A Novel Approach for Real Time Facsimile Transmission over Packet Switched Network

Soban Nazir Syed, Farroq-e-Azam and Omar Bashir
Department of Avionics Engineering
College of Aeronautical Engineering
National University of Sciences and Technology
Pakistan
Email: soban@ieee.org, fazam@ieee.org, omarbashir@hotmail.com

***Abstract*:** *The research effort presented in this paper focuses on two main issues encountered in designing real time FoIP gateways using ITU-T T.38 protocol recommendations. The first issue deals with reducing the complexity of FoIP gateways whereas the second issue aims to provide the required Quality of Service (QoS). The former is accomplished by minimizing the T.30 state machine required to be implemented in the gateways with an alternative architecture. This architecture maps a full duplex IP channel over a half duplex facsimile session in a T.38 gateway. Thus, two simplex channels operate concurrently, transferring facsimile control and image data in either direction. The latter of the two issues discussed here is traditionally resolved in FoIP gateways via spoofing. Here, the required QoS is achieved mainly through minimizing the packetization and de-packetization latencies within the gateways to the minimum by transmitting Internet Facsimile Protocol (IFP) packets that contain partial T.30 High Level Data Link Control(HDLC) frames. Additionally, implementation of some unique spoofing techniques is also discussed that utilize special HDLC frames. This unique spoofing technique is required to keep the facsimile session alive when the packet switched network introduces excessive latencies.*

***Keywords*:** FoIP Gateway, T.38, FoIP, Communications, ON-Ramp, OFF-Ramp, Architecture

I. INTRODUCTION

Organizations around the world seek to reduce telecommunication costs by converging all network traffic over packet based infrastructures like Internet Protocol (IP) networks. This convergence is having a profound impact on all communications traditionally available on Public Switched Telephone Networks (PSTN) and in this regard facsimile technology is no exception. Facsimile communication is inherently a digital form of communication that has been optimized for communication over PSTN. Facsimile communication over packet switched networks can deliver significant benefits. Costs can be greatly reduced by converting facsimile signals into packetised data and communicating these packets using corporate intranets and public Internet as the carrier instead of PSTN.

The vast majority of existing facsimile machines are designed to the Group 3 (G3) standard. G3 defines modem protocols for data transport over audio channels, a protocol (ITU-T T.30) for the two G3 facsimile devices to exchange data and formats (ITU-T T.4 and ITU-T T.6) for interpreting data as encoded bit mapped images. T.30 protocol defines a ”lock-step” mechanism for the operation of transmitting and receiving facsimile devices [1].

To allow facsimile devices to communicate over the Internet, Facsimile over Internet Protocol (FoIP) gateways are required. ITU-T Recommendation T.38 specifies the procedures for real time communication of facsimile over Internet. Source and destination facsimile machines connect to these gateways over PSTN links. Peer gateways are connected to each other over the Internet. Real time FoIP gateways permit G3 facsimile machines to communicate with other G3 facsimile machines over IP using the interlocking T.30 protocol. Commands and image data from the transmitting facsimile machine are demodulated at the connected gateway, transformed into packets and transferred over the IP network to the gateway connected to the receiving facsimile machine. Contents of these frames are converted back into T.30 frames, re modulated and then transmitted to the receiving facsimile device. FoIP gateways should provide a transparent medium in the form of an IP network to the connected facsimile terminals [2].

Facsimile transmissions are inherently half duplex and gateway solutions usually employ T.30 and T.38 state machines are per respective recommendations [3]. T.30 state machine determines, at the end of the transfer of a facsimile frame, if the line direction needs to be reversed. Knowledge of a particular state of T.30 protocol is of a paramount importance to the operation of a typical T.38 FoIP gateway. This involves maintaining an account of each phase of T.30 facsimile session by monitoring all of the binary coded signaling procedures and the T.4 data, and synchronization of these procedures with connected facsimile terminals. However, implementing the complete T.30 state machine in a FoIP gateway to preemptively determine when the direction of information transfer needs to be reversed, makes the FoIP gateway complex and introduces additional computational load. Complexity increases further if the gateways are required to maintain synchronization in the event of data losses and other failures.

As latency over PSTN is negligible, maintaining synchronization and timing relationships between the communicating facsimile devices is not difficult. However, packet switched networks employing best effort protocols can introduce significant

latency and jitter to the network traffic. An additional component of latency is the delay encountered in demodulating facsimile messages in the gateways and forming Internet Facsimile Protocol (IFP) packets [2]. In most cases, this latency can exceed the required interlocked timeout periods specified in the T.30 protocol. This could cause facsimile machines to timeout while waiting for commands, data or acknowledgements resulting in the disruption of real time facsimile session over Internet. Such issues related to excessive round trip delays are dealt inside the FoIP gateways by transmitting facsimile spoofing signals to the respectively connected facsimile machines. These signals enable the facsimile machines to extend their timers appreciably while the FoIP gateway waits for the required packets to arrive.

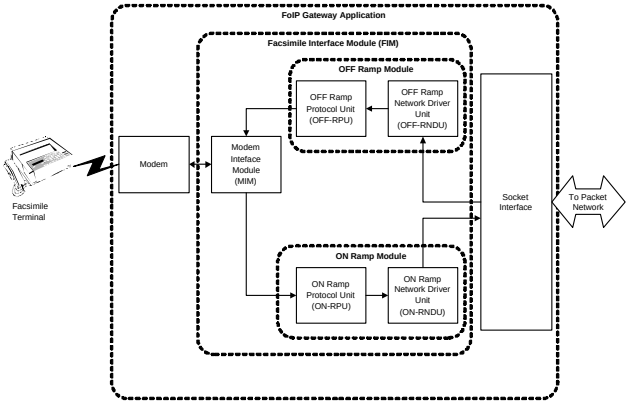

Fig. 1. Proposed FoIP gateway architecture.

II. T.38 Gateway Architecture

During a T.30 facsimile session, the two linked facsimile terminals exchange binary coded signaling information in a half duplex fashion, thus line direction may or may not be reversed at the end of information transfer depending on T.30 state machine [1]. Knowledge of this state machine is of paramount importance while designing FoIP gateways. Implementing complete state machine in a FoIP gateway makes it complex and computationally expensive by preemptive calculation of when the information transfer direction will be reversed. This involves keeping an account of each phase of T.30 facsimile session by monitoring all binary coded signaling procedures and T.4 data. Synchronisation of these procedures with connected facsimile terminal has to be achieved to comply with T.30 timing constraints. Complexity increases even more if this synchronization gets disturbed due to data loss. The complexity can be reduced if incoming T.30 bit stream can be intelligently mapped onto an IP network and vice versa.

Few terms must be understood before moving on to gateway design to fully grasp the design process. ON-RAMP direction is from PSTN towards an IP network while OFF-RAMP direction is from an IP network towards PSTN. Keeping in view OFF-RAMP and ON-RAMP directionality, if gateway functionality is split into OFF-RAMP and ON-RAMP directions, monitoring the T.30 line reversion is not required. Thus ON-RAMP modules should always map T.30 stream from PSTN towards IP network direction, whereas OFF-RAMP modules always map incoming packets from an IP network towards PSTN direction. This implies that data from ON-RAMP modules of an emitting gateway will be channeled to OFF-RAMP modules of a receiving gateway. Same is true for ON-RAMP modules of receiving gateway and OFF-RAMP module of emitting gateway. When the two connected facsimile terminals with FoIP gateways change the direction of data transfer, no state transition is required at the gateways due to this interlocked mechanism. With this interlocked mechanism in place, a very minimal T.30 state machine is now required to monitor changes in modulation rates as commanded by facsimile binary signalling DCS message and start/stop of T.4 image transfer [1]. Monitoring of these states is mandatory to correctly command gateway modem in order to receive binary coded signaling procedures. This methodology is employed in the proposed FoIP gateway design and is shown in Figure 1.

A. Facsimile Interface Module

The Facsimile Interface Module (FIM) is a software module that resides within a FoIP gateway application. FIM performs protocol conversion between G3 T.30 facsimile protocol and the digital T.38 facsimile protocol employed over the packet network. Following sections discuss functionality of proposed FoIP gateway modules.

1) OFF-RAMP Protocol Unit: OFF-RAMP Protocol Unit (OFF-RPU) decodes Abstract Syntax Notation One (ASN.1) encoded packets into ASN.1 data structures [1]. Information from ASN.1 data structures is then extracted to assemble required HDLC or T.4 data. The assembled data is then passed on to MIM for onward delivery to the connected facsimile terminal. OFF-RPU also compensates for the effects of timing and lost packets caused by the packet network delay by preventing the connected facsimile terminal from timing out while waiting for a response from the other end.

2) OFF-RAMP Network Driver Unit: The OFF-RAMP Network Driver Unit (OFF-RNDU) in OFF-RAMP module is responsible for receiving UDP packets from IP network. After striping off UDP header, a User Datagram Protocol for Transport Layer (UDPTL) packet is recovered and passed to OFF-RPU for processing. UDPTL sequence number is also monitored in case the packets arrive out of sequence.

3) ON-RAMP Protocol Unit: ON-RAMP Protocol Unit (ON-RPU) encodes received T.30 bit stream as per ASN.1 module syntax and a UDPTL packet is thus formed. This UDPTL packet is then passed to OFF-RAMP network driver unit for onward delivery to the other gateway.

[1] ASN.1 is governed by ITU-T Recommendation X.680 and ITU-T Recommendation X.691 whereas data structures for Internet Facsimile Transfer (IFT) protocol are defined in ITU-T.38 recommendations

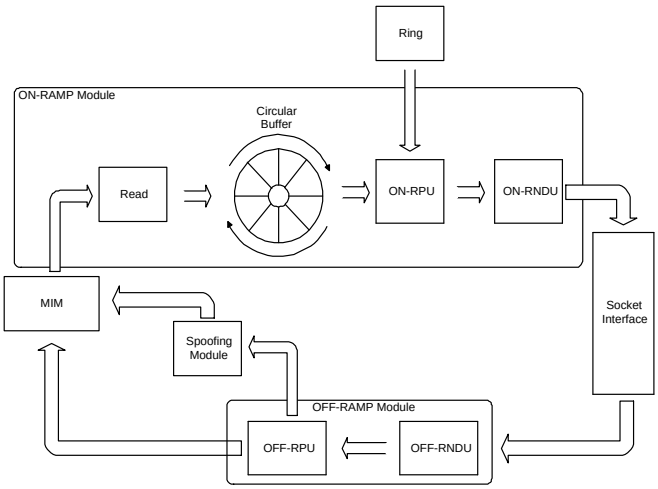

Fig. 2. Software components of FoIP gateway.

4) ON-RAMP Network Driver Unit: ON-RAMP Network Driver Unit (ON-RNDU) unit in ON-RAMP module encapsulates ASN.1 encoded UDPTL packet onto a UDP specific layer and delivers it to packet network for onward delivery to the peer gateway.

B. Modem Interface Module

This module processes T.30 bit streams as per Class 1 fax modem data exchange procedures through a connected modem [4], [5]. T.30 data received from G3 facsimile terminal is directed towards ON RAMP direction, whereas data received from Off RAMP direction is directed to G3 facsimile terminal. While the modem gives some timing support by providing accurate clocking, the MIM issues right command at the right time as per T.30 recommendations. Class 2 and above modems are not implemented in Modem Interface Module (MIM) because they do not provide flexibility in an application software to handle T.30 sessions and thus would fail to function in a FoIP gateway, where the network latencies are varying according to network loading.

III. FoIP Gateway Software Components

The FoIP gateway software components are shown in Figure 2. The architecture of these components revolves around multi-threaded application and is described in following sections.

A. Modem Interface Module

Serial communication is needed to interface a modem with gateway in Modem Interface Module (MIM). Handshaking is used to control the amount of data that can be transmitted to avoid any modem transmit buffer over run phenomenon. Hardware handshaking mechanism is utilized for this purpose in which the RTS/CTS lines are used. Overlapped I/O technique is utilized that allows more flexibility and efficiency. A port

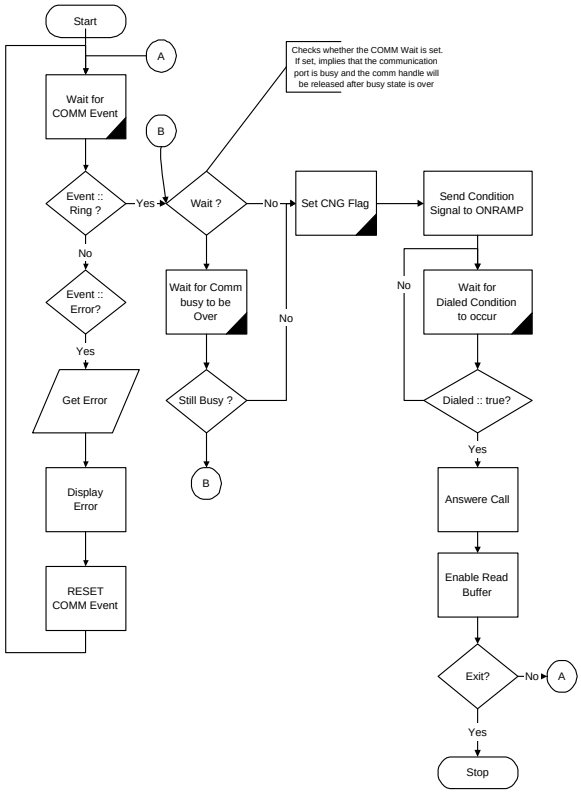

Fig. 3. Ring trapping functionality of MIM.

open for overlapped operations allows multiple threads to do I/O operations at the same time and perform other work while the operations are pending. Furthermore, the behavior of overlapped operations allows a single thread to issue many different requests and operate in the background while the operations are pending. This relieves MIM to block all I/O requests while servicing of an I/O request is in progress.

1) Ring Trapper: Functionality of detecting a ring from PSTN is implemented as a separate thread which is always waiting for a communication event of type RING to occur. When ever an event of type RING occurs, it notifies ON-RAMP module through a condition signal. After notification, event handlers are reset and the thread goes to a wait state for another communication event, as shown in Figure 3.

B. ON-RAMP Module

The ON-RAMP module is implemented as a separate thread and consists of two distinct functions as illustrated in Figure 2, namely protocol conversion (ON-RPU) and network interface (ON-RNDU) as discussed earlier. Figure 5 shows the functional flow diagram of this module.

In its idle state, ON-RAMP module thread is waiting for a condition signal. A detection of a ring in MIM generates a condition signal for CNG indication to other gateway. Appropriate ASN.1 data structures are populated, encoded and then

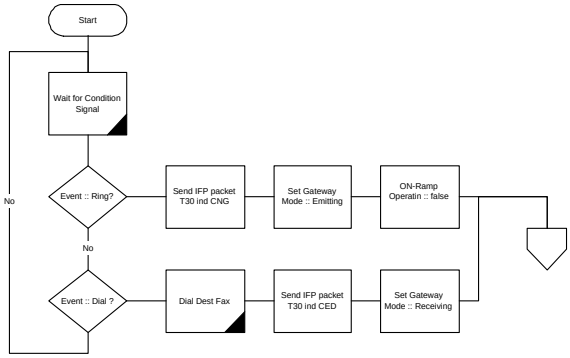

Fig. 4. Flow diagram of ON-RAMP module 1 of 2.

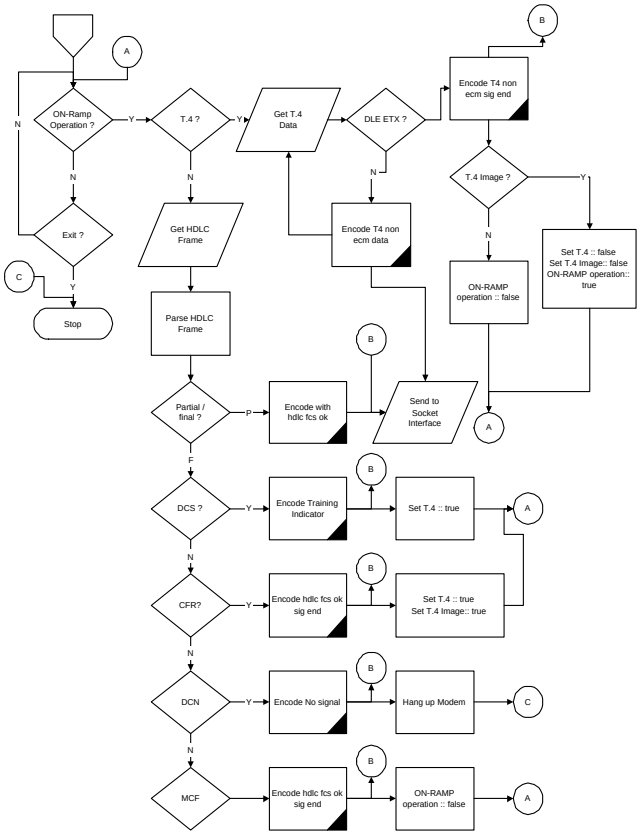

Fig. 5. Flow diagram of ON-RAMP module 2 of 2.

passed to network interface for onward delivery [2]. Gateway mode is set to an emitter in this condition. On the contrary, a dial condition can be signaled if CNG indication is detected in OFF-RAMP module. In this case, the gateway mode is set as a receiver and destination facsimile terminal is dialed. Two distinct modes of binary coded signaling procedures are monitored in this module, HDLC (phases A, B, D and E) and T.4 (phase C). DCS, CFR, DCN and MCF commands are monitored to implement a minimal T.30 state machine [2].

[2]The binary coded signalling messages DCS, CFR etc are defined in ITU-T.30 recommendations

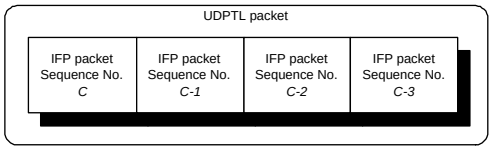

Fig. 6. Redundant IFP packets in UDPTL.

Incoming HDLC frame is parsed to populate appropriate ASN.1 T.38 module data structures, which are then encoded and sent to network interface object. While encoding UDPTL packets, error recovery information is provided by embedding redundant information in form of prior IFP packets within each packet payload. The strategy used is to provide n prior IFP packets after current one with monotonically decreasing sequence numbers. This implies that if $n \geq 0$, then n consecutive UDPTL packets are protected against packet loss. This scheme of embedding redundant information is capable of transmitting a block of redundant IFP packets whose sequence numbers are contiguous. Therefore, if a current IFP packet has a sequence number C and it is desired to redundantly transmit IFP packet $C - 3$, then the UDPTL packet must contain all IFP packets from *C*, *C-1*, *C-2*, *C-3* in the same order as shown in Figure 6. Value of $n = 2$ is implemented during ASN.1 encoding process in the proposed gateway implementation.

1) Read functionality: Read operation from MIM is implemented as a separate thread in ON-RAMP module to isolate I/O read process from rest of the units, as illustrated in Figure 7. The read thread receives data available for processing from MIM and inserts it into a circular buffer as shown in Figure 2. The circular buffer is of 50 octets in size. After writing incoming data into circular buffer, it sends a condition signal to ON-RPU to process the data and starts looking for any new data from MIM. Implementation of a seperate read thread allows other units of ON-RAMP module to continue processing while data is being fetched from MIM or while MIM is blocked waiting for data from the modem.

C. OFF-RAMP Module

This module of FIM is also implemented as a separate thread so that all tasks related to OFF-RAMP direction are sequenced. It consists of two distinct functional units i.e. OFF-RNDU and OFF-RPU. Functional flow diagram is illustrated in Figure 8. Reception of a valid data from OFF-NDU socket interface is decoded to get a UDPTL packet. Received packet sequence number is compared with expected sequence number expected. All packets with sequence number less than the current one are dropped. For sequence numbers greater than or equal to current value a difference, Δd, is generated by the relation $\Delta d = Received - Current$. Value of Δd will be zero when received and current sequence numbers match. It is quite evident that for values of $\Delta d > 0$, $|\Delta d|$ packets have not been received and have to be extracted out of from redundant

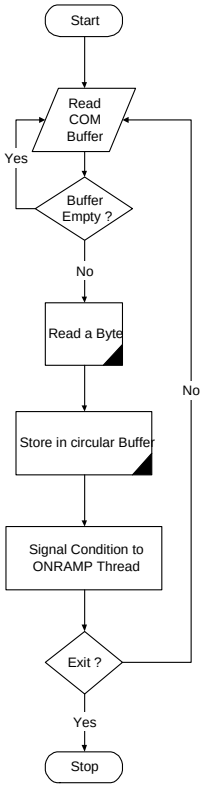

Fig. 7. Read thread functional flow diagram.

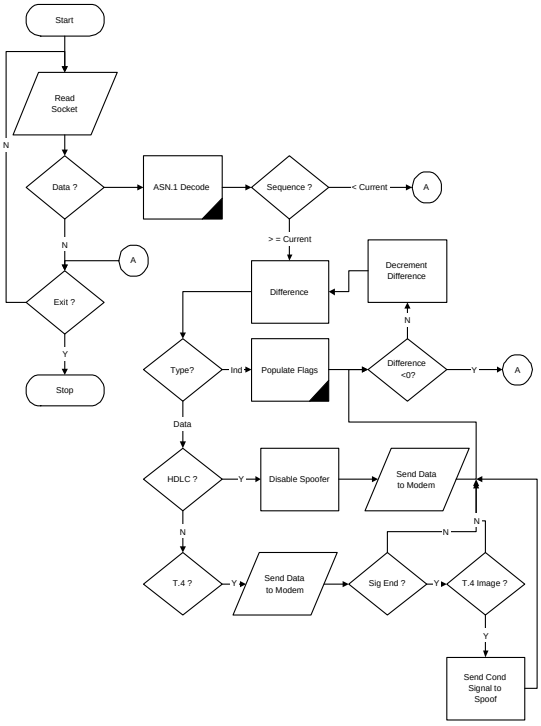

Fig. 8. Functional flow diagram of OFF-RAMP module.

information embedded in received UDPTL packet. After extraction of each IFP packet, necessary information is extracted to assemble HDLC frame or T.4 compliant data. This assembled data is then sent to MIM for onward delivery to connected facsimile terminal.

D. Spoofing Module

The spoofing function or module is implemented as a separate thread in FIM. In its idling state, it waits for a condition signal to start spoofing as shown in Figure 9. When this condition is detected, the spoofing module waits for one second and then signals MIM to command modem to transmit a HDLC spoof frame. It then again waits for one second and then checks condition for spoofing state. In case a HDLC data has arrived in OFF-RAMP module, spoofing module shall revert to idling state and no spoof frame will be sent. In case no data has arrived in OFF-RAMP module, a spoof frame will be sent every second. During this one second interval, spoof state will be monitored. Any time an HDLC data arrives in OFF-RAMP module, the spoofing module shall abort the transmission of spoofing frames and return to its idling state.

E. Socket Interface

Socket interface uses UDP as a transport mechanism due to its simplicity, less packets overhead, no connection setup delays, no flow control and necessity of retransmission and hence

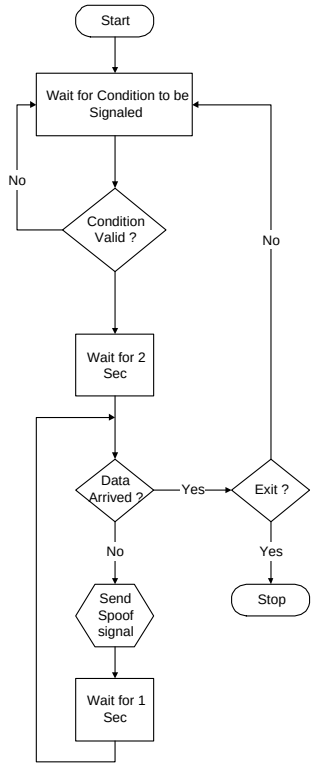

Fig. 9. Flow diagram of spoofing function.

provides applications with a raw interface to the network [6]. The simplicity of UDP meets the requirements of delay sensitive real time applications that can implement their own flow control and retransmission schemes. UDP has an advantage over TCP in aspects of latency and less packet overheads. T.38 provides UDPTL in Internet Facsimile Transport (IFT) layer which sits on top a UDP/IP stack. UDPTL packets are based on the principle of framing. Each packet may contain one or more IFP packet as its payload section. In case of multiple IFP packets in UDPTL payload, the first IFP packet is termed as primary, whereas the rest are called secondaries. To enable gateways to be synchronized upon receipt of any packet, the first primary packet is assigned a sequence number zero, whereas the successive secondary packets have linearly decreasing integer adjacent sequence numbers.

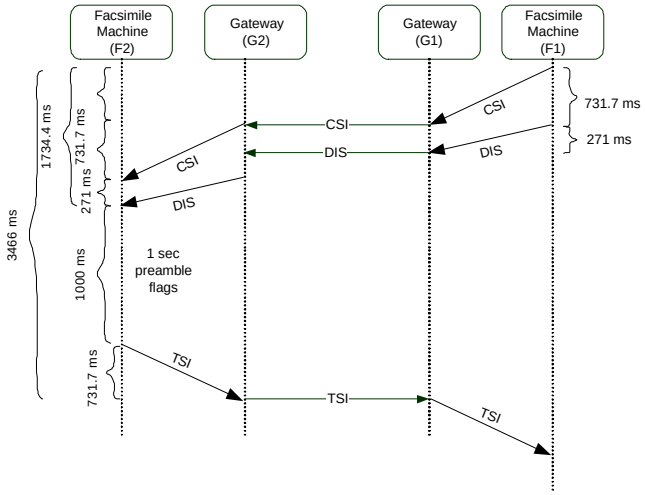

Fig. 10. Timing required for transmission of complete HDLC frames.

IV. Timing Issues in a T.38 Gateway

In addition to the format of the messages, the T.30 standard also specifies various timing requirements. The most crucial T.30 timers with respect to a T.38 gateway are T2 (6 ± 1 seconds) imposed by receiver and a transmitter timeout of 3 seconds with no response. IP network latencies severely affect these timers to timeout and subsequently abort a fax session [7]. All commands and responses are negotiated at low speed of 300 bps V.21 modulation rate. This implies that an octet transfer from a facsimile terminal to gateway modem will take place in $26.67\,ms$. The modem in turn is connected to serial port of the gateway at 19200 bps with 2 extra bits per octet, i.e. start and stop bits and will take $520.83\,\mu s$ for transmission of received octet to gateway port. Thus an octet takes a total of $26.67\,ms + 520.83\,\mu s = 27.1\,ms$ for reception in gateway application. The longest HDLC frame in phase A, B, D, and E is 27 octets long which is either TSI or CSI. In the worst case, longest HDLC frame will take $731.7\,ms$ for transmission from facsimile terminal to gateway application. It is assumed for time being that there are no processing delays in gateways and a negligible IP network delay. Therefore, it is inferred that the received HDLC frame in gateway (G1) is available to other gateway (G2) instantly after encoding and transmission as shown in Figure 10.

Gateway G2 then starts pumping the received HDLC frame to modem transmit buffer which takes $731.7\,ms$ to be received at connected facsimile terminal F2. Thus an HDLC frame carrying TSI or CSI in its FCF field will take a total of $1463.4\,ms$ from one facsimile terminal to another facsimile terminal using a T.38 gateway. TSI/CSI frames are always followed by either DIS/DCS frames of 10 octets length including DLE shielding. It is pertinent to note that while CSI/TSI HDLC frames are being transmitted from G2 to connected facsimile terminal F2, a DCS/DIS will be available at G2 after $271\,ms$ as shown in Figure 10, and will be transmitted after previous frame. Hence a total of $1734.4\,ms$ are required to transfer a sequence of CSI-DIS/TSI-DCS [3] HDLC frames from one facsimile terminal to another.

If the received HDLC frames in F2 were a CSI-DIS pair, it starts transmitting a response to received HDLC frames in form of TSI-DCS message pair. Assuming no processing delay in F2, a $1\,s\,(1000\,ms)$ preamble will be transmitted followed by TSI message. Since it is known that TSI takes $731.7\,ms$, it will be available at G1 after $731.7\,ms$, which then starts transmitting it to F1. At the beginning of this transmission total time elapsed is $1734.4\,ms + 1000\,ms + 731.7\,ms = 3466\,ms$ which is greater than $3000\,ms$ timeout limit. These frames will not be received by F1 due to expiry of transmitter timeout. Transmission of these frames either have to be delayed till next receive cycle when F1 transmits CSI-DIS pair again or spoofing signals have to be sent while G1 was waiting for packets from network. It is quite evident from this discussion that transmitter timeout of 3 seconds will occur if complete HDLC frames are first received in gateways and then mapped onto IFP packets.

V. Spoofing Requirements

Discussion in Section IV first assumes that there are no network delays and no processing delays in either gateways or facsimile terminals. Practically this ideal situation is difficult to achieve. Keeping in view inherent latency of IP networks, it cannot be assumed to be negligible. Further more after receiving a valid command or response, facsimile terminals have their own processing delays before they start transmitting next binary coded signaling procedures. If complete HDLC frames are first received in gateway and then mapped onto IFP packets, above discussion proves that requirement of spoofing becomes mandatory as $3466\,ms$ are required to receive the first octet.

[3] These binary coded signalling HDLC messages are defined in T.30 recommendations

A. Present Spoofing Practices

There is a need to spoof a facsimile terminal connected to T.38 gateway while the gateway is waiting for T.38 packets to arrive from IP network. The present spoofing practices involve sending HDLC preamble flags to reset T.30 timer T2 and is done at data link layer of Open System Interface (OSI) reference model. In case of T.4 image transfer, phase C, extra line padding techniques are used to keep feeding receiving facsimile terminal with T.4 data in order to prevent fax session from aborting. In proposed T.38 gateway implementation, external modems are used where data link layer is embedded in modem hardware. The only control available for gateway application is through AT+F [4] related modem commands which do not provide any access for sending HDLC preamble flags. A new spoofing scheme is proposed in order to maintain HDLC command/response synchronization in a T.38 gateway which uses external modem. The main purpose of this spoofing scheme is to prevent facsimile session from aborting when network latencies cross bounds of T.30 timing constraints.

B. Proposed Spoofing Scheme

Before describing the proposed spoofing scheme, framework of T.30 line control procedures and error recovery are summarized in the following:

1) All commands are initiated by transmitting terminal, the one which sends a DCS, and a response is permitted when commanded by a valid command.
2) If a transmitting terminal does not receive a valid response within 3 seconds, it will repeat the command.
3) After three successive unsuccessful attempts, transmitter will send a DCN message and the fax session will be terminated.
4) A command or a response sequence is not valid if:
   a) Any of the frames within the sequence has an FCS error.
   b) Any single frame exceeds $3\,\mathrm{sec} \pm 15\%$ in its time length.
   c) The final frame in sequence does not have P/F [5] bit set to a binary 1.
   d) The final frame FCF is not recognized.

Keeping in view the above corollaries of T.30 recommendation, a spoofing HDLC frame with P/F field bit 5 set to 0 which indicates that it is not the final frame in this sequence with rest of the fields set to 1, FF hex, is proposed as shown in Figure 11. Sending this spoof frame to a facsimile terminal waiting for a response will reset transmit time out timer of 3 seconds and shall achieve same result of sending preamble flags. FoIP gateway developed in Chapter 3 uses this spoofing strategy in spoofing thread module. Whenever a facsimile terminal receives this spoof frame, the P/F bit indicates that more frames are to follow and the receiver looks for more frames while disregarding this

[4] Fax-Modem AT command set for facsimile related functionality
[5] Partial or final frame in the sequence

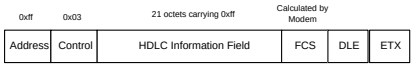

Fig. 11. Proposed HDLC spoof frame.

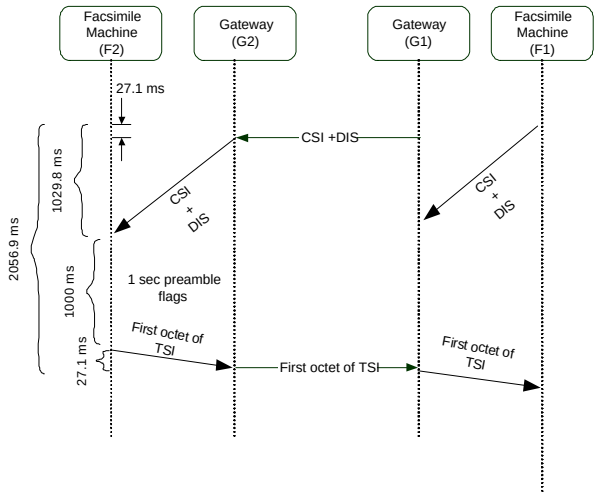

Fig. 12. Timing diagram for partial HDLC frames with m=1.

frame due to non-recognizeable FCF field. The local modem keeps on asserting carrier on the line due to P/F bit set to binary 1.

VI. Partial HDLC Frames in an IFP Packet

It was shown in Section IV that spoofing becomes mandatory if a complete HDLC frame is first received and then formulated into an IFP packet for ASN.1 compliance. T.38 provides an option for partial HDLC frames in its recommendations to formulate IFP packets comprising of m octets of an HDLC frame, with $m \geq 1$. The condition when $m = 1$ is discussed first.

The $m = 1$ condition means that for the first HDLC octet received in gateway G1 from connected facsimile terminal F1, an IFP packet is formed, ASN.1 encoded and then sent to other gateway through IP network as shown in Figure 12. It was described in Section IV that a single octet takes $27.1\,ms$ from F1 to G1. Assuming negligible network delay and negligible processing delay at gateway for the time being, it can be shown that while it is being transmitted from gateway G2 to facsimile terminal F2, G1 starts receiving another octet from F1. This implies that a partial HDLC frame transmitted time from F1 to F2 follows relationship:

$$T_{oneway} = (n + m) \times 27.1ms \tag{1}$$

where:
m=number of octets of partial HDLC frame.
n=total number of octets in a HDLC message sequence.

For example, considering CSI-DIS and TSI-DCS signal pairs, it can be shown that with $m = 1$, a CSI-DIS sequence of HDLC frames comprises of 37 partial frames (27 for CSI

and 10 for DIS) and will take $1029.8\,ms$ from F1 to F2 by using Equation 1. Assuming negligible processing delay in F2, F2 will start transmitting preamble flags for $1\,sec$ immediately followed by TSI octets. First octet will be available at G1 after an elapsed time of $1029.8\,ms + 1000\,ms + 27.1\,ms = 2056.9\,ms$. Thus F1 will start receiving HDLC frame $2056.9\,ms$ after start of transmission, which is well within 3 seconds timeout limit.

When $m > 1$, it is observed that for $m = 20$ the value of time lapse becomes $3086.7\,ms$ and crosses timeout limits of 3 seconds. Thus for $m = 20$, spoofing again is required to avert facsimile session recycle.

It is observed that by sending partial HDLC frames of one octet each, the requirement of spoofing has been eliminated altogether. This is true in the light of assumptions that were made earlier about negligible processing and network delays.

The implemented T.38 gateway was tested with full/partial HDLC frames. Spoofing was required for transmitting full HDLC frames, while for partial HDLC frame of m octets, with $m \leq 19$, no spoofing was required. For all values of $m \geq 20$, spoofing became mandatory.

VII. Lost Packet Compensation

Error recovery information is provided by embedding redundant information in form of prior IFP packets within each payload of UDPTL packet. The strategy used is to provide n prior IFP packets after current one with monotonically decreasing sequence numbers. This implies that if $n \geq 0$, then n consecutive UDPTL packets can be recovered. This scheme of embedding redundant information is capable of transmitting a block of redundant IFP packets whose sequence numbers is contiguous. However, embedding n prior IFP packets in UDPTL payload comes at cost of increased network bandwidth utilization.

For T.4 data, an IFP packet of maximum 24 octets is formed with an additional overhead of 5 octets during encoding process. Thus for 3 IFP packets in UDPTL payload, 15 octets overhead is incurred while forming a UDPTL packet versus a payload of 72 octets. UDP header overhead is 4 octets in addition to pseudo header of 12 octets. Therefore, a total overhead of 31 octets is added to a payload of 72 octets of which 21 octets overhead is always there. A UDP packet sent over IP network is thus 103 octets in length.

VIII. Conclusions

It has been shown that T.38 FoIP Gateway complexity can be reduced drastically by adopting an interlocked mechanism of tunneling HDX fax session onto FDX IP channel through ON-Ramp and OFF-Ramp modules. This interlocked mechanism provides a very minimal T.30 binary coded signaling messages monitoring thus making a significant contribution towards gateway complexity reduction. T.30 timing issues affecting T.38 implementation in a FoIP gateway have been presented in detail. It has been shown that partial HDLC framing in formulation of IFP packet as per ASN.1 module definition, performs better than IFP packets containing complete HDLC frames, in connection with spoofing requirements. A new spoofing strategy has been introduced for modems which do not allow access to data link layer functions, especially control of sending HDLC preamble flags.

IX. Future Work

The contributions made in this research effort provide a basic impetus for reducing complexity of FoIP gateways apart from providing solutions to trivial T.30 timing issues in T.38 implementation. In the light of presented research, further work can be undertaken in FoIP gateways with T.38 implementation in following areas:

1) The real time FoIP gateway developed uses fixed IP addresses for packet communications on an IP network. A scheme may be developed as per provisions of RFC 3026 and RFC 2916 draft documents to resolve gateway address from received destination facsimile number.
2) Data encryption scheme may be applied to IFP packets for sending secure fax through a T.38 FoIP gateway in military/security application. Recommendations of FED-STD-1028 April 04, 1985 for facsimile encryption may be incorporated for this purpose [8].

References

[1] ITU-T Recommendation T.30. Procedures for document facsimile transmission in the general switched telephone network, 1996.
[2] ITU-T Recommendation T.38. Procedures for real time group 3 facsimile commnuicaion over IP netwoks, 1998.
[3] Robert G. Tebbs. Real time IP facsimile : Protocol and gateway requirements. *Bell Labs Technical Journal*, 1999.
[4] William Stallings. *Data and Computer Communications*. McMillan Publishing Company, New York, fourth edition, 1994.
[5] Andrew Margolis. *The Fax Modem Source Book*. John Wiley & Sons Inc, 1995.
[6] J. Postel. RFC 768 user datagram protocol, August 1980.
[7] Kenneth McConnell. *Facsimile Technology and Systems*. Artech House, third edition, 1999.
[8] Federal Standard FED-STD-1028. Telecommunications: Interoperability and security requirements for useof the data encryption standard with CCITT group 3 facsimile equipment, April 04 1985.