TCP Accelerator for DVB-RCS SATCOM Dynamic Bandwidth Environment with HAIPE

F. Dell Kronewitter, Bo Ryu, Zhensheng Zhang, and Liangping Ma

Abstract: **A high assurance IP encryption (HAIPE) compliant protocol accelerator is proposed for military networks consisting of red (or classified) networks and black (or unclassified) networks. The boundary between red and black sides is assumed to be protected via a HAIPE device. However, the IP layer encryption introduces challenges for bandwidth on demand satellite communication. The problems experienced by transmission control protocol (TCP) over satellites are well understood: While standard modems (on the black side) employ TCP performance enhancing proxy (PEP) which has been shown to work well, the HAIPE encryption of TCP headers renders the onboard modem's PEP ineffective. This is attributed to the fact that under the bandwidth-on-demand environment, PEP must use traditional TCP mechanisms such as slow start to probe for the available bandwidth of the link (which eliminates the usefulness of the PEP). Most implementations recommend disabling the PEP when a HAIPE device is used. In this paper, we propose a novel solution, namely broadband HAIPE-embeddable satellite communications terminal (BHeST), which utilizes dynamic network performance enhancement algorithms for high latency bandwidth-on-demand satellite links protected by HAIPE. By moving the PEP into the red network and exploiting the explicit congestion notification bypass mechanism allowed by the latest HAIPE standard, we have been able to regain PEP's desired network enhancement that was lost due to HAIPE encryption (even though the idea of deploying PEP at the modem side is not new). Our BHeST solution employs direct video broadcast-return channel service (DVB-RCS), an open standard as a means of providing bandwidth-on-demand satellite links. Another issue we address is the estimation of current satellite bandwidth allocated to a remote terminal which is not available in DVB-RCS. Simulation results show that the improvement of our solution over FIX PEP is significant and could reach up to 100%. The improvement over the original TCP is even more (up to 500% for certain configurations).**

Index Terms: **Direct video broadcast return channel service (DVB-RCS), global information grid (GIG), high assurance Internet protocol encryption (HAIPE), satellite communication, transmission control protocol performance enhancing proxy (TCP-PEP).**

I. INTRODUCTION

The future global information grid (GIG) will be a single, end-to-end information system that includes a secure network environment, allowing users to access shared data and applications regardless of location, and is supported by a robust network/information-centric infrastructure. Satellite communication is expected to be one of the key facilitators of GIG, because of its ability to cover a very large area with a few assets and its ability to bypass terrestrial communication infrastructure whenever necessary. The communication scenario we consider in this paper is shown in Fig. 1. Two satellite links are used to carry data between two devices located at two distant red enclaves respectively. The IP-layer encryption via high assurance IP encryption (HAIPE) is used for the two satellite links, and not for other links on the data path.

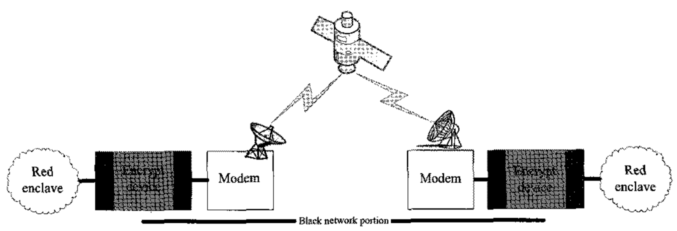


Fig. 1. Our communication scenario.

However, the strengths of satellite communication often come with the hefty cost of development (in terms of bandwidth per unit investment). These costs are due to relatively low user volume, low utilization attributed to static allocation and bursty traffic nature, and lack of widespread and affordable commercial deployment of broadband two-way terminals that the government could readily access.

The introduction of the direct video broadcast-return channel services (DVB-RCS) standard published and maintained by the European Telecommunications Standard Institute (ETSI) [1] and its growing adoption by satellite industry and Defense Information System Agency (DISA) [2]–[5] provide an array of hopes to tackle the aforementioned weaknesses. Because of its potential of supporting large user base with bandwidth-on-demand capability, the cost of terminals is becoming more affordable. In addition, the multi-frequency time division multiple access (MF-TDMA) frame structure, together with the dynamic slot allocation modes (rate based dynamic capacity, volume based dynamic capacity, etc.), provides an ample opportunity to achieve high uplink (reverse link) utilization for bursty multimedia traffic via statistical multiplexing. This will lower the system cost because more users can be supported by a single system.

Despite these promising features and major push by DISA for wider adoption of DVB-based technologies, one of the key technical challenges still remains for DVB-RCS based systems (and for all geosynchronous-based (GEO-based) satellite systems in

Manuscript received April 14, 2010; approved for publication by Fotini-Niovi Pavlidou, Guest Editor, March 20, 2011.

This project was funded in part by Air Force Small Business Innovative Research program.

The authors are with ArgonST, Network Systems, 6696 Mesa Ridge Road, San Diego, CA, email:dell@ieee.org, epicis@gmail.com, zhenshengz@gmail.com, maliangp@yahoo.com.

1229-2370/11/$10.00 © 2011 KICS

general) if they are to be seamlessly integrated into and widely deployed within the GIG infrastructure: How to support transmission control protocol (TCP) performance enhancing proxy (PEP) in the presence of end-to-end HAIPE, GIG's layer-3 security standard? It is a well-documented problem that once HAIPE is enabled, the popular PEPs employed for boosting TCP performance over GEO satellite network such as TCP spoofing will not work because HAIPE's tunnel mode will hide TCP header information required by PEP agents. A HAIPE is a type 1 encryption device that complies with the national security agency's HAIPE IS (formerly the HAIPIS, the high assurance IP interoperability specification). The cryptographies used are suite A and B, also specified by the national security agency (NSA) as part of the cryptographic modernization program. HAIPE IS is based on IP security protocol (IPSEC) with additional restrictions and enhancements. A HAIPE is typically a secure gateway that allows two enclaves to exchange data over an untrusted or lower-classification network [6].

A technique called multi-level IPSEC was proposed to support both TCP PEP and HAIPE (which is based on Internet Engineering Task Force (IETF) IPSEC standard) [7]. However, our past experience with both IETF IPSEC working group and HAIPE community indicates that they do not perceive the degraded performance of TCP over a certain type of network (satellite in this case) nor the problem or deficiency of HAIPE (or IPSEC) that it should address. In addition, multilayer IPSEC (ML-IPSEC) is considered not as strong as original IPSEC in terms of end-to-end security because it proposes trusted intermediate nodes to access TCP/IP header information. Consequently, it is unlikely that the HAIPE community will adopt this new change anytime soon, if at all, and therefore a new method of boosting TCP performance while fully supporting HAIPE and seamlessly interoperable with existing TCP-based applications must be developed, tested, and implemented.

Here we propose an explicit congestion notification (ECN) based solution for the aforementioned issues with TCP. Other work utilizes ECN signaling for network optimization. For example, in [8], the standard mechanism for call admission control in a HAIPE environment where the signaling goes from plaintext enclave to plaintext enclave is modified to take advantage of ECN. Such work relies on differentiated services code point (DSCP) which is found in modern IP headers and is not a protocol accelerator, but is instead a quality of service (QoS) mechanism. Also, others have proposed using ECN to effect TCP behavior [9]. but such optimization would require modification of the host while our proposal does not. In contrast, our solution is especially suited to high bandwidth, high latency satelite communication (SATCOM) link TCP-PEPs useful with standard network equipment. We believe that this is the first paper using ECN based mechanisms for explicit rate signaling.

While the primary focus of our research is a feasible solution towards the aforementioned problem, we also adopt a comprehensive system approach towards the development of a secure, efficient SATCOM system using readily available, commercially available communications equipment and software whenever possible by addressing the following two other challenges:

- Modern tactical, net-centric mobile ad hoc network (MANET) communication requirements include beyond-line-of-site needs. DVB-RCS systems must be closely integrated with terrestrial wireless technologies, such as 802.11 or 802.16, to serve as a backbone between out of reach subnets or back to the communication, command, and control (C3).
- Certification/accreditation authorities, including NSA, must approve the system architecture and packaging for deployment within the department of defence (DoD) information technology ecosystem.

The result is an inexpensive, compact, and powerful system whose components are already well known by potential customers, certification authorities, and procurement personnel. A block diagram of our system implementation is given in the implementation section.

The rest of the paper is organized as follows. In Section II, we describe the HAIPE compliant TCP-PEP in more details, covering detailed protocol design. In Section III, we present our results from extensive simulations and emulation. Section IV discusses implementation of the proposed solution. We extend our results to wireless networks in Section V. Section VI concludes the paper.

II. HAIPE COMPLIANT TCP-PEP

The communication scenario is shown in Fig. 1. The end-to-end TCP data path is split into three connections with the connection in the middle being the satellite links.

As noted in the introduction, the splitting of TCP connections to perform acceleration requires the manipulation of TCP headers. The presence of HAIPE encrypts those headers so that they are unavailable to the PEP. While certain network architects have suggested that the PEP may be deployed in the host rather than at the gateway, extensive network research reported in [10] indicates that this solution is sub-optimal: TCP gateways provide the maximum benefit when they are deployed right next to a satellite link, because they can use highly optimized protocols specifically designed for a SATCOM environment without affecting the rest of the network. Other obvious advantages of incorporating the PEP in the SATCOM modem gateway are that legacy devices may enjoy the benefits of the PEP without upgrading software, PEP management is centralized and easier, and the PEP has better access to information concerning the behavior of the problematic satellite link whose performance needs to be mitigated.

While the solutions we propose are amenable to most PEP systems, we have chosen to use the space communication protocol standard-transport protocol (SCPS-TP) [11] to validate our approach due to its wide use and open availability [12]. Indeed SCPS-TP has exhibited performance equal to or surpassing commercial solutions. Reference [13] states that qualitative analysis of the protocols shows that SCPS would provide the greatest benefit to complex operational networks involving TCP-based communications, multiple network paths, and other redundancies. SCPS provides the flexibility that a complex redundant network would need. Additionally, SCPS-enabled gateways possess other advantages such as one-way acceleration and

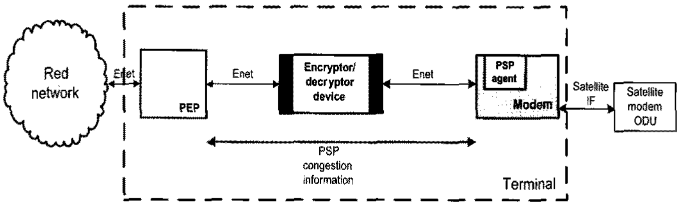


Fig. 2. PEP signaling protocol architecture.

Table 1. Black to red signaling format.

ECN bits	Description (BW=bandwidth)
00	Reduce current BW 50% from current level
01	Reduce current BW level 50 kbps
10	Increase current BW level 50 kbps
11	Increase current BW level 50% over current level or set current BW to 512 kbps

fail-over/fallback.

A. PEP Signaling Protocol Solution

While some PEPs, including a mode of SCPS-TP, operate over satellite links without explicit bandwidth information, they must resort to standard network "bandwidth probing" mechanisms such as slow start and congestion avoidance (as in TCP Reno) to determine the network bandwidth currently available. More effective PEPs, including SCPS-TP open-loop rate control, make use of direct bandwidth information. When the PEP is placed in the satellite modem such bandwidth information is readily available especially with legacy fixed bandwidth satellite protocols such as SCPC. With modern statistically multiplexed protocols such as DVB-RCS bandwidth information is not typically directly available at the subscriber terminal, but can be inferred from lower layer signaling on a much faster time scale than transport layer methods.

Our scenario which includes a bandwidth on demand satellite protocol, DVB-RCS, and HAIPE encryption makes the problem especially challenging. As noted above the PEP must reside on the red side of the HAIPE encryptor while the SATCOM modem which converts the Ethernet data to satellite intermediate frequency (IF) resides on the black side. Fig. 3 illustrates the positions of our components: PEP, HAIPE, and modem.

Our solution is a bandwidth signaling method we call the PEP signaling protocol (PSP). We require a slight change to the software which runs on the SATCOM modem, by placing a PSP agent on board which is able to infer the available bandwidth and inform the PEP module of the estimated bandwidth via methods described below.

The new PSP protocol we have designed relies on marking two ECN bits in encrypted packets to carry signaling information through the HAIPE encryptor. Modeled somewhat after frame relay's forward explicit congestion notifications (FECNs) and backward explicit congestion notifications (BECNs), IP ECN was first proposed in experimental draft RFC 2481 in 1999 and accepted as an Internet standard in 2001 as RFC 3168. This technique of signaling across cryptographic boundaries using the HAIPE ECN bypass feature has been exploited previously in integrated service (INTSERV) QoS research [14]. The standard DVB-RCS traffic granularity rate is 2 Kbps or 32 Kbps depending on the scaling_factor bit defined in DVB-RCS satellite access control (SAC) messages. That is, capacity requests are scaled to 2 or 32 Kbps. However, our testing has indicated that this resolution is too fine for our purpose, and in PSP, we set the granularity to 50 Kbps. Note that the most important signaling is rapid notification of large changes in available bandwidth, so our four signaling levels are roughly additive and multiplicative increase and decrease. With this in mind we have the following PSP black-to-red signaling format, illustrated in Table 1.

The PSP agent in the modem can then inform the PEP of the currently available bandwidth over the satellite link through numerous ECN signals, as shown in Fig. 2. This signaling is at a primitive state and must be tuned with simulations and network traffic experiments.

As a practical matter we note that the PSP signaling is confined to the modem. The ECN bits on in-bound packets are cleared by the red side single board computer (SBC). The ECN bits on outbound packets can be cleared by the black side modem or by restricting our signaling to the ECN bits on inbound packets, we can support GIG DSCP preemptive class of service by applications in the red enclave which wish to make use of this GIG feature.

B. Bandwidth Estimation

DVB-RCS does not provide direct insight into the currently available bandwidth being provided by the network control center (NCC) scheduler. The PSP agent in the modem must infer the current bandwidth from the currently allocated slots and the bandwidth requests coming from the modem to the NCC. The bandwidth requests coming from the modem could result in all of the requested bandwidth allocations during periods of low network usage or none of the requested bandwidth allocations during periods of high network usage. While the return channel satellite terminal (RCST) has no direct insight into the NCC's dynamic capacity allocation (DCA) scheme we suggest a method to infer future allocations based on (recent) past allocations. Mathematically we give the estimated bandwidth as:

$$EBW(i) = BW(i-1) + \frac{BG(i-\lambda)}{BR(i-\lambda)} BR(i) \qquad (1)$$

where $EBW(i)$ is the current bandwidth estimate, $BW(i)$ is the currently allocated bandwidth in the current terminal burst time plan (TBTP), $BG(i-\lambda)$ is the bandwidth granted previously from that request, $BR(i-\lambda)$ is the bandwidth requested previously, and $BR(i)$ is the currently requested bandwidth. An unburdened network will result in the granting of all requested bandwidth or $BG(i-\lambda)/BR(i-\lambda) = 1$. In this case, $EBW(i) = BW(i-1) + BR(i)$. The accuracy of the bandwidth estimation is illustrated in the simulation section.

C. Quick Start Signaling

One difficult requirement for our approach is the existence of data flowing through the encryptor to use for signaling. Under non-zero traffic load, in steady state, the TCP protocol guarantees the existence of TCP data flowing from black to red, the forward link, acknowledging the TCP data flowing from red to black, the reverse link. At the beginning of a large TCP data transfer to the NCC however no data is guaranteed to occupy the forward link to leverage for signaling. In a system with a non-zero free capacity access (FCA) satellite link we can solve this problem with no reverse link bandwidth penalty by sending a periodic ping packet from the PEP over the link in the absence of TCP data. While the latency associated with each ping packet is very large over the satellite link (on the order of 550 ms), this is irrelevant since we require only the periodic existence of data to use for signaling. We expect to be able to provide 20 pings per second offering a signaling opportunity every 50 ms. This brings the PEP signaling latency to a level along the same magnitude as inter-frame DVB-RCS time which is typically 26.5 ms for practical implementations.

The minimum size for a HAIPE tunnel encoded Internet control message protocol (ICMP) echo-request packet over the link is 88 bytes (while 28 for the unencoded ICMP over IP echo-request). The 88 bytes translates to 2 asynchronous transfer mode (ATM) cells or 1 MPEG frame, typically a single DVB-RCS burst in either case. At the 20 packet per second rate this translates to 14.1 Kbps which should be the minimum rate allocated to a RCST in standard DVB-RCS satellite network. As counterintuitive as this may be, the addition of such ICMP echo-request traffic results in no penalty on the network except a minimal transient penalty at the beginning of unsolicited TCP transfers over the forward (high-bandwidth) link. It is difficult to imagine such transfers since we would expect any traffic over the forward link to be solicited by the remote TCP node served by the RCST.

Studies have indicated that satellite users' experience is significantly improved by keeping a minimum non-zero bandwidth allocation for each user terminal. This allows small application layer request packets to traverse the satellite link without any delay associated with requesting a trivial amount of bandwidth. This fits in well with our quick start PSP signaling echo flow which requires this trivial amount of reverse link bandwidth (Fig. 3). In the DVB-RCS QoS guide [15], ETSI makes a similar free capacity assignment recommendation. Of course if the NCC multiple access (NCC MAC) scheduler is under extremely heavy load and no slots are available on the return link the PSP agent in the modem would signal the PEP and the PEP would refrain from sending the echo requests.

D. *Quality of Service in Military*

The prioritization and preemption of network traffic is a central feature in GIG architecture. The GIG net centric implementation document [4] states that traffic must be handled according to the priority associated with its DSCP value. Since our network device services a potential bottleneck link to the high speed backbone, differentiated traffic handling becomes especially important.

As mentioned earlier, the standard strategy we use is to keep the data in the unencrypted state as long as possible. This is a similar problem faced by the Linux enthusiasts accessing the Internet over digital subscriber (DSL) lines. The Linux kernel contains built in queuing support including token bucket filters, classifiers, and conditioners as described in RFC 2475.

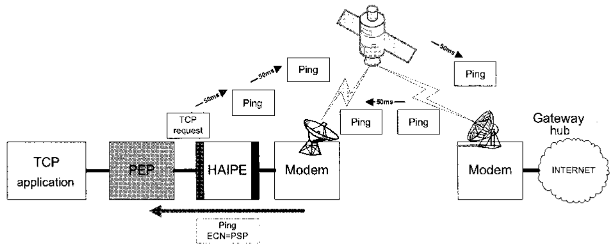


Fig. 3. Echo signaling in the absence of TCP data.

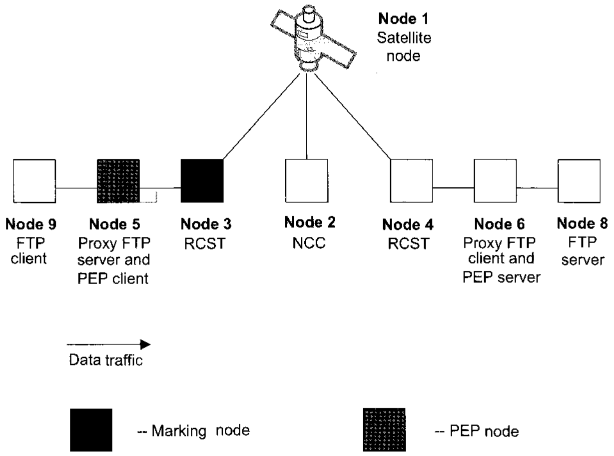


Fig. 4. PEP signaling protocol for qualnet simulation.

We have modified the standard public script which implements such precedence and pre-emption (P&P), "wondershaper," to be compliant with GIG network centric implementation documents (NCID) directives and turn any modern Linux computer into a GIG compliant traffic classification node. We call our new script "GIG-shaper."

III. SIMULATION AND EMULATION

In order to evaluate the performance of the proposed PSP signaling scheme, we conducted extensive simulation and emulation. In this section, we will present our simulation and emulation results.

A. *Simulation Results*

We have designed and implemented a Qualnet DVB-RCS environment to test our HAIPE compliant PSP. We have found that some of the features which make up SCPS-TP are standardized in RFC 1323 and have already been implemented in Qualnet TCP. We have had to add sensor network application kit (SNACK) functionality and open-loop rate control as all of the Qualnet built in TCP variants use some form of rate estimation. Our Qualnet PSP simulation work contains one new "GATEWAY_PEP" application which serves as either PEP server or PEP client.

The Qualnet simulation scenario which appears in Fig. 4 demonstrates this split connection for the two-hop case where our TCP hosts are connected via hub or network control center. Here, the connections between nodes 5 and 9 and nodes 6 and 8 are standard TCP, while the transport layer connection between nodes 5 and 6 is specially designed for satellite environments. In the case of this two-hop case, the delay between hosts is typically 540 ms and standard TCP protocol performance suffers dramatically.

The PEP client, node 5, terminates the first (proxied) TCP connection and the PEP server, node 6, initiates the final TCP connection. The protocol between these PEP nodes is SCPS-TP. The node 3 simulates the PSP agent in Fig. 2 and marks packets which are going through over the DVB-RCS connection. The simulation includes a DVB-RCS satellite protocol implementation we have developed in compliance with Advantech's DVB-RCS implementation and the ETSI standard [1]. The resulting Qualnet software is highly configurable allowing the system engineer to rapidly carry out experiments with many different network configurations and many different traffic models. In the simulation, we assumed two hosts can communicate with each other through a two-hop DVB-RCS architecture, shown in Fig. 4. The protocol between these PEP nodes (nodes 5 and 6) is SCPS-TP with SNACK enabled. Node 3 simulates the PSP agent and marks packets which are going through over the DVB-RCS connection. The bandwidth of the satellite link is assumed to be 550 Kbps. The one-way propagation delay between node 3 and the satellite, node 2, is about 540 ms. The application is file transfer protocol (FTP) to transmit a big file and the packet size is 50 bytes. There are 6 constant bit rates (CBR) background traffic sharing the same satellite link, each with rate of 480 Kbps. The TCP buffer size is set at 80 Kbyte. The satellite link is shared using the MF-TDMA scheme defined in the DVB-RCS standard. We compared the performance of the proposed PSP with a FIX PEP and the original TCP (without PEP). Here, FIX PEP refers to a SCPS-TP open loop rate control with a pre-determined fixed rate, while PSP is a SCPS-TP open loop rate control based on the available bandwidth of the satellite link. Based on the simulation results (see Fig. 5), we observe that the improvement of PSP over FIX PEP is significant and could reach up to 100%. The improvement of PSP over the original TCP is even more (up to 500% for certain time periods).

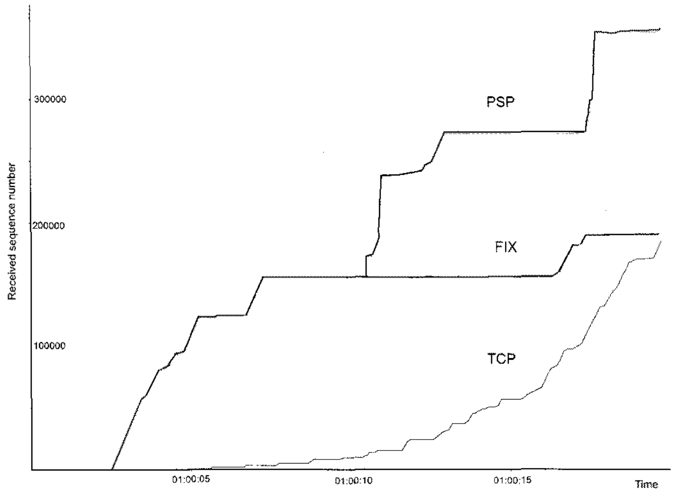


Fig. 5. Simulation results of PSP with comparison against existing schemes.

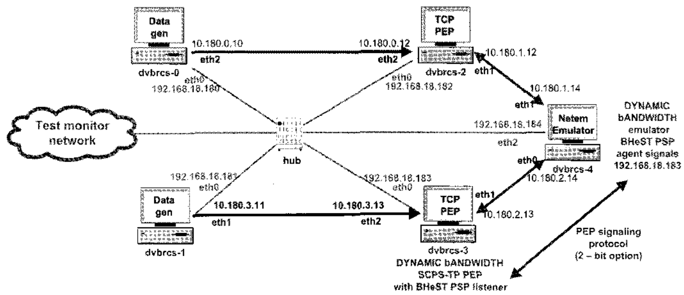


Fig. 6. Emulation test-bed setup.

B. The Emulation Environment

In order to further complement the simulation results, we have created an emulated satellite test bed to experiment with our PSP protocol. Our test bed consists of five computers as shown in Fig. 6. The links around the outer perimeter of the figure represent the data path under test. The green links represent the satellite portion, the black links represent the hosted (secure) network, and the red segment demonstrates where the PSP signaling occurs in our emulation test bed. The computers at the upper left and lower left serve as traffic generators, sink and source respectively. For our initial experiments we have used the bandwidth measurement tools iperf and scp. The computer to the right in Fig. 6 serves as the emulated two-hop satellite network. We have used the Linux based netem network emulation software to introduce a delay of 540 ms and a 0.1% packet loss in both directions. This represents a two hop geosynchronous satellite. We also rely on netem to limit the bandwidth of the emulated satellite links to rates between 1Mbps and total blockage. The other two computers in Fig. 6 host our modified SCPS-TP reference implementation. The reference implementation SCPS-TP PEP does not support dynamic bandwidth satellite environments such as DVB-RCS. Rather the bandwidth of the satellite link is entered in a configuration file. This appears to be the first modification commercial PEP vendors make. Our dynamic bandwidth enhancement simply adjusts the rate used by the standard SCPS-TP code which has already implemented the token bucket filtering for open-loop rate control in a static satellite bandwidth environment. A similar situation occurs in systems which make use of external network compression equipment so that the data emitted from the SCPS-TP module does not reflect what actually ends up transmitted over the satellite link. In such a case vendors have implemented a feedback loop which informs the SCPS-TP module of the true traffic size.

Our PSP agent runs on the modem as depicted in Fig. 2. In our emulation scenario the PSP agent runs on the netem computer, in Fig. 6, signaling the SCPS-TP. To emulate bandwidth on demand the emulation scenario modifies the rate of the emulated satellite link between 400 Kbps and 1 Mbps. Changes occur every 500 ms and happen in increments of 100 Kbps. Our PSP agent operates in two signaling modes: FullBWInfo which immediately signals the SCPS-TP the current rate, and EstimatedBWInfo which counts the packets which have traversed the link and provides one two bit signal for every packet. EstimatedBWInfo mode provides an accurate emulation for the fielded integrated HAIPE compliant DVB-RCS system.

To validate our approach we performed experiments under three different PEP scenarios using the same traffic generation

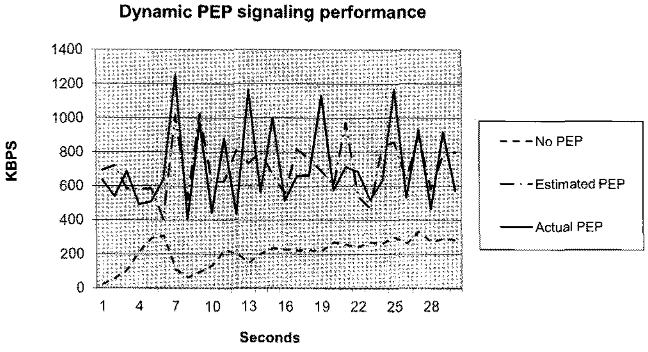


Fig. 7. TCP-PEP experimental results.

techniques under each PEP scenario. For each PEP scenario we used iperf to initiate a single TCP connection with client (source) dvbrcs-1 and server (sink) dvbrcs-0. The TCP connection attempted to transfer the maximum number of bytes over the emulated two-hop satellite link for 30 seconds. The PEP scenarios included "NoPEP" in which no PEP was used, "Estimated PEP" which used the PEP signaling protocol in EstimatedBWInfo mode, and "Actual PEP" which use the PEP signaling protocol in FullBWInfo mode. The "Actual PEP" scenario demonstrates how our dynamic bandwidth PEP would perform if the signaling channel were not restricted by HAIPE and the "Estimated PEP" demonstrates how our HAIPE compliant solution will perform. The "No PEP" scenario demonstrates the performance of a standard HAIPE and satellite modem with no PEP enabled.

Fig. 7 shows the results of our experiment under the different PEP scenarios. Averaging throughput over the entire 30 second experiment gave us a "NoPEP" throughput of 215.9 Kbps, an "Estimated PEP" throughput of 704.45 Kbps, and an "Actual PEP" throughput of 711.4 Kbps. As expected the "Actual PEP" performs best and the "No PEP" is worst. Since the "Actual PEP" performance is close to the "Estimated PEP" performance we assert that our PSP is an effective method for improving performance in a HAIPE DVB-RCS environment.

We performed a similar experiment using scp (secure copy) as the traffic generation and measurement method. We transferred a 2.8 GB file from dvbrcs-1 to dvbrcs-0 under each of the PEP scenarios described above. Table 2 shows the results of our scp file transfer experiments in throughput and total time required. Again, the "Actual PEP" performs best and the "No PEP" is worst. Since the "Actual PEP" performance is similarly close to the "Estimated PEP" performance we have further evidence that our PSP is an effective method for improving performance in a HAIPE DVB-RCS environment. Since the upper layers of scp are rather verbose, the throughput is not equivalent to that exhibited by the raw iperf transfer. Still, this experiment demonstrates the effectiveness of our method on a real world TCP data transfer.

IV. IMPLEMENTATION

The DoD has mandated (TEMPEST) one-meter separation between a red processor and black equipment, wire lines, power lines, or conductors [16]. In order to comply with this mandate and at the same time to provide multiple options, we have chosen to provide our broadband HAIPE-embeddable SATCOM tTerminal (BHeST) solution in two configurations, depending on whether the HAIPE device is embedded within the BHeST box or external to it. Fig. 8 illustrates these two options, and provides more details to the system architecture shown in Fig. 1.

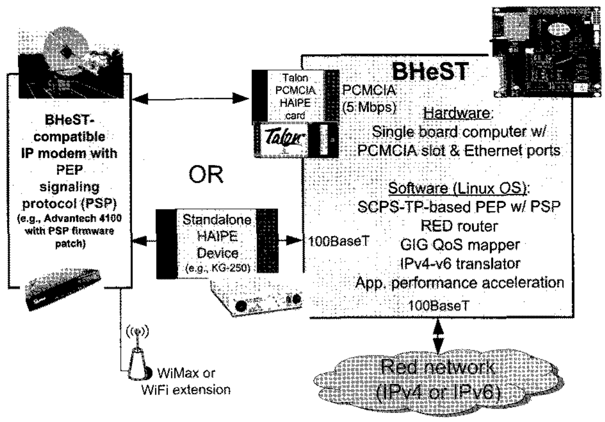


Fig. 8. Prototype integrated modem using COTS equipment.

Table 2. Comparison among various schemes.

Scenario	Throughput	Transfer time
Actual PEP	46.41 KBps (100%)	59.1 sec (100%)
Estimated PEP	38.32 KBps (82%)	71.4 sec (82%)
No PEP	29.7 KBps (63%)	94.1 sec (63%)

A major component of BHeST is the red side single board computer. Our prototype single board computer is Pentium M X86 based, and comes in the 3.5" PC/104 type of form factor. Features include a 10/100 BaseT Ethernet controller, integrated drive electronics (IDE) support for a hard drive, and two PCMCIA slots. We use the personal computer memory card international association (PCMCIA) slot to host the embeddable HAIPE Talon card made by L-3. The HAIPE PCMCIA Talon in turn connects to a universal serial bus (USB) style adapter which then converts to Ethernet. Keys may be loaded via a proprietary dongle on the Talon card which interfaces to the standard DS-101 data transfer device key fill. Our single board computer runs Linux 2.6 kernel and hosts high-performance networking software, such as TCP-PEP, QoS queuing, and IP version 4 (IPv4) to IP version 6 (IPv6) translation. By introducing a powerful general purpose processor into the red environment, we can offer better synchronization between red traffic and the black physical satellite modem environment.

V. CONCLUSION

In this paper, we have presented a comprehensive description of BHeST system design which includes many novel and practical features that are essential for a GIG-compliant system. The biggest contribution of this solution is its ability to maintain TCP PEP function in the presence of HAIPE and bandwidth-on-demand SATCOM links. Preliminary results based on our detailed simulation testbed of DVB-RCS and PSP show promising trends. Further research on prototype design, demonstration and performance evaluation will further prove the usefulness and effectiveness of BHeST for GIG.

ACKNOWLEDGEMENT

The authors would like to thank Mr. William Cook at Air Force Research Laboratories for his guidance and support of the work.

REFERENCES

[1] "Digital video broadcasting (DVB); interaction channel for satellite distribution systems," ETSI EN 301 790, European Telecommunication Standards Institute, Mar. 2003.

[2] B. Bennet, K. Quock, E. Summers, and M. DiFrancisco,"DVB-S2 technology development for DoD IP SATCOM," in *Proc. IEEE MILCOM*, Washington D.C., 2006.

[3] B. Bennett, K. Quock, M. Skowrunski, and M. Difrancisco, "Digital video broadcast return channel satellite (DVB-RCS) architectures and applications for the department of defense (DoD)," in *Proc. IEEE MILCOM*, Atlantic City, NJ, Oct. 2005.

[4] B. Bennet, D. Hannan, J. Marshall, and R. Gibbons, "WGS capacity using the DOD joint IP modem (DVB-S2, RCS)", in *Proc. IEEE MILCOM*, Washington D.C., 2006.

[5] "CIO John grimes: DoD policy for transmission of Internet protocol over DoD-leased and DoD-owned transponded satellite communication systems," DoD, Feb. 2006.

[6] High assurance Internet protocol encryptor. [Online]. Available: http://en.wikipedia.org/wiki/HAIPE

[7] Y. Zhang, "A multi-layer IP security protocol for TCP performance enhancement in wireless networks," *IEEE Trans. J. Sel. Area. Commun.*, vol. 22, no. 4, pp. 767–776, May 2004.

[8] G. Elmasry, J. Lee, M. Jain, S. Snyder, and J. Santos, "ECN-based MBAC algorithm for use over HAIPE," in *Proc. IEEE MILCOM*, Boston, 2009.

[9] A. Ayyagari and O. Brewer, "System and method for providing integrated services across cryptographic boundaries in a network," U.S. Patent 7 623 458, Nov. 24, 2009.

[10] T. Henderson, M. Duke, J. Megan, and S. Yi, "TCP performance enhancements for tactical networks," Boeing, Tech. Rep., Sept. 2005.

[11] "Space communications protocol specification (SCPS): Transport protocol (SCPS-TP)," CCSDS 714.0-B-1, Blue Book, May 1999.

[12] Space communication protocol standards. MITRE. [Online]. Available: http://www.openchannelsoftware.com/projects/SCPS

[13] J. Doffoh, R. Mereish, and M. Puckett, "Analysis and comparisons of acceleration protocols for TCP over satellite," in *Proc. IEEE MILCOM*, Atlantic City, NJ, Oct. 2005.

[14] B. Bennett, B. Jaspal, and F. Yao, "The next generation IP SATCOM: Exploration of IPv6 technology in global broadcast service technology refresh," in *Proc. IEEE MILCOM*, Atlantic City, NJ, Oct. 2005.

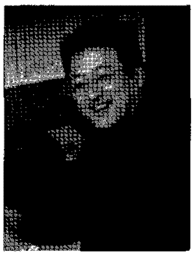
[15] ETSI, "Draft ETSI TS 102 462: Satellite earth stations and systems (SES); broadband satellite multimedia (BSM) services and architectures: QoS functional architecture," Mar. 2006.

[16] (1995, Dec.). Red/black installation guide. WBDG. Washington D.C. [Online]. Available: http://www.wbdg.org/ccb/FEDMIL/hdbk232a.pdf

[17] "Global information gridNet-centric implementation document: Quality of service (T300)," DISA, Dec. 2005.

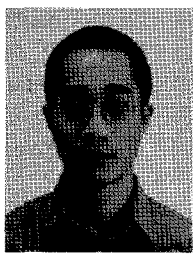
[18] O. Brewer, A. Ayyagari, and M. Foster, "Integrated services provisioning across cryptographic boundaries," in *Proc. IEEE MILCOM*, Washington D.C., 2006.

F. Dell Kronewitter received the B.S., M.S., and Ph.D. degrees in Mathematics from University of California Santa Barbara, Irvine, and San Diego, respectively, completing his studies in 2000. His thesis investigated noncommutative computer algebra approaches in linear algebra and control theory. His subsequent research has found pragmatic applications for novel algorithms which have resulted in superior deployed systems as well as several publications in journals and conferences. He has served as Reviewer and Session Conference Chair for IEEE MILCOM and IEEE CDC. He also has more than fifteen years of commercial experience designing communications systems and developing embedded networking software, including robotic mechatronic systems, POS systems, enterprise routers, carrier grade telecom analysis equipment, wireless MANET, sensor networks, and satellite communication equipment both GEO and LEO. He is currently with Argon ST, a wholly owned subsidiary of Boeing. He is a Senior Member of IEEE and American Math Society. His research interests include wireless networking, communication systems, graph theory applications, and complex emergent systems.



Bo Ryu has over 15 years as principal investigator in the area of communications and networking for various projects sponsored by DARPA, Army SBIR, Navy ONR, and Air Force SBIR. He is currently with Argon ST, a wholly owned subsidiary of the Boeing company, and is responsible for managing internal research projects, pursuing new government programs, and performing various government- and industry-sponsored projects in the areas of mobile ad hoc networking, sensor networks, satellite networking, information assurance, and network security. Previously, he was the Head of Network Analysis and Systems Department at HRL Laboratories. He is author/co-author of 30+ publications, and holds 5 U.S. patents issued. He received two performance awards for his technical achievements on DARPA's Adaptive C4ISR Node program, and is a recipient of a Meritorious Award from Raytheon in 2001 for technical performance recognition. He received his Ph.D. in Electrical Engineering from Columbia University in 1996.

Zhensheng Zhang received his Ph.D. in Electrical Engineering from the University of California, Los Angeles in 1989. He has over twenty years experience in design and analysis of network architecture, protocols and control algorithms with very strong backgrounds in performance analysis, and modeling and simulation of the communication networks. He is currently with Argon ST (formerly SDRC), Principal Engineer, Networking Research, serving as Principal Investigator for several DoD projects. Before joining SDRC, he visited Microsoft Research in the summer of 2002 and worked at Sorrento Networks, Department of System Architecture, for 2 years, responsible for designing the next-generation optical metro networks using the GMPLS control framework. Prior to Sorrento Networks, he was with Bell Laboratories, Lucent Technologies, focusing on research and development in wireless networks. He served as Editor of IEEE Transaction on Wireless Communications from 2002 to 2006. He served as the General Chair of Broadband Wireless Networking Symposium, October 2004. He has served as Guest Editor for the IEEE JSAC special issue on Overlay Networks, 2003 and the Journal of Wireless Networks issue on multimedia wireless networks, August 1996. He served as Member at Large of the IEEE San Diego section 2004 and as Chair of IEEE Communication Society, San Diego Chapter, 2004-2008. His research interests include wireless ad hoc networks and wireless sensor networks. He has given many invited talks and tutorials on wireless ad hoc networks at various conferences. He will serve as the IEEE Globecom2012 TPC Chair.



Liangping Ma received his B.S. degree in Physics from Wuhan University, Hubei, China, in 1998, and his Ph.D. degree in Electrical Engineering from the University of Delaware, Newark, DE, in 2004. He was with San Diego Research Center Inc. (later merged with Argon ST, Inc.), San Diego, CA from 2005 to 2009. Since then, he has been with InterDigital Communications, Inc., in King of Prussia, PA. His research interestes include cognitive radios, wireless sensor networks, wireless mobile ad hoc networks, and cellular networks, with emphasis on issues at the physical layer and the MAC layer.