about Millimeter and Sub-millimeter (THz) wave antennas, Photonics, Plasmonics, and Quantum fields. His previous research interests include Electromagnetic Compatibility (EMC), MetaMaterials, Microwave Devices, Radar Systems and Networking.

Mohammad Hossein Noranian received the B.Sc. and M.Sc. degrees in electrical and electronic engineering from Iran University of Science and Technology (IUST), Tehran, Iran, in 2010 and 2012, respectively. He is currently Ph.D. student of electrical and computer science engineering in Khaje Nasir Toosi University of Technology (KNTU), Tehran, Iran.
He has been also R & D manager in AZM Electronics Company for many years.