

MITIGATING THE COST OF INFORMATION ASSURANCE IN THE SDR ENVIRONMENT

William T. Scott PhD General Dynamics C4 Systems 8220 E. Roosevelt Street
Scottsdale, Arizona 85257, William.T.Scott@gdc4s.com
James Kohler Department of Defense Washington DC
Greg Osborn General Dynamics C4 Systems.

ABSTRACT

The commercial Software Defined Radio (SDR) environment recognizes that all delivered services come with both benefits and costs. For inclusion, the benefit a new service brings must outweigh the costs, including services that are transparent to the user, such as Information Assurance (IA). The traditional view has been to reluctantly include IA services into devices because classical implementations of IA impose a large overhead penalty on bandwidth. The move to Internet Protocol (IP) based services on SDR devices changes the landscape. Internet Protocol Security (IPsec¹), the internet engineering task force (IETF) standard for securing IP traffic, supplies IA services by creating virtual tunnels and these virtual tunnels offer ideal places for compressing IP, transport and session layer headers. The packets generated by the IPsec protocol are also compressible. This paper presents the results of an implementation study that integrated packet header compression techniques into the SDR IA services. The IPsec services were based on the DoD version of IPsec the high assurance IP encryptor protocol (HAIPE®). The pre-encryption compression was based on the IETF RObust Header Compression standard (ROHC) request for comment (RFC) 3295². The post-encryption compression technique leveraged the deterministic format of the packets generated by IPsec protocol. The results of the study show that the combination of compression with the IA services results in an overall reduction of overhead. The improvement of bandwidth efficiency over the original Voice over IP (VoIP) packets was 30 bytes per packet allowing a VoIP application running 1200 baud MELP-e to be transmitted over a 1.5 kilobit wireless link (HF). These results indicate that a much more robust IA can be made available to the commercial market place, while allaying the concern that IA always comes at a cost to bandwidth.

1. INTRODUCTION

The short history of cell phones and SDR shows two trends: the number and complexity of multi-media applications hosted by platforms is growing, and these applications are adopting a common underlying communications protocol – IP.

There has been reluctance in the acceptance of IP based applications. Traditionally IP based applications, including

communications applications, operate in a high-bandwidth, fixed, wired infrastructure where protocol overhead is of little consequence. Such is not the case in the SDR environment. The mobile RF environment is bandwidth constrained. Even high capacity 3G and 4G cannot afford to be profligate with its limited capacity. SDR application providers face a choice between adopting standard IP based communication applications that carry considerable overhead or a bandwidth efficient application that conflicts with IP standards.

Multimedia applications carry with them liabilities that exacerbate the cost of communication overhead. Multimedia content inevitably involves intellectual property rights that must be protected. The potential of intercepting streaming videos or downloaded music is considerable and the onus for protecting that information will inevitably place liabilities on the service providers and SDR manufacturers. Both will be expected to supply and support IA features adding additional communication overhead on top of that added by IP. If IP is used as the standard communication protocol and IPsec as the standard IA protocol used to protect IP traffic then per-packet overhead for common applications such as VoIP can exceed 100 bytes as shown in **Figure 1**.

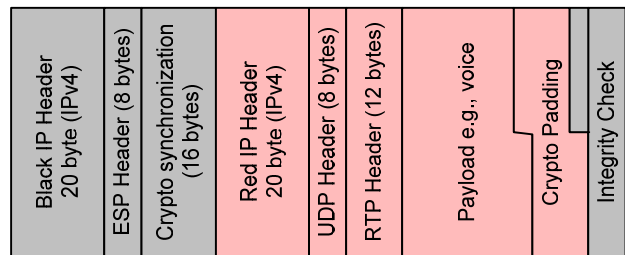


Figure 1 - IP and IPSEC Overhead

Providers and platform developers need not resign themselves to such high costs. Modern header compression techniques, especially Stateful Header Compression (SFHC), dramatically reduce the ratio of overhead to payload needed to support IP based communication. SFHC takes advantage of the redundant and deterministic characteristics found in the network, transport and application layers of the IP protocols. By sending redundant information only once and small deltas to update deterministic information SFHC greatly reduces bandwidth overhead.

The location of the SFHC peers has a significant impact on the ability to reduce overhead. SFHC peers at the end host need to preserve the IP header intact, thus they are limited to compressing upper layers only. COMSEC also impacts the placement of the SFHC functions. This paper's investigators have found that in both practice and theory, for IP based networks with IP based COMSEC, the ideal place to do header compression is at the network based IP-COMSEC function. Following sections detail the reasons for this conclusion.

2. IP PROTOCOL OVERHEAD

The IP environment is designed to allow communication between generic applications residing on hosts located anywhere on the Internet. The approach requires three levels of overhead: **application** overhead that tells peers critical information about the underlying payload, **transport** overhead that tells the peer the target application (UDP or TCP) and **host** overhead and tells the network needed information about how to get a packet to its target destination (IP).

2.1 Application Data

IP applications create and consume application data. Communication applications make tradeoffs between fidelity and bandwidth. Land line voice applications with little constraints on bandwidth encode the voice traffic into 64 kbps. While this provides excellent voice quality, it is not compatible with low bandwidth links that operate at less than 64 kbps. In order to place more voice calls on a link, cellular applications format voice traffic at rates of 8 kbps.

To reduce the bandwidth overhead even further the United States Department of Defense (DoD) Digital Voice Processing Consortium (DDVPC) selected MELP-e (Mixed-Excitation Linear Predictive enhanced) as the new 2400 bps Federal Standard speech vocoder. MELP-e is robust in difficult background noise environments such as those frequently encountered in commercial and military communication systems. It is very efficient in its computational requirements and operates with low power consumption making it ideal for portable systems. MELP-e supports rates of 600 bps, 1200 bps, and 2400 bps.

2.2 Application Overhead

IP applications must frame and format application data into packets suitable for IP. Applications utilize a packet size best suited for the desired service. Packet size selection is about balance. Relative to voice applications, larger packet sizes significantly reduce the overall throughput but adds to delay by forcing more wait time on the sender filling up the payload. This increases the delay in the voice call as the

time between packet arrivals is increased. To minimize these effects, voice applications typically implement small packet size. Smaller packet size also minimizes the impact of lost or dropped packets as there is less user information in each packet. The negative impact of smaller packet size is the increased overhead as each of the smaller packets requires the same overhead.

To reduce this per packet overhead, application may queue up several voice frames, sending them in a single packet. In doing so, the application trades additional delay for higher throughput.

2.3 Transport

SDR usually support multiple communication applications that can run concurrently, e.g., voice, instant messaging, and video streaming. The host must be able to handle multiple concurrent communication streams and does so through the transport layer. UDP and TCP protocols create platform specific communication pipes. Because of time sensitivity, most multimedia applications use UDP for their transport layer.

2.4 Networking

IP networks require additional overhead. The network needs to know the source and target hosts' IP addresses, the quality of service that should be applied to the packet, time-to-live and other necessary information.

2.5 Total IP Overhead

The application, transport and network protocol layers each contribute overhead to the VoIP packet. A VoIP packet usually contains an RTP header of 12 bytes, a UDP header of 8 bytes and an IP (IPv4) header of 20 bytes for a total of 40 bytes of overhead. When this is applied to very efficient codex algorithms such a 28 byte MELP-e voice packet (four padded frames), the protocol overhead is 142% as shown in Figure 2



Figure 2 - VoIP Overhead

While networking the overhead is necessary for the proper operation of the network, the additional overhead can reduce the number of calls that may be supported in bandwidth constrained environments.

3. INFORMATION ASSURANCE AND COMSEC

The growing demand for digital rights management support by SDR is forcing IA requirements on SDR vendors and service providers. Protection of data-in-transit is supplied by Communication Security (COMSEC).

Historically, COMSEC has been supplied by authenticating and encrypting the link between the handset and the service provider's network (SGSN in GPRS networks and RAN in UMTS networks.) Link encryption was sufficient when the communication was restricted to the providers' and SS7 networks, but the move towards IP networks forces a move to end-to-end protection driving IA to IP layers.

3.1 Information Assurance and Applications

Embedding COMSEC within applications is usually a poor fit. Though there have been examples where COMSEC has been embedded in an application, the applications usually are dependent on the platform to supply need COMSEC support such as key and certificate management. Supplying COMSEC functions that have an acceptable level of assurance at the application level is particularly difficult when applications share a platform and use common services. Achieving the needed level of information segregation is virtually impossible.

3.2 Information Assurance and IP

When multiple applications needing COMSEC share a platform, the better fit is to have COMSEC as an independent platform service. If delivered as a platform service then the corresponding communication layer is the IP layer, and if the COMSEC service is supplied at the IP the appropriate protocol is IPsec.

There are advantages to COMSEC as an independent, IP layer platform service. A short list of these benefits includes:

- COMSEC becomes end-to-end not hop-to-hop, improving overall security.
- Both commercial and DoD have developed standard for IP based COMSEC. Accepted and adopted standards greatly improve interoperability between vendors and platforms.
- An IP based COMSEC is consistent with the move towards IP based networks.
- The same COMSEC protocol is used by multiple applications and platforms increasing interoperability.
- Use of an IP based COMSEC avoids the increased latency and jitter necessitated by the multiple encrypt and /decrypt cycles of hop-by-hop COMSEC.

- Improved interoperability between vendors and platforms derived from the use of commercial and DoD standards for IP based COMSEC.
- Alignment with commercial and DoD move towards IP based networks.
- Lower cost of deployment and verification stemming from reuse of a common COMSEC solution across many applications and simplified key management.

As is all COMSEC, IP based COMSEC relies on a peer-to-peer relationship. The sending peer adds the IA services, such as confidentiality, integrity and authentication, protecting the data in transit. The receiving peer uses shared information to remove confidentiality services, authenticate the origin and verify the integrity.

4. HAIPE® AND IPSEC

The United States Department of Defense (DoD) in adopting an edge-to-core communication strategy that embraces IP, has developed and embraced the HAIPE³ protocol to provide end to end COMSEC across untrusted IP networks. HAIPE is the DoD version of IPsec. It supplies information assurance services such as integrity, authentication, confidentiality and replay detection. This paper explores the use HAIPE protocol as a COMSEC solution.

The commercial world's IA needs are virtually identical to those that have been addressed by HAIPE: separation of data, end-to-end protection and authentication of both source and destination hosts. HAIPE not only addresses the same set of IA needs, it is based on the commercial world's IPsec standard. Efficient bandwidth utilization techniques explored in this paper using HAIPE based COMSEC are easily generalized to IPsec based COMSEC.

There are two predominant HAIPE Interoperability Specification (IS): HAIPE IS 1.3.5, and an updated version HAIPE IS 3.X. HAIPE IS 3.X includes updates suitable for low bandwidth environments. The low bandwidth relevant updates introduced by HAIPE 3.X falls into two areas: 1) reduced overhead and 2) increased determinism which offers potential for improved header compression.

4.1 HAIPE Overhead

IP based COMSEC contains per packet synchronization overhead for the cryptographic engines. HAIPE overhead includes a sequence number, state variable, and if required authentication data. Figure 3 shows the header format. Those familiar with the RFC 4304 will recognize that the HAIPE format is compliant with RFC 4304.

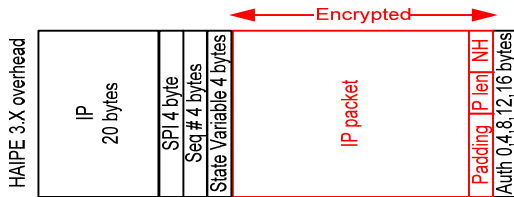


Figure 3 - HAIPE 3.X Packet Format

4.2 HAIPE and Plain Text Header Compression

IP based communications between streaming user applications (e.g. voice and video) result in significant redundancy and determinism in the IP, UDP and RTP protocol headers. These attributes present an ideal opportunity for effective compression.

Header compression is not a new idea. The IETF has defined ROHC with tailored profiles optimized for different applications (e.g. voice vs. data). Given the drive to standards, this paper's investigators adopted the IETF RFC 3095 ROHC for its SFHC

For the purposes of simplicity, the case discussed below uses ROHC of VoIP packets. Packets traveling between a compressor and a de-compressor are given a context identifier for which state memory is allocated for the IP/UDP/RTP headers at each end point. Each subsequent packet in the flow omits the underlying headers from the transmission from compressor to de-compressor. The 40 bytes of IP/UDP/RTP header are compressed to between 2 and 4 bytes.

By its nature, header compression is a peer-to-peer activity as are HAIPE functions. The security associations (SA) set up between HAIPE peers offer an ideal context for compression. There are three reasons for compression of Plain Text (PT) traffic across the SA virtual tunnel:

1. The HAIPE function expects well formed plain text IP packets, preventing the compression of the IP headers before arrival at the HAIPE function.
2. The SA between HAIPE peers is a logical tunnel. Logical tunnels, point-to-point connections, are ideal for aggressive PT compression.
3. The encryption performed by the HAIPE transmitter prevents any further compression of the encrypted data.

Peer HAIPE devices are required to hold state memory for each traffic flow. The de-compressor updates the state of the RTP time stamp and sequence number with each packet received. Replayed, corrupted or dropped packets, common in wireless networks, force the de-compressor to re-establish state with the compressor greatly reducing the efficiency of the compression.

These inefficiencies are reduced when used with HAIPE through Replay protection in which duplicate packets are dropped. Another method to reduce the impact on performance is to perform generic windowing on the RTP time stamp and sequence number allowing the de-compressor to exam and potentially correct the RTP time stamp and sequence number before updating the de-compressor state. Even so, the overhead penalty to re-establish ROHC state due to impaired communications is a significant technical issue requiring further investigation.

4.3 HAIPE and Cipher Text Header Compression

Once the HAIPE device encrypts the compressed IP packet, the resulting ESP payload is encapsulated in a new black side IP datagram. The HAIPE 3X header fields shown in Figure 3 are: IP header, SPI, and a 64 bit sequence number (the IV is the upper 32 bits of the sequence number). The IP header is constant per data flow and the sequence number is incremented on a per packet basis. The values are either redundant or deterministic for a given data stream thus amenable to header compression by the waveform link between the SDR and its radio access point. The waveform sets up a context associated with each cipher text traffic stream, sending the redundant header information once at context setup. For each subsequent packet of the data stream, the waveform sends a context id, cipher text payload, and delta values that reflect changes between the previous packet's deterministic field values and the current packet's values. A resynchronization process restores state disruption resulting from packet loss and/or corruption.

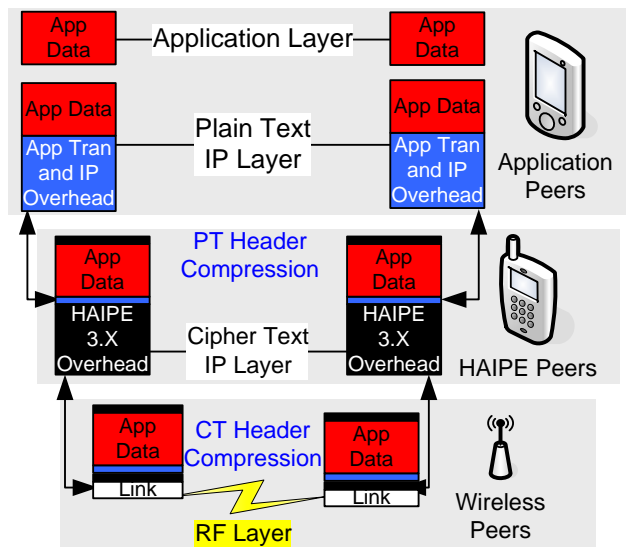


Figure 4 - Two Step Compression

The theoretical benefits of combining HAIPE 3.X and header compression are dramatic. 1200 MELPe⁴ encodes 45

milliseconds of voice into 54 bits (padded to 7 bytes). Four MELPe frames representing 180 milliseconds of voice produce a 28 byte payload. A 28 byte MELPe packet enclosed in standard RTP/UDP/IP headers results in a 68 byte VoIP packet as shown in Figure 5 - Comparative Packet Size. Encryption using HAIPE 3.X in tunnel mode produces a packet that is 104 bytes. However, using HAIPE 3.X with both CT and PT header compression produces a packet only 38 bytes in size, just 10 bytes over the original MELPe payload. The combination of header compression and HAIPE produces a COMSEC function that returns 30 byte that can be used for data as compared to the uncompressed and unencrypted plain text VoIP packet!

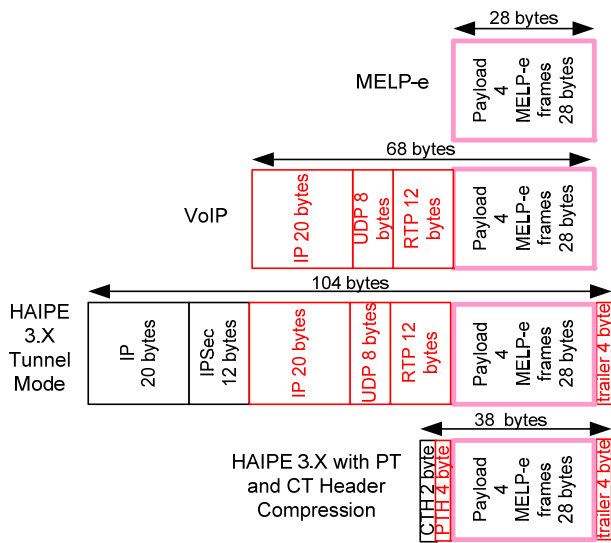


Figure 5 - Comparative Packet Size

5. IMPLEMENTED INFOSEC ARCHITECTURE

To reduce the theory to practices, we assembled a proof-of-concept wireless network. Essential features of our test wireless networking architecture are:

- Partial to full embedment of IP routing, COMSEC and waveforms into software defined radio
- Cipher Text routing between disparate waveforms
- Waveform CT Compression Service
- HAIPE PT Compression Service
- HAIPE as a universal COMSEC
- Suite B algorithms
- Representative user applications
- Interoperability with legacy and emerging COTS equipment
- Complete end-to-end control of applications, protocols, hardware and RF

Header Compression	IETF RFC 3095 (PT header compression)	HAIPE based Header compression CT header compression	
Routing	Half-Wits PT router	Half-Wits CT router	
Algorithms	AES Galois Counter Mode		
Waveforms	T-WWiN	HF	SATCOM
Applications	C2PC	IVOX	PolyCom

Table 1 - Components of Wireless Network

5.1. SDR Network test bed

With the background of the previous section in mind, the objectives of the network test bed are to:

- 1) Demonstrate integration of HAIPE 3.x into an SDR.
- 2) Implement and demonstrate benefits of HAIPE when combined with PT and CT compression across narrowband deployed waveforms.
- 3) Demonstrate interoperability of embedded HAIPE with third party HAIPE INE implementations over legacy narrowband data links.
- 4) Explore viability of HAIPE as a universal end-to-end COMSEC solution for heterogeneous networks.

The **First** objective is met by developing and integrating an embedded version of HAIPE 3.x into a General Dynamics Systems Software Defined Radio (SDR) platform. The **Second** objective is met by implementing a HAIPE PT Compression Service and a waveform optimized CT compression service into the test-bed SDR components. The **Third** objective is met by inserting and interoperating with existing HAIPE 3.x solutions from third party vendors. The **Fourth** objective is met by integrating multiple radio networks into a common black IP routable network that transported HAIPE protected IP packets where the HAIPE function used commercially available IA algorithms (AES Galois Counter Mode). Waveforms include the Tactical Wideband Wireless Network (T-WWiN) waveform⁵, SATCOM and HF. All three serial waveforms are adapted to transport IP traffic.

The test bed is comprised of five General Dynamics C4 Systems software defined radios (SDR) capable of running narrow and wideband waveforms with data link and network layer protocols, two half-duplex legacy PRC150 HF radios, a KG250 FI INE, and two software-based HAIPE supplied by the HAIPE Program Management Office (PMO). The General Dynamics C4 Systems SDR used in the test-bed is a black side variant of the legacy SDR described in previous work⁶. It includes a red Ethernet base-band interface protected with internal HAIPE, red and black side IP routing, modulation and demodulation (modem) functionality, and full duplex Radio Frequency

(RF) translation. Each RF channel can be configured through a Human Machine Interface (HMI) to operate as a distinct radio type.

A number of deployed waveforms have been adapted for use on the SDR radio. These waveforms include High-Data-Rate Tactical OFDM, SINCGARS ESIP, HaveQuick II, UHF SATCOM 181, 182, 183 “DAMA”, HF-ISB ALE, Link 11/TADIL-A, STANAG 4529 (HF NB Modem), VHF-FM, VHF-AM ATC, VHF/UHF-FM LMR, UHF-AM/FM/PSK, and Link-4A/TADIL-C. Of these supported waveforms, T-WWiN, HF and SATCOM were chosen for this demonstration. But given the approach followed, it is feasible to extend any of the supported waveforms to transport IP traffic.

Figure 6 depicts the mapping of network stack functionality to the primary hardware modules in the SDR for a single channel.

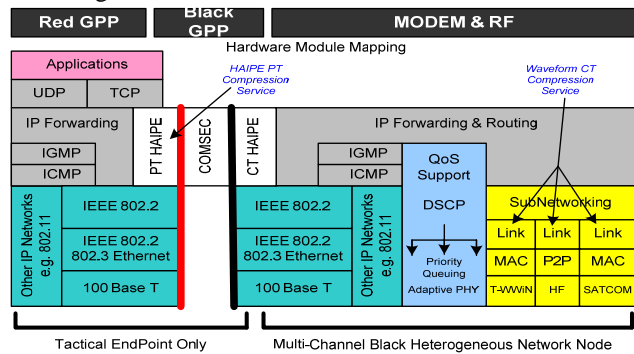


Figure 6 - SDR Internal Network Stack

6. COMPARATIVE TEST RESULTS

Empirically Measured Results

Over-The-Air Throughput Performance	1200 Baud MELPe over 2400 Baud HF	
	135 ms voice Pkt Size (bytes)	500 ms voice Pkt Size (bytes)
Voice Payload	21	81
Red VoIP packet	61	121
HAIPE protected VoIP packet	96	156
HAIPE protected Compressed VoIP packet	60-96	120-156
Compressed HAIPE protected Compressed VoIP packet	44-80	104-140

7. CONCLUSIONS

Results from our experiment show that:

- HAIPE based header compression offers significant bandwidth savings over traditional COMSEC techniques. The HAIPE protected packets transmitted over the waveforms, both legacy and modern, were, for our VoIP application, 30 bytes smaller than the packets generated by the host application.
- The strategic use of HAIPE SA as the basis for the compression peering demonstrates how COMSEC becomes integral to compression effectiveness, compressing the IP header as well as the transport and application headers.
- Use of the HAIPE standard to supply a common COMSEC across all waveforms increases interoperability and greatly simplifies integration with legacy stovepipe architectures. The approach demonstrated that the promise of true end-to-end security is practical and achievable even over existing infrastructure.
- The separation of the COMSEC from the waveforms turned the waveforms black. Once black, the waveforms were easily integrated into a black network using standard off-the-shelf routing techniques. Adoption of waveforms is not encumbered by COMSEC certification.
- The use of HAIPE as an end to end COMSEC solution allows packets to be easily routed between the black wired and wireless domain. Waveforms following this approach are easily tied into wired infrastructure such as the DoD’s GiG achieving true edge to core protection.
- COMSEC provided as a platform service, separate from waveform or routing applications, allows for rapid adaptation of new waveforms and inter-waveform MANET routing protocols without sacrificing security.
- The use of commercially available Suite B algorithms shows the solution is viable for both DoD and commercial environments.

8. FUTURE WORK

The work shown in our lab network can be extended to show how other HAIPE features support wireless networking. Specifically, HAIPE allows the bypass of type of service (ToS) bits. These bits can be used for prioritization by black side routing to supply Quality of service (QoS). Traffic marked with ToS bits indicating a higher sensitivity to delay could be routed over a path with lower delay while other traffic would be routed over lower priority paths, all without the black router having any access to the contents of the payload.

Our proof-of-concept test-bed employed a relatively simple static, four node black network. Future

investigations will look at extending the network architecture to reflect operational environments with node mobility, a large number of nodes and a percentage of intermittent and unreliable links. An advantage of the proposed architecture is that it cleanly distinguishes the black routing application from both COMSEC and waveform functions.

9. SUMMARY

The work presented in this paper shows that use of HAIPE as the common COMSEC for wireless networking creates considerable value for the wireless domain. The research showed that compressed HAIPE packets were 30 bytes smaller than the original VoIP packets, resulting in a COMSEC solution with reduced overhead.

This research was reduced to practice by leveraging a flexible network test bed incorporating General Dynamics C4 Systems software defined radios with embedded HAIPE 3.x and narrow/wide band waveforms connected with third-party radios and third party HAIPE devices. In this architecture, HAIPE encapsulated, compressed voice data was routed through a black network of disparate waveform links transporting compressed IP traffic. The result was an integrated heterogeneous black IP wireless network made up of both legacy and modern waveforms that, due to compression techniques, had very efficient payload to

overhead ratio and end-to-end COMSEC. The notion that HAIPE based COMSEC is an undo burden to wireless environments may be put to rest. We have shown that instead of being an onerous burden, the combination of HAIPE COMSEC and compression techniques greatly benefits bandwidth efficiency and makes internetworking possible and practical even with low bandwidth legacy serial waveforms.

- [1] S. Kent, IP Encapsulating Security Payload (ESP), IETF RFC 4303, December 2005
- [2] C. Bormann et al, RObust Header Compression (ROHC) Framework and four profiles: RTP, UDP, ESP, and uncompressed, IETF RFC 3095, July 2001
- [3] High Assurance Internet Protocol Encryptor Interoperability Specification Version 3.1.0 December 2006
- [4] Analog-To-Digital Conversion Of Voice By 2,400 Bit/Second Mixed Excitation Linear Prediction (MELP), MIL-STD-3005, 20 December 1999
- [5] J. Kleider, S. Gifford, K. Nolan, Derrick Hughes, and S. Chuprun, "Demonstrating Robust High Data Rate Capability on Software Defined Radio Using Anti-jam Wideband OFDM Waveforms," in *proc. of MILCOM*, Oct. 2005.
- [6] D Cohlman, G. Osborn, "Feasibility and Roadmap for SCA, Wideband, and Networking Technology Insertion Into A Fielded SDR", in *proc of MILCOM*, Oct. 2005.

Copyright Transfer Agreement: The following Copyright Transfer Agreement must be included on the cover sheet for the paper (either email or fax)—not on the paper itself.

“The authors represent that the work is original and they are the author or authors of the work, except for material quoted and referenced as text passages. Authors acknowledge that they are willing to transfer the copyright of the abstract and the completed paper to the SDR Forum for purposes of publication in the SDR Forum Conference Proceedings, on associated CD ROMS, on SDR Forum Web pages, and compilations and derivative works related to this conference, should the paper be accepted for the conference. Authors are permitted to reproduce their work, and to reuse material in whole or in part from their work; for derivative works, however, such authors may not grant third party requests for reprints or republishing.”

Government employees whose work is not subject to copyright should so certify. For work performed under a U.S. Government contract, the U.S. Government has royalty-free permission to reproduce the author's work for official U.S. Government purposes.