Internet Protocol Header Compression Technology and Its Applicability on the Tactical Edge

Bow-Nan Cheng and James Wheeler, MIT Lincoln Laboratory
Brian Hung, Defense Information Systems Agency

ABSTRACT

The increased usage of net-centric IP applications at the tactical edge has pushed DoD communications systems to maximize bandwidth efficiency amid a limited availability of RF spectrum. One method of increasing bandwidth efficiency (especially with the desire to move to IPv6), is the use of IP header compression (IPHC) to compress headers from the network layer and above into small identifiers before sending to the link layer. Although widely used in cell phone technology, the tactical edge provides some unique challenges to traditional IPHC techniques including highly dynamic links and link conditions due to potential jamming threats and difficult environments, multi-hop scenarios due to lack of infrastructure, and a highly diverse set of radio systems lacking interoperability. In this article, we examine two common IP header compression schemes, Robust Header Compression (RFC 5225) and IP Header Compression (RFC 2507) and one experimental scheme, MANET IP header compression, and identify their current use and applicability in the tactical edge. Furthermore, we identify some challenges in implementing header compression schemes in emerging systems.

DISTRIBUTION STATEMENT A: Approved for public release; distribution is unlimited IAW DoDD 5230.24, Distribution Statements on Technical Documents and DoD Directive 5230.9 (reference (f)) Clearance of DoD Information for Public Release. This work is sponsored by the Defense Information Systems Agency (DISA) through Air Force Contract #FA8721-05-C-0002. Opinions, interpretations, recommendations and conclusions are those of the authors and are not necessarily endorsed by the United States Government.

INTRODUCTION

In recent years, radio frequency (RF) spectrum allocated to Department of Defense (DoD) communication systems have become increasingly constrained due to higher demand on data rates and government spectrum re-allocation. Coupled with the desire for the DoD to move to an IPv6 (or dual stack IPv4/IPv6) network architecture where the IP header sizes increase dramatically, it becomes increasingly important to reduce IP header overhead sent over the air. The Internet Engineering Task Force (IETF) has explored IP header compression (IPHC) and produced several options, including RObust Header Compression (ROHC, RFC 5225 [1]), header compression over low-power IEEE 802.15.4 networks (RFC 4944 [2]), and others. While many of the techniques have been vetted through commercial vendors in industry, the tactical edge poses some unique challenges due to its disconnected, intermittent, and low-bandwidth (DIL) nature.

Figure 1 illustrates the issues associated with compressing IP headers at the tactical edge. These issues can be summarized in the following observations:

Multi-IP-hop nature: Traditionally, IP header compression protocols were designed for one-hop cellular networks. Tactical edge radio networks use mobile ad hoc network (MANET) routing protocols to route packets over multiple IP and RF hops in highly dynamic networks. When a next hop changes, traditional IP header compression protocols require additional message exchange to share context information for compression per flow per IP hop. It is unclear whether traditional IP header compression protocols can handle the amount of network churn.

HAIPE encryption: Tactical radios typically employ encryption using high assurance IP encryptors (HAIPEs) or other communications security (COMSEC) devices. This requires plaintext (PT) header compression in addition to ciphertext (CT) header compression, leading to additional IP header compression context setup. This effect is most pronounced on small packets such as TCP acknowledgments.

Disconnected, intermittent links: Tactical radios often experience highly variable link quality. IP header compression protocols that require synchronization of header information could potentially fail in environments where links are not stable and experience high loss.

Multicast (one-to-many) traffic: Tactical edge networks typically operate in a one-to-many paradigm. This is evident by almost all Link 16 and other waveform message-sets being broadcast in nature. As tactical edge communications moves to IP, broadcast and multicast will need to be supported. Traditional stateful IPHC schemes like ROHC and RFC 2507 were designed primarily for unicast point-to-point links.

Although there are several challenges with performing IPHC in tactical edge networks, which are intermittent and error prone, the

0163-6804/13/$25.00 © 2013 IEEE

potential gains are evident. Studies performed in 2008 by the Cooperative Association for Internet Data Analysis (CAIDA) [3] have shown that in core networks, 55 percent of IPv4 traffic and 90 percent of IPv6 traffic traversing the Internet are under 200 bytes in size. Even just using these numbers, the potential bandwidth savings per packet for IPv4 and IPv6 UDP and TCP packets on the core networks is 10–30 percent. While traffic on the tactical edge is different, one can imagine voice over IP (VoIP) and periodic situational awareness packets (both small packets) would benefit from reduction in load for bandwidth constrained environments of tactical radios.

IP header compression protocols come in two broad categories: stateful and shared-state (often called stateless). Stateful protocols like ROHC and RFC 2507 maintain a mapping of header information to a context identifier (CID) for every IP hop and every flow. Shared-state protocols (MIPHC and IEEE 802.15.4 header compression), in contrast, have preconfigured mappings on every node, requiring little to no coordination.

In this article, we survey two industry-backed IP header compression schemes: ROHC version 2, (RFC 5225) and IP Header Compression (RFC 2507) and one experimental scheme, MANET IP header compression (MIPHC), identifying the strengths and weaknesses of each protocol as well as considerations for integrating IPHC into current and emerging tactical edge radio systems. We briefly describe each of the three IP header compression protocols, and compare and contrast each while we examine implications of applying IPHC to current and emerging DoD radio systems and potential use cases. Finally, we conclude the article.

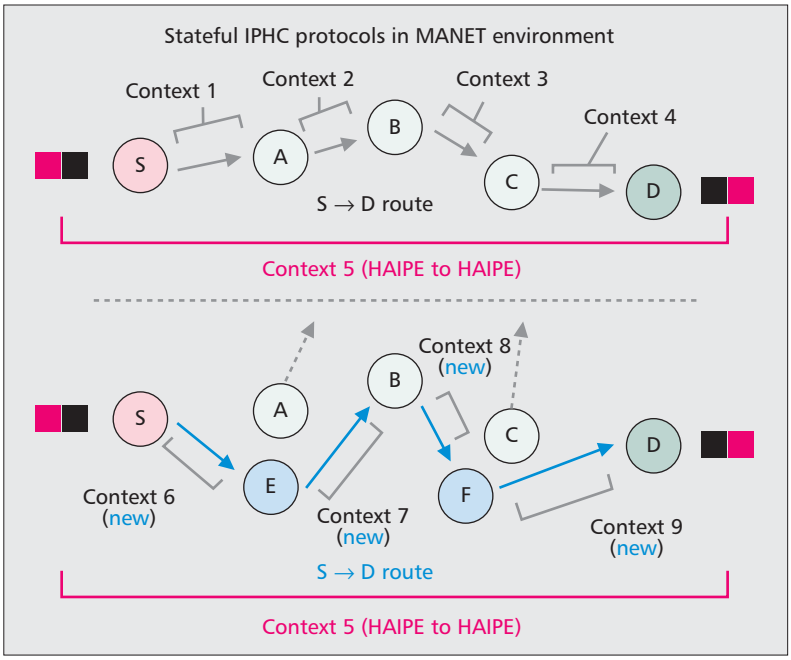

Figure 1. *Stateful IPHC schemes like ROHC and RFC 2507 set up context hop by hop for every reroute.*

IP Header Compression Protocols Overview

In this section, we overview the basic functionality of RFC 2507, ROHC version 2, and MIPHC.

IP Header Compression

IP Header Compression (RFC 2507) [4] was one of the first IPHC schemes developed, extending the work done in Van Jacobson TCP header compression [5] to compress IPv4, IPv6, and UDP in addition to TCP headers on a per link basis. Although it is intended for use on point-to-point links, most of the elements work the same on a broadcast medium, and the specification includes suggestions for how to implement it for non-point-to-point links. The compression operates by grouping packets into streams based on certain key fields of the headers (source IP, destination IP, protocol, and port numbers being the most common).

To initiate compression of headers for each packet stream, full headers carrying the context identifier (CID) are transmitted over the link. Both the compressor and decompressor store almost all header information and CID mapping in a context table. Subsequent packets use this context table to send compressed headers, omitting certain fields that are not expected to change frequently. Any change in the omitted header fields results in the compressor sending another full header to update the context at the decompressor. As long as the context is the same at the compressor and decompressor, headers can be compressed and decompressed successfully. Because packet loss is expected in wireless networks, compression mechanisms need to be able to protect against packet loss. These mechanisms differ for UDP and TCP streams.

Packet loss in TCP streams is handled much the same as Van Jacobson TCP Header Compression. But rather than relying on TCP's built-in reliable packet delivery for error recovery, RFC 2507 uses the "twice" algorithm [4]. Certain TCP fields (sequence number, TCP window) change from packet to packet in a predictable fashion. These fields are represented in the compressed header as deltas from the previous value. When a compressed header is received, the decompressor will compute the TCP checksum and compare it to what would be expected if the compression context were up to date. If they fail to match, it is assumed a lost packet caused the context to not be updated. The delta is used to recompute and repair the context. This change from RFC 1144 makes this method much better on medium-speed error-prone links such as wireless.

For UDP and non-TCP streams that are not well protected by sequence numbers and checksums, an identifier called a generation is added to the full and compressed headers. This identifier is incremented whenever the context associated with the CID changes. When the decompressor receives a packet with a generation that does not match the one stored in the context for a particular packet stream, the packet must be discarded or stored until a full header is received. To speed up decompressor context

recovery from the loss of a full header, full headers are sent periodically with an exponentially increasing period after a change in context until an upper limit. In this way, RFC 2507 ensures that context desynchronization does not occur for long periods of time due to packet loss.

In tactical edge networks, HAIPE devices are typically used to provide COMSEC to radios. In this case, RFC 2507 is not only used hop by hop, but HAIPE to HAIPE. Figure 2 conceptually depicts the headers compressed by RFC 2507 for a Real-Time Transport Protocol (RTP) packet with HAIPE devices. Because RFC 2507 does not support RTP compression, only the original UDP and IP headers (28 bytes if IPv4, 48 bytes if IPv6) are compressed to approximately 4–6 bytes on the red side. On the black side, ESP headers and IP headers are compressed. Additionally, RFC 2507 builds and maintains separate context state on a per IP hop and HAIPE to HAIPE basis.

RFC 2507 has been recommended by the Third Generation Partnership Project (3GPP) and 3GPP2 standards committees for use in 2.5G and 3G mobile phone networks. Satellite modem manufacturers have also adopted it for use on satellite communications (SATCOM) links. Although there are newer protocols that might work even better, it would be a good fit for providing header compression of IPv6 traffic for both SATCOM and line-of-sight (LOS) wireless links.

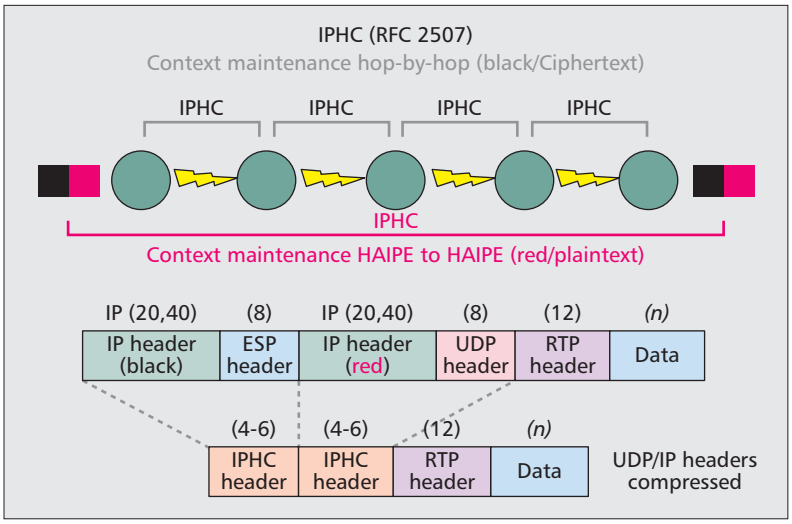

Figure 2. *IPHC state maintained hop by hop.*

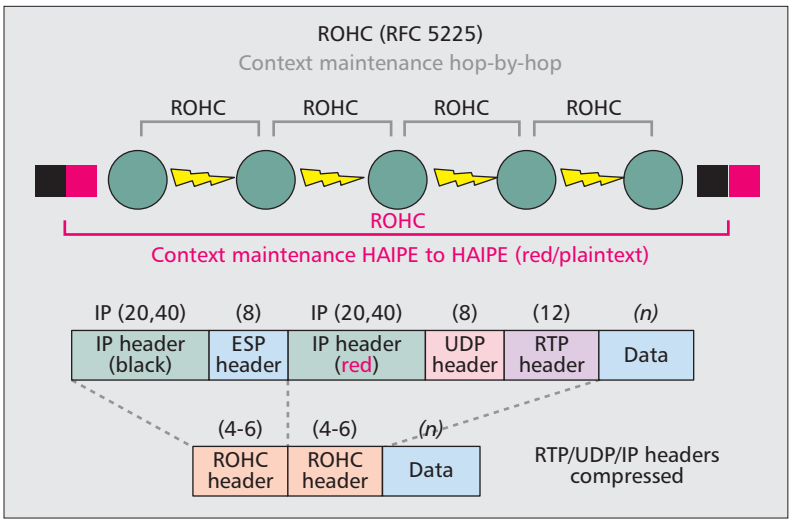

Figure 3. *ROHC state maintained hop by hop.*

ROBUST HEADER COMPRESSION VERSION 2

Robust Header Compression — ROHC [6] was designed to perform over high packet loss links such as wireless links. It supports most IP header formats including IPv4 and IPv6, UDP, RTP, and Encapsulation Security Protocol (ESP). ROHCv2 [1] defines a second version of the profiles found in RFC 3095. The ROHCv2 profiles introduce a number of simplifications to the rules and algorithms that govern the behavior of the compression endpoints. It also defines robustness mechanisms that may be used by a compressor implementation to increase the probability of decompression success when packets can be lost and/or reordered on the ROHC channel. Unless otherwise noted, all references to ROHC refer to ROHCv2.

Similar to RFC 2507, ROHC builds state between the compressor and decompressor by sending full and incremental headers periodically. In ROHC, both the compressor and decompressor have two different operational states,and both compressors and decompressors start in the lowest compression state and attempt to work toward the higher state The transitions between states do not need to be synchronized between the compressor and decompressor. The two compressor states are the Initialization and Refresh (IR), and Compressed (CO). The two decompressor states are No Context (NC) and Full Context (FC). Occasionally, the decompressor will enter a Repair Context (RC) state if it is unable to decode certain packets.

ROHC also has two modes of operation: unidirectional and Bidirectional Mode. The states described above are the same in all modes of operation. Compression with ROHC must start in U-mode. Transition to the Bidirectional mode can be performed as soon as a packet has reached the decompressor and the decompressor has replied with a feedback packet indicating that a mode transition is desired.

Figure 3 conceptually depicts the headers compressed by ROHC (using the RTP/UDP/IP profile) for a RTP packet using HAIPE devices end-to-end. The original RTP, UDP, and IP headers (40 bytes if IPv4, 60 bytes if IPv6) are compressed to approximately four to six bytes on the red side. On the black side, ESP headers and IP headers are compressed. Additionally, ROHC builds and maintains context state on a per IP hop basis. Maintenance of RTP headers can be expensive due to its highly dynamic nature. In terms of adoption and usage of both ROHCv1 and ROHCv2, the 3GPP and 3GPP2 standards committees have recommended ROHC for use on High Speed Packet Access (HSPA), Long Term Evolution (LTE), and Evolution Data Optimized (EV-DO) mobile phone networks. Satellite modem manufacturers have also adopted it for use on SATCOM links.

MANET IP Header Compression

IRFC 2507 and ROHC were designed primarily for single wireless IP hop networks where context setup and maintenance is fairly stable. MANET environments potentially have multiple IP hops, constant next-hop routing changes, and high packet loss. Combining these factors make constant context setup and maintenance difficult. To mitigate the issue, MIPHC [7] was developed.

MIPHC is a shared-state/shared-context header compression protocol derived from concepts found in [8], stripped of 802.15.4-specific items and generalized to support both IPv4 and IPv6. In contrast to ROHC and RFC 2507, MIPHC compresses layer 3 IP headers only. And while it can be combined with stateful end-to-end layer 4 and above header compression protocols, MIPHC is a standalone protocol. MIPHC was designed to remove the need to build new compression context for every IP hop within a MANET. Although it does not achieve the same compression ratio as stateful compression methods such as ROHC, it achieves gains due to not needing to build compression context on a hop-by-hop basis.

In MIPHC operation, a shared context table that maps a CID to the first three octets of IPv4 addresses and the network portion (first 64 bits) of IPv6 addresses are preconfigured at each router running MIPHC, much as routing protocol timers are configured. Figure 4 illustrates the compression ratio of the IPv4 and IPv6 headers through MIPHC. Since pure MIPHC only compresses IP headers and does not exchange state/context information, the gains are not as great as with ROHC (20-byte IPv4 and 40-byte IPv6 headers to 8- and 22-byte MIPHC headers).

MIPHC compresses IP headers at each wireless IP hop, leaving end-to-end compression for layer 4+ headers to other protocols like ROHC. When MIPHC is coupled with ROHC end to end (MIPHC/ROHC), only one context is set up end to end, and ROHC compression takes place going from an uncompressed interface to a wireless MIPHC compressed interface. Additionally, ROHC decompression and context state is maintained when a packet is moving from a wireless interface to an uncompressed interface.

It is expected that when MIPHC is coupled with ROHC (MIPHC/ROHC), ROHC will handle compressing layer 4+ headers. ROHC is normally used on two ends of a single link; however, when integrated with MIPHC, it is used only on the initiating and terminating routers. Any MANET router may be an initiating, intermediate, or terminating Router for a given IP subnet based on whether the subnet is reached by that router through a compressed or an uncompressed interface.

Figure 5 conceptually depicts the headers compressed by MIPHC/ROHC (using the RTP/UDP/IP profile) for an RTP packet using HAIPE devices end to end. The original RTP, UDP headers (20 bytes) are compressed to approximately 4–6 bytes using ROHC, while IP headers are compressed to 8 and 22 bytes for IPv4 and IPv6, respectively. On the black side, ESP headers are compressed using ROHC and IP headers compressed using MIPHC.

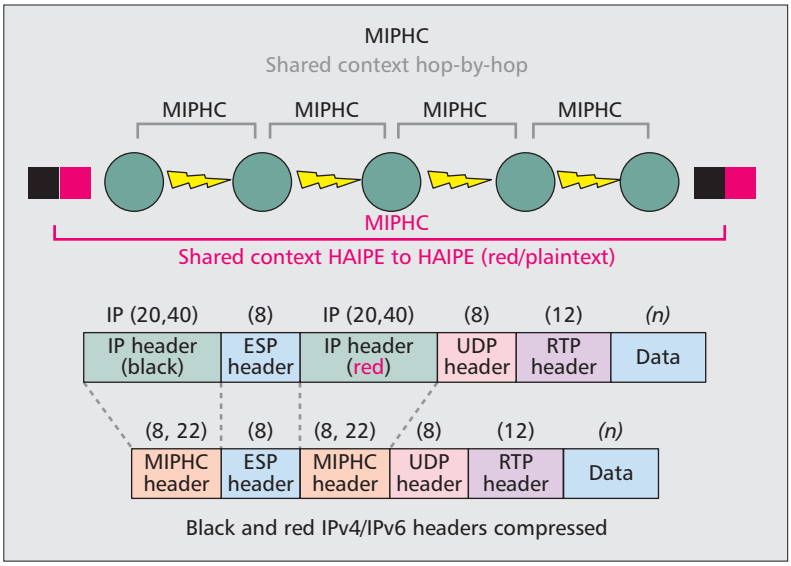

Figure 4. *MIPHC uses shared state hop by hop.*

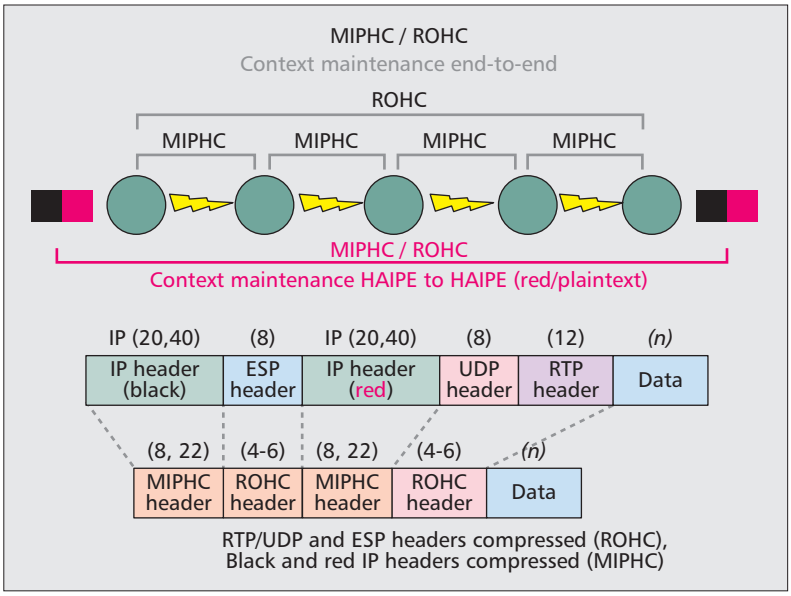

Figure 5. *MIPHC/ROHC uses shared state hop by hop and maintains context end to end.*

Summary

Table 1 compares the characteristics of the three protocols and current implementations. In comparing the protocols, there are several key distinctions:

- ROHC yields the highest compression ratio followed by RFC 2507, but both require state maintenance hop by hop.
- MIPHC by itself produces the lowest compression gains, but is the simplest protocol and requires no state/context exchange.
- Although ROHC can be used for multicast, the RFC is not clear on how it would be implemented. RFC 2507 describes potential usage with multicast traffic. MIPHC is inherently designed to support MANET environments and supports multicast.
- ROHC and RFC 2507 were not designed for multihop environments like the tactical edge.

- MIPHC hop by hop with ROHC end to end can potentially yield gains, but the trade-off is complexity.

Although each protocol has its trade-offs, understanding the operating conditions and underlying link characteristics are important in choosing the one with the best fit.

IPHC Considerations at the Tactical Edge

Although utilizing IP header compression can reduce load and potentially provide greater delivery success in tactical networks, and previous work [9] has examined its usability in the global information grid (GIG), there are several special considerations when dealing with DoD tactical edge networks. In the following subsections, we attempt to highlight some of the implications of applying IP header compression on current and emerging DoD tactical edge systems.

Single-Hop vs. Multihop Networks

Most header compression protocols in use commercially were designed primarily for one-IP-hop networks. Context mappings are built dynamically for every IP hop per IP flow. In dynamic tactical edge networks that use MANET routing protocols, every next hop change (assum-

	IPHC (RFC 2507)	ROHC (RFC 5225)	MIPHC (experimental)	MIPHC/ROHC (experimental)
RFC type	Standards track	Standards track	N/A	N/A
RFC status	RFC 2507	RFC 5225	N/A	N/A
Authors' organization(s)	LUT/SICS, Telia Research	Ericsson	MITLL	MITLL
Compression type	Stateful/replace	Stateful/replace	Shared state/elision	MIPHC: shared state/elision ROHC: stateful/replace
Layers compressed	Layer 3+	Layer 3+	Layer 3 (IP)	MIPHC: Layer 3 (IP) ROHC: Layer 4+
Profiles available	UDP/IP, IP, ESP/IP	RTP/UDP/IP, UDP/IP, IP, ESP/IP	IP	MIPHC: IP ROHC: RTP/UDP, UDP, ESP
IP version support	IPv4, IPv6	IPv4, IPv6	IPv4, IPv6	IPv4, IPv6
Designed for multihop	No	No	Yes	Yes
Compression range	Hop-by-Hop	Hop-by-Hop	Hop by hop	MIPHC: hop by hop ROHC: end to end
Multicast support	Yes	Yes	Yes	Yes
Minimum compressed header	UDP/IPv4: 75% ESP/IPv4: 82% IPv4: 75% UDP/IPv6: 79% ESP/IPv6: 83% IPv6: 93%	RTP/UDP/IPv4: 10% UDP/IPv4: 54% ESP/IPv4: 50% IPv4: 45% RTP/UDP/IPv6: 46% UDP/IPv6: 46% ESP/IPv6: 50% IPv6: 73%	IPv4: 10% IPv6: 33%	IPv4: 10% (MIPHC) RTP/UDP/IPv4: –35% (M/ROHC)* UDP/IPv4: –11% (M/ROHC)* ESP/IPv4: –14% (M/ROHC)* IPv6: 33% (MIPHC) RTP/UDP/IPv6: 2% (M/ROHC) UDP/IPv6: –10% (M/ROHC)* ESP/IPv6: –6% (M/ROHC)*
Maximum compressed header	UDP/IPv4: 82% ESP/IPv4: 90% IPv4: 85% UDP/IPv6: 83% ESP/IPv6: 87% IPv6: 95%	RTP/UDP/IPv4: 98% UDP/IPv4: 96% ESP/IPv4: 96% IPv4: 95% RTP/UDP/IPv6: 98% UDP/IPv6: 96% ESP/IPv6: 96% IPv6: 98%	IPv4: 60% IPv6: 45%	IPv4 60% RTP/UDP/IPv4 78% UDP/IPv4 68% ESP/IPv4 68% IPv6 45% RTP/UDP/IPv6 62% UDP/IPv6 50% ESP/IPv6 50%
Implemented in	3G/4G	4G	Experimental	Experimental

* Negative compression ratios are a net increase in header size

Table 1. *IP header compression protocol comparison.*

ing the MANET routing protocol uses IP) requires a new context to be set up. Recent work [10] has shown in simulation that ROHC and RFC 2507 perform sufficiently in dynamic environments of constantly changing links, but suffer from medium access issues like 802.11 backoff timers. Additional work is needed to understand whether a protocol like MIPHC is needed instead of using traditional ROHC and RFC 2507.

Fixed-Length Frames

Implementation of IP header compression with link layers that use a fixed frame size (also sometimes referred to as a cell) has some special considerations. Such link layers may either fill frames with multiple packets or packet fragments, or use padding bits to fill out the fixed size in cases where packets or fragments do not fill the frame. Even if the link layer puts multiple packets or fragments in a single frame, this may depend on the rate of packets being sent as typically there is a timeout value, at which point a frame will be padded and sent as opposed to waiting for more data. In such cases, reducing the packet size using header compression may not reduce the actual bandwidth used since padding bits may be added as needed to form the fixed frame size.

Unicast vs. Multicast Operation

IP header compression mechanisms and considerations differ depending on whether the traffic is unicast or multicast, and most standards and implementations focus on unicast traffic. In environments where a significant percentage of traffic is expected to be multicast, including multicast-based routing protocols, consideration needs to be given to an implementation's ability to handle multicast efficiently.

Multicast requires unidirectional header compression operation. As such, the RFC 2507 *full header timer* and ROHC *IR timers* configuration is important, since these timers determine how often full header data is sent and therefore available to MANET nodes that have not previously received it. A balance must be found between setting these timers too short, resulting in using bandwidth for full headers or IR more than necessary and for too long, resulting in new MANET nodes (or corrupted contexts) going longer before receiving a full header or IR and therefore being able to decompress multicast traffic.

Multi-Access Networks

Conceptually, point-to-point links are fairly simple when it comes to CID space/ROHC channel in that a single point-to-point link forms a single CID space/ROHC channel. It is important to note that the CID is selected by the compressor, so the issue for multi-access networks is identified in RFC 2507, which states:

The major difficulty with multi-access links is that several compressors share the CID space of a decompressor. CIDs can no longer be selected independently by the compressors as collisions may occur. This problem may be resolved by letting the decompressors have a separate CID space for each compressor. Having separate CID spaces requires that decompressors can identify which compressor sent the compressed packet, perhaps by utilizing link-layer information as to who sent the link-layer frame.

This is not stated in ROHC RFCs, but the issue is the same. Essentially the "CID space," for ROHC is the ROHC channel. Thus, the end result is that for multi-access networks, the ideal implementation is to establish a unique RFC 2507 CID space or ROHC channel based on the source link layer address (i.e., Ethernet medium access control, MAC).

This concept provides some additional potential benefits with regard to ROHC in that one ROHC parameter that is established on a per-channel basis is whether or not small CIDs or large CIDs will be used in a given channel. If each MAC address pair is a separate ROHC channel, there is more potential to be able to use either small CIDs or a range of large CIDs that only use one byte. If we extend this concept to a multicast-based routing protocol such that each source MAC sending to a routing protocol's well-known multicast address is a separate channel, this channel could use small CID zero resulting in no CID byte at all in the ROHC header. This would be especially beneficial since such routing protocol traffic is continuous.

Wired multi-access networks provide a more predictable environment with respect to the number of expected CIDs than wireless multi-access networks do because wired networks have a fixed broadcast domain. Wireless multi-access networks, however, operate such that broadcast domains are dynamically created and broken as devices move in and out of range of each other.

Medium Access Constraints

Although header compression can reduce network load significantly in networks, medium access constraints can reduce its effectiveness. In the case of 802.11, when collisions are detected, the protocol initiates a backoff procedure that waits a certain amount of time before initiating a random backoff. The total wait time per attempt is not dependent on packet size and is on the order of a few hundred to a few thousand microseconds depending on network congestion. This wait time is significantly greater than the compressed header transmit time, and as a result, roughly the same number of packets are delivered with and without compression. Because more compressed packets fit in the fixed size 802.11 queue, the result is higher delay to send out larger numbers of packets. With many military radio systems, medium access constraints have the potential to negate many affects of header compression.

Header Compression on Routing Protocols

Different routing protocols use broadcast, multicast, or unicast traffic, or a combination of these. Some use their own protocol encapsulated in IP, while others use UDP/IP. With UDP/IP and IP-only profiles enabled, multicast and unicast traffic from routing protocols should operate properly with IP header compression. Unless IP header compression context setup

In environments where a significant percentage of traffic is expected to be multicast, including multicast-based routing protocols, consideration needs to be given to an implementation's ability to handle multicast efficiently.

Since IP header compression manipulates the IP headers, potentially including checksums, systems that provide hardware checksum offload may not work as expected. Such offload may simply be ineffective and/or may actually interrupt communication if the hardware offload mechanism is not "ROHC aware."

and so on negatively impacts a routing protocol's formation of neighbor relationships and/or exchanging of routes in a timely manner, no specific exclusion of routing protocol traffic should be required.

Hardware-Based Checksum Offloading

Since IP header compression manipulates the IP headers, potentially including checksums, systems that provide hardware checksum offload may not work as expected. Such offload may simply be ineffective and/or may actually interrupt communication if the hardware offload mechanism is not "ROHC aware." Configuring such systems to disable the use of checksum offload may be required.

QoS Functions

Quality of service classifies/marks IP packets and manages transmission queues based on priority and/or bandwidth allocation and so on. When and how each QoS function acts on a packet within a system's protocol stack/buffers in relation to when and where IP header compression occurs can impact QoS operation. This may also be true of other functions that act on packets as they are transmitted and received. The interaction with and/or impact on such functions needs to be considered.

Because header information is stripped by IPHC protocols prior to being put onto the device (IPHC is between the network and link layers), and because queues are often configured and maintained on devices (Ethernet, etc.) or implemented internally on DoD tactical radios, QoS information such as type of service (TOS) and source/dest IP address must be preserved for applying queue discipline. Two methods for achieving this include:

- A new method to parse compressed packets at the link layer for TOS and remap contexts to IP addresses
- A "side-channel," to pass per packet information down to the link layer with uncompressed information

The second method is preferred since the first method requires all ROHC/RFC 2507 functions to be replicated. If IPHC is used in a subnet routing environment (i.e., radio net layer 2 routing) where QoS is used to prioritize forwarding, mechanisms are needed at layer 2 to read QoS during context initialization or from compressed headers. Another alternative is that the layer 2 frame needs its own "priority" field whose values can be mapped to IP QoS values prior to or during header compression. Otherwise, all compressed headers will be treated as the same priority — care is needed that once header information is lost, QoS can potentially be nullified. If the IP router implementing IPHC is physically separated from the layer 2 radio (e.g., with Ethernet as with HNW or NCW), the issue described above regarding mapping QoS in some way to layer 2 also includes a need to propagate QoS markings over this link. In the case of Ethernet, this could include the use of 802.1P class of service (CoS) marking in an 802.1Q virtual LAN (VLAN) header but would require the radio to support 802.1Q/P.

Fragmented IP Packets

IP packets are fragmented when they are too large to fit within one maximum transmission unit (MTU) for a given link layer. One key factor with IP fragments is that higher-layer headers and/or extension headers are all in the first fragment, while additional fragments contain only data payload after the fragment header. As a result, higher-layer and/or extension header data in other than the first fragment cannot be examined to determine the proper packet stream for the fragments. Furthermore, fragments may be out of order at the compression point or take different routes through a network such that a compressor cannot rely on seeing the first fragment before other fragments. Consequently, RFC 2507 and ROHC do not compress IP fragments, not even with an IP-only profile. The end result with ROHC is that IP fragments may be sent with the ROHC uncompressed profile, which actually adds at least a one-byte ROHC header to each fragment. Applications, systems, and networks should therefore be configured to avoid fragmentation whenever possible when IPHC is used.

Radio-to-Router Separation and Header Compression

There has been a big push in recent years to physically separate the radio (one RF hop) functionality from the router (multiple RF hops) functionality. Because DoD tactical radios typically rely on IP headers to perform prioritization, flow control, and so on, care should be taken to either implement IPHC schemes on the radio after these functions are performed, or provide a mechanism to pass metadata with full header information between the radio and the router on a per packet basis.

HAIPE/IPSec Tunnel Mode and Transport Mode

RFC 2507 and ROHC both address the compression of ESP/IP headers that represent the ciphertext (CT), a.k.a. "black side," of the HAIPE or other IPSec device. The compression of plaintext (PT), a.k.a. "red side," IP headers (including RTP, UDP, etc.) before HAIPE/IPSec encapsulation in ESP is addressed specifically for ROHC in RFCs 5856, 5857, and 5858. Future HAIPE devices will highly likely support some of the common header compression schemes. It is important to note that because HAIPE also uses padding to conceal the true length of the unencrypted payload to protect against traffic flow analysis, the percentage traffic reduction achieved by header compression is typically lower than those not protected by HAIPE.

IANA has assigned the protocol number 142 to ROHC, so the "next-level" protocol field of the ESP header would use 142 to indicate that the next header is ROHC, as opposed to 4 if it were tunneled IPv4 or 41 if it were tunneled IPv6. Both RFC 5858 and the HAIPE IS 4.1.0 specification reference the use of protocol number 142 in the ESP header. There do not appear to be any standards or other ongoing work related to supporting IPHC other than ROHC over

IPSec. Based on this, red-side header compression appears to be limited to ROHC and requires compliant hardware/software.

Packet Segmentation

The segmentation protocol defined in ROHC (RFCs 3095 and 4995) is inefficient and requires in-order delivery of ROHC packets; ROHCv2 supports out-of-order delivery. ROHC segmentation is not intended to replace link layer segmentation, which should be used when available and needed. ROHC segmentation should only be used for occasional packets with sizes larger than the link layer can handle, assuming the link layer will not segment the packets. This can occur with some ROHC and ROHCv2 IR headers when both ROHC-specific and most original IP header info is sent. Ideally, applications would send packet sizes that allow for worst-case ROHC headers within the link layer's MTU, or the link layer would perform its own segmentation.

Protocol Vulnerability

Stateful protocols that establish context mappings are potentially open to attacks. While the ROHC specification [1] identifies potential attacks, it explicitly mentions that an intruder having the ability to inject arbitrary packets at the link layer raises additional security issues that dwarf header compression issues. Because tactical edge networks often carry time-sensitive information, attack mitigation techniques are needed. Reference [11] quantifies the effects of several potential ROHC attacks and suggests several simple strategies such as adding authentication to critical headers (IR, FEEDBACK) to protect context setup and maintenance.

Conclusion

Military networks connected to the GIG at the tactical edge are increasingly constrained in available bandwidth. The desire to move to an all-IPv6 infrastructure exacerbates this issue. IP header compression is one method that can potentially increase bandwidth efficiency at the tactical edge. Traditional approaches in industry have focused on single-hop networks, and build and maintain state/context over the link. While effective for cellular networks, tactical edge networks operate in a disconnected, intermittent, low-bandwidth, and multihop environment. As a result, several special considerations must be explored. In this article, we survey two industry-backed IP header compression schemes: Robust Header Compression (RFC 5225) and IP Header Compression (RFC 2507`); and one experimental scheme, MANET IP header compression (MIPHC), identifying the strengths and weaknesses of each protocol. Additionally, a review of several potential issues and areas to address in integrating IP header compression into existing DoD tactical edge waveforms is given. Overall, IP header compression techniques show promise in the overall goal of reducing bandwidth consumption at the tactical edge, but work is still needed to implement and evaluate these on existing radio systems.

References

[1] G. Pelletier and K. Sandlund, "RObust Header Compression Version 2 (ROHCv2): Profiles for RTP, UDP, IP, ESP and UDP-Lite," IETF RFC 5225, 2008; http://tools.ietf.org/html/rfc5225.

[2] G. Montenegro *et al.*, "Transmission of IPv6 Packets over IEEE 802.15.4 Networks," IETF RFC 4944, 2007; http://tools.ietf.org/html/rfc4944.

[3] CAIDA, "Packet Size Distribution Comparison Between Internet Links in 1998 and 2008," Mar. 2008; http://www.caida.org/research/trafficanalysis/pkt_size_distribution/graphs.xml.

[4] M. Degermark, B. Nordgren, and S. Pink, "IP Header Compression," IETF, RFC 2507, 1999; http://tools.ietf.org/html/rfc2507.

[5] V. Jacobson, "Compressing TCP/IP Headers for Low-Speed Serial Links," IETF RFC 1144, 1990; http://tools.ietf.org/html/rfc1144.

[6] C. B. *et al.*, "RObust Header Compression (ROHC): Framework and Four Profiles: RTP, UDP, ESP, and Uncompressed," IETF RFC 3095, 2001; http://tools.ietf.org/html/rfc3095.

[7] B.-N. Cheng *et al.*, "MANET IP Header Compression," to appear, *IEEE MILCOM '13*, 2013.

[8] J. Hui and P. Thubert, "Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks," IETF RFC 6282, 2011; http://tools.ietf.org/html/rfc6282.

[9] E. Ertekin and C. Christou, "Internet Protocol Header Compression, Robust Header Compression, and Their Applicability in the Global Information Grid," *IEEE Commun. Mag.*, Nov. 2004.

[10] B.-N. Cheng *et al.*, "A Comparison of IP Header Compression Schemes in MANET," under review, 2013.

[11] B.-N. Cheng and S. Moore, "Securing RObust Header Compression (ROHC)," to appear, *IEEE MILCOM '13*, 2013.

Biographies

Bow-Nan Cheng (bcheng@ll.mit.edu) is a member of technical staff in the Airborne Networks Group at MIT Lincoln Laboratory. His research interests include design, development, prototyping, and test and evaluation of next generation routing solutions for airborne backbone and tactical networks. Recent work has focused heavily on radio-aware routing, which leverages link layer information at the network layer to enhance multihop MANET routing. He received M.S. and Ph.D. degrees in computer systems engineering from Rensselaer Polytechnic Institute and holds a B.S. degree in electrical engineering from the University of Illinois at Urbana-Champaign.

James Wheeler (jim.wheeler@ll.mit.edu) is a network architect with BT Federal, Inc., and has been a consultant to the Airborne Networks Group at MIT Lincoln Laboratory since 2008. Having received his B.S. in mechanical engineering and a commission as a U.S. Air Force Officer from Norwich University in Vermont in 1986, he served at what was then the Electronic Systems Division of Air Force Systems Command at Hanscom AFB, Massachusetts, supporting the acquisition of both airborne and ground radios. He has subsequently worked in various technical roles related to communications and networking, accumulating over 25 years of experience with both commercial and DoD systems. Among other industry certifications, he has been a Cisco Certified Internetwork Expert (CCIE No. 8194) since 2001.

Brian Hung (brian.t.hung.civ@mail.mil) is an electronics engineer at the Enterprise Wide Systems Engineering Branch of the Defense Information Systems Agency. He provides task and technical leadership in identifying and analyzing issues, developing reference architectures and interoperability guidance for tactical communications, networking, and network security across the Department of Defense. He received his Professional Engineer degree in electrical engineering from the University of Southern California, M.S. degree in computer engineering from the University of South Carolina, and B.E. degree in electrical engineering from the University of Canterbury.

IP header compression techniques show promise in the overall goal of reducing bandwidth consumption at the tactical edge, but work is still needed to implement and evaluate on existing radio systems.