International Journal of Energy, Information and Communications
Vol. 2, Issue 2, May 2011

Header Compression Method and Its Performance for IP over Tactical Data Link

Yongkoo Yoon[1], Suwon Park[1], Hyungkeun Lee[2],
Jong Sung Kim[3], Seung Bae Jee[3]
1Dept. of Electronics and Communications Engineering,
2Dept. of Computer Engineering,,
Kwangwoon University, Seoul, Korea
ykooyoon@gmail.com, {spark, hklee}@kw.ac.kr
3Tactical Data Link PMO
Agency for Defense Development, Seoul, KoreaA
jskim_add@yahoo.com, asherjee@gmail.com

Abstract

Header compression is necessary for IP over tactical data link such as Link-16. In this paper, a novel header compression method for IP over tactical data link is proposed. And the monolithic message is also proposed for the efficient IP packet transmission of the tactical data link message. An indexing method is used for transmission of typical IP packets. In addition, the function of transmitting ACK to the compressed header is added in order to compensate the disadvantage of the UDP application. For monolithic message, the proposed header compression method outperforms 90.7% for IP packet transmission and maximum 95.8% for tactical data link message compared to existing Link-16.

Keywords: *Tactical data link, link-16, IP, Header compression*

1. Introduction

Modern war concept is changing from the platform centric warfare to the network centric warfare. The quantity of owned platforms and weapons do not guarantee the victory of the war. Situation awareness (SA), real-time command and control capability, and precise attack to targets are more important. In the network centric warfare, a surveillance system, command and control system, and attack system are networked. And, the situational awareness is shared among them. Thus, joint and precise attack can be achieved. [1]

There has been a need using IP (internet protocol) contents on a tactical data link. The advantages of IP over a tactical data link are as follows. First, tactical data link systems such as Link-16, Link-4A, Link-11, and the like, can be easily integrated. Second, new services can be easily and efficiently created by using open API (Application Programming Interface). Third, broadband tactical communication networks can be achieved. In the military communication network, the IP-based services can be popular like the commercial communication networks. Fourth, various tactical data such as multimedia tactical data can be easily introduced. The IP over the tactical data link can provide both raw tactical data and multimedia tactical data such as voice and image. By using those tactical data, the probability that can defeat the enemy in the war can be increased.

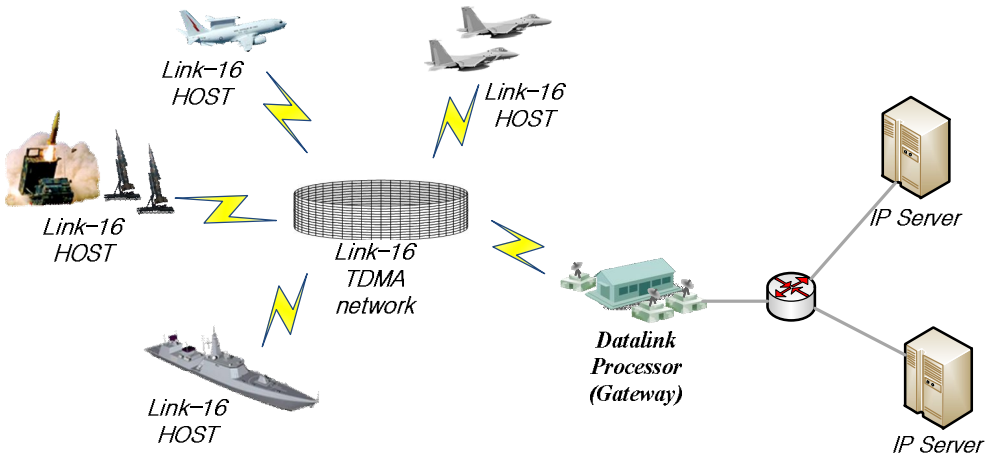


Figure 1. Network Model of IP over Link-16

Figure 1 shows a network model of IP over Link-16. Link-16 hosts using their own time slots are connected each other through Link-16 TDMA (Time Division Multiple Access) network. DLP (Data Link Processor) is a gateway between a Link-16 TDMA network and an IP network, and makes possible to communicate between a unit in Link-16 TDMA network and an IP server within an IP network.

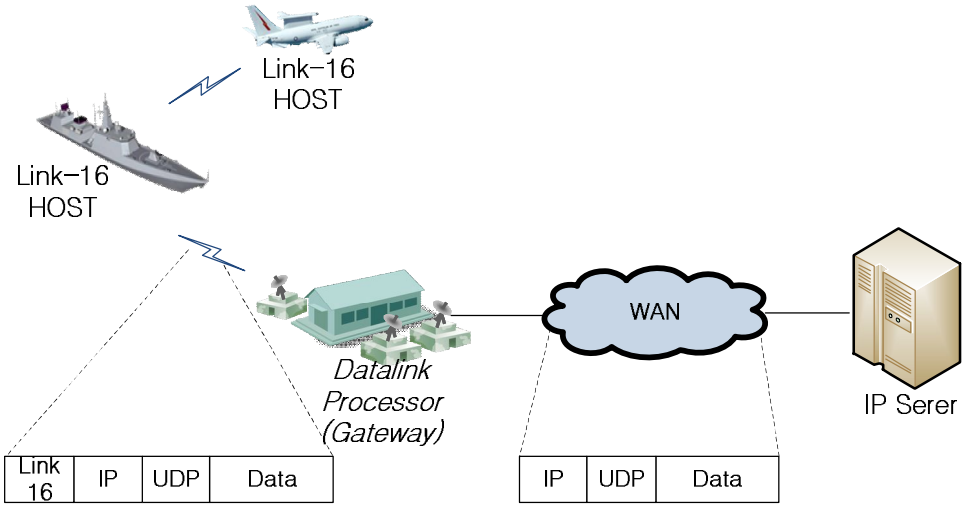


Figure 2. UDP/IP packet header for IP over Link-16

Figure 2 describes an example of a data transmission for IP over tactical data link such as Link-16. A host in a Link-16 TDMA network communicates an IP server located in either the internal Link-16 TDMA network or the external IP network connected through the DLP. The former is an intra-network case, and the latter is an inter-network case. In the TDMA network,

a transport layer header, a network layer header and a Link-16 header are sequentially attached to the payload.[3] In the inter-network case, a data payload from a Link-16 unit passes through the DLP, which transforms it to an IP packet, and delivers it to the external IP network.

2. Problem statements

2.1 Header overhead

Link-16 has four modes of data packing to a time slot; STDP (STandard Double Pulse), P2SP (Packed-2 Single Pulse), P2DP (Packed-2 Double Pulse), and P4SP (Packed-4 Single Pulse). STDP, P2SP/P2DP and P4SP transmit 210, 420 and 840 bits per a time solt, respectively. Transmitting data on IP over Link-16 is one of a tactical data link message (Fixed-J series) and a typical IP application message. The tactical data link message is composed of one to eight words, and each word is 70 bits.[4]

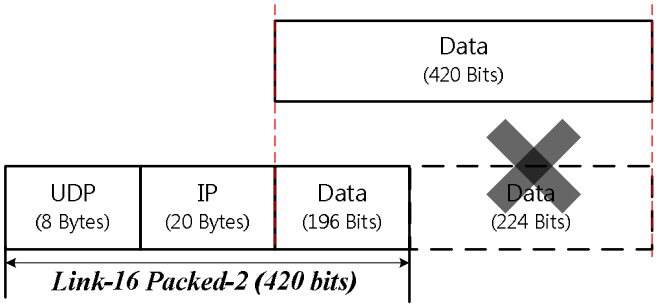


Figure 3. Data transmission inefficiency generated by a UDP/IP header

For the IP over Link-16, the transmission efficiency can be low. That causes from small transmission rate of the Link-16 and the large header size of an IP packet. For example, If a Link-16 host transmits data with the packed-2 mode, 6 words (about 53 bytes) are transmitted within a timeslot. A UDP/IP header is 28 bytes. Headers and data use about 53% and 47% of the transmission capacity, respectively. It is very inefficient because more than half of the transmission capacity is used for transmitting headers. In order to reduce the inefficiency of IP over tactical data link, UDP/IP header for an IP packet should be compressed.

2.2 Header compression

Figure 4 describes a header compression method for IP packet transmission over Link-16. Because the header of an IP packet is too large, the IP packet moves to the header compression layer that compresses it to the minimum size. The header compression layer should reduce the total size of the headers for IP packet such as UDP and IP headers, and output a compressed header. The original headers should be recovered based on the transmitted compressed header at the corresponding receiver.

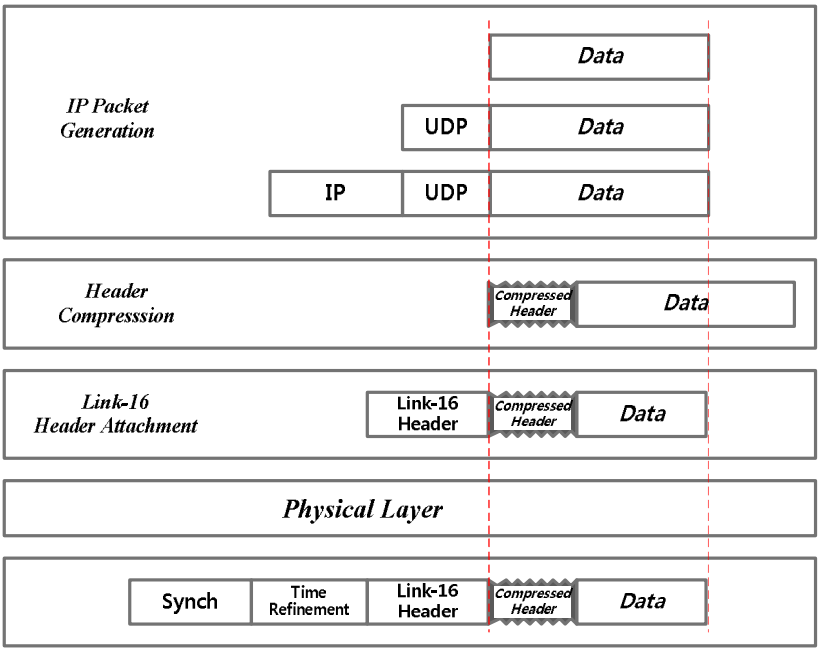


Figure 4. Header compression layer for IP over Link-16

3. Conventional solutions

In order to reduce the overhead of header in the field of wired or wireless communications, especially, for IP applications, there have been many studies for a long time. RFC 2507 and RFC 2508 are popular header compression algorithms.[5] They use delta coding which transmits the difference of the previous header and current header.[6][7] Even though the compression efficiency is high, they are vulnerable to packet errors that are common for all kinds of delta coding. That is, if a packet is erroneous, then the consecutive packets are not reliable.[8] However, ROHC (Robust Header Compression: RFC 3095) is strong due to not delta coding but LSB (Least Significant Bit) encoding, and data compression ratio is good.[9] Recently, it was studied as ROHCv2 (RFC 4995, 4996, 5225) and it was applied to 3GPP LTE (Long Term Evolution), that is one of 4G Mobile Communication candidate technologies.[9]

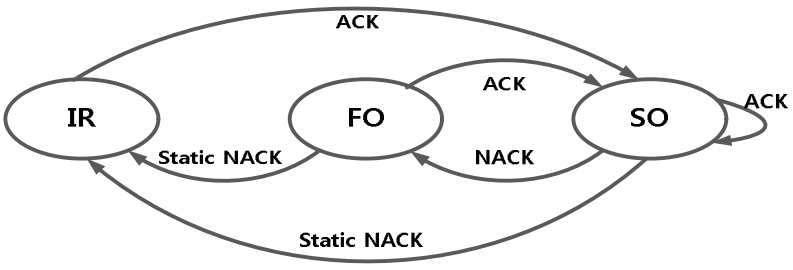


Figure 5. Finite State Machine (FSM) of ROHC compressor

ROHC with the best compression efficiency is used in commercial mobile communications. Figure 5 shows the FSM (Finite State Machine) of ROHC compressor. By using the feedback information from the compressor to the decompressor, the error of the compressed packet is checked. IR (Initializing and Refresh), FO (First Order), SO (Second Order) indicate the form of the compressed packet which a compressor transmits. IR is a full header that is transmitted when a compressor starts a connection. SO is a compressed packet which is transmitted after the transmission of unerrored IR. FO is a compressed packet which is transmitted in case that an error of the SO packet was detected.

The robustness against packet errors and the high compression ratio of ROHC are caused from the adaptive change of operation mode. ROHC has three operation modes. First, U-mode (Unidirectional mode). It is the method being designed in order to operate in the unidirectional channel without the feedback channel. Second, O-mode (Optimistic mode). It operates in the bidirectional channel. The compressor transmits an SO packet without ACK. Then, if an error of the packet is detected in the SO state, by using NACK, FSM is changed to FO or IR. Third, R-mode (Reliable mode). In the SO state, R-mode receives ACK and NACK of all compressed packets. The transfer efficiency is high in the O-mode, and the reliability is high in the R-mode.

4. Proposed Header compression method

4.1 Header compression

Two kinds of message can be transmitted on IP over a tactical data link such as Link-16. One is a tactical data link message, and the other is a typical IP packet. Link-16 message is a fixed format J-series message consisting of one to eight words. Each word is composed of 210 bits. The IP packet payload is one of audio, image, text, tactical data, and the like.

After the header compression layer processing, the compressed header for the tactical data link message in the intra-network case is given as shown in Figure 6.

(a) More fragment = '0'

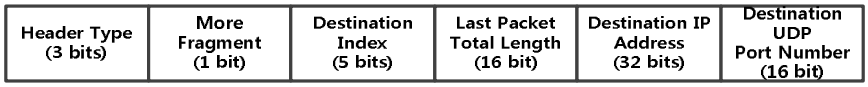
(b) More fragment = '1'

Figure 6. Compressed header format for intra-network case

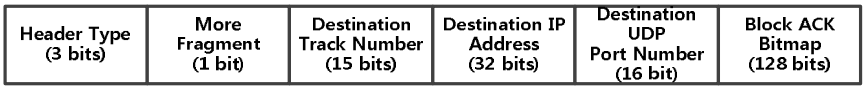
The header type field indicates the kind of a compressed packet. It is a 3-bit information as shown in Table 1. The monolithic message field indicates whether all of a message is transmitted within a time slot or not. The message length field indicates the number of words for a J-series message. It is used for recovering the total length value of IP header. The boundary point field indicates the boundary position when two messages are transmitted within one time slot. It prevents the consecutive error of packets.

Table 1. Header types

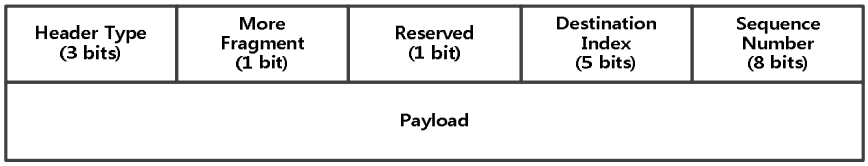
Header Type	Description
000	Tactical datalink message transmission
001	IP packet transmission(ACK mode)
010	IP packet transmission(NACK mode)
011	Client connection request
100	ACK request
101	Server IP packet transmission(ACK)
110	Server IP packet transmission(NACK)
111	Reserved



(a) Connection request



(b) Response



(c) IP packet transmission

Figure 7. Compressed header format for inter-network case

An IP packet over a tactical data link is delivered by using a point-to-point communication. Figure 7 is the compressed header format for an IP packet. It is composed of the connection request, response, and IP packet data transmission. A unit willing to transmit an IP packet sends the connection request packet which contains the information including IP address and port number, and an index number of the destination unit. The destination index of 5-bit information used in a receiver identifies its own packet. After a receiver receives a connection request packet, it sends a response packet after setting transmitter information. If the response packet with the assigned index number is received, the transmitter sends a packet.

The proposed header compression method can use the ACK as shown in Table 1 in order to complement the disadvantage of UDP protocol.

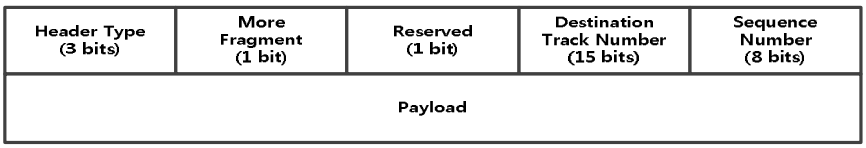


Figure 8. Compressed header format for data transmission at a gateway

Figure 8 is a compressed header format for data transmission from IP server at a gateway. The server uses the connection request and the response packets, too. Instead of the index number, the server uses TN (Track Number) for its data transmission. The 5-bit index number can identify 32 connections, but 15-bit TN can identify 32768 connections. In general, a client connects to small number of servers, but a server connects to large number of clients. Thus, in the proposed scheme a client identifies 32 servers by using the index number, and a server identifies 32768 clients by using the TN.

4.2 Header decompression

The objective of compression is to transmit reduced information and to restore the original from it. Within UDP and IP headers, the fixed field is removed, and the varying field is used for compression. After decompression, all of the fields including fixed and varying fields should be restored. Most of compressed protocols classify their fields into either fixed field or varying field.[6][7][8] Version, Header Length, Service Type, TTL, and Protocol fields are classified as fixed fields. The compression block of a transmitter does not transmit them after the initial transmission. They are restored at the decompression block at the corresponding receiver. In the Link-16 network, it is assumed that the constitutional units know IP addresses corresponding to TN's. Thus, the source address need not be transmitted. The destination address field is compressed during the connection request procedure and transmitted. The checksum field substitutes 12-bit CRC of Link-16. The length field and fragmentation field are remained. For the tactical data link message transmission, the length field is compressed to the message length field within the compressed header.

4.3 Example of header compression and decompression

The procedure of tactical data link message transmission using the proposed header compression method is shown in Figure 9(a).

A tactical data link message on IP over Link-16 is classified into one of three types of compressed packets.

- When there is no message in a buffer, the compressed packet (1) is a packet for new message.
- The compressed packet (2) is a packet with a monolithic message set to 1 and for enhancing the transmission efficiency.
- The compressed packet (3) is a packet composed of both a final fragment of a message remained in the buffer and a new message.

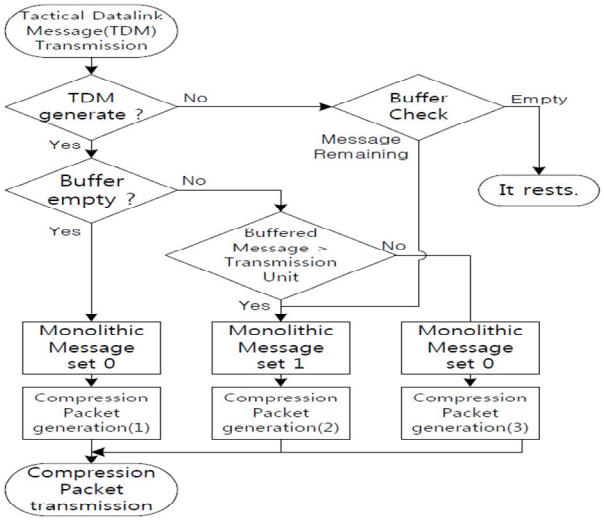
Figure 9(b) describes the tactical data link message reception. According to the Monolithic Message field value and Boundary Point field value, the received message is classified into one of three types of packets. By using a context and a received compressed header, the original header can be restored. The context is known in advance. The checksum of transport and network layer, and Identifier value is restored at the receiver. Because they are not fragmented, the tactical data link message sets the Fragment offset value to '0'. The Length field is set by the unit of byte.

Figure 10 indicates a procedure where the shipboard receives the tactical data link message which an air-fighter transmits. An air-fighter generates the message composed of the random number of words (for example, 3 or 6 words). The header type is set to 000. As to the first message, since being the message consisting of 3 words, the Message Length field is set to 010. As to the Monolithic field and Fragment Point field, the packet in which the message transfer starts is set to 0. After receiving the compressed packet, the shipboard confirms the Message Length and allocates 210 bits to a buffer. And a payload 193 bit except header is stored in the buffer. As to shipboard, getting a transmission of the second compressed packet, next message can know the message composed of 5 words (Message Length in Second Packet). And since the Fragment Point is 17 (decimal number), 17 bits except header are transmitted to a buffer and the previous message is decompressed. When generating third compressed packet, the transmitter calculates the remaining data size of the second message. If data size remaining more than data size which can be transmitted in the time slot is big, the Monolithic Message field is set to '1'. If this field is set to '1', the Message Length field and Fragment Point field are converted to a payload. The receiver getting a transmission of this packet stores a buffer in a payload directly.

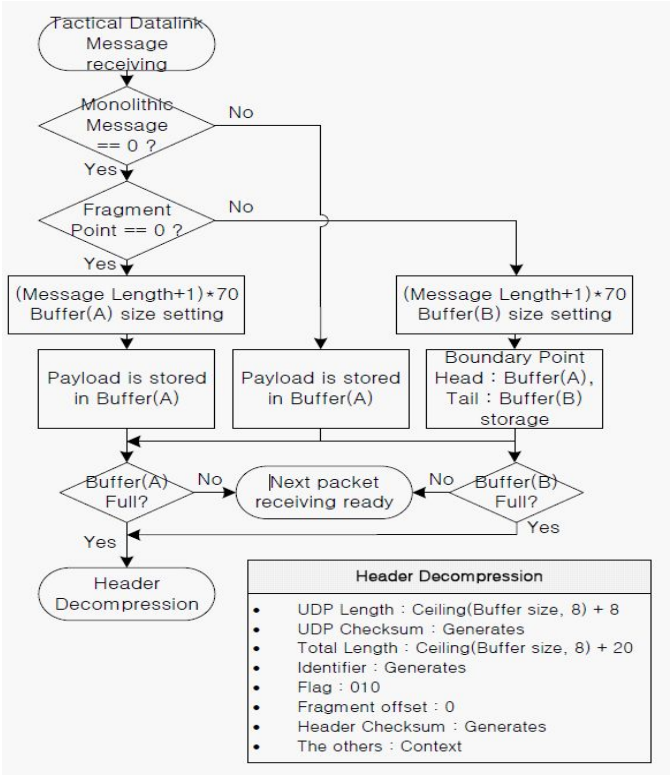
Figure 11 is transmission and reception procedures of an IP packet. Figure 11(a) describes the IP packet transmission. A destination unit should be identified and a connection should be checked whether it is set or not. In case of no configuration, a connection request packet is transmitted. After the establishment of the connection, fragmented packets are sequentially transmitted, where the More Fragment bit of the last packet is set to 0. Figure 11(b) describes the IP packet reception. The IP packet is received based on a point-to-point communication. Therefore, it is important that deciding whether the received packet is its own or not. If it is not its own, it is discarded. According to the connection request and ACK request, it is classified as (3). The connection request packet saves the received information as a context used for header decompression. As to the ACK response packet, if the 128-th or the last packet is received, the received packet is transmitted. Feedback information is not transmitted if the ACK response mode is not used.

Fig 12 indicates the step for the IP packet transmission between an air-fighter and a shipboard. After the header type is set to 010 and inputting the destination information, the air-fighter wishing the IP packet transmission transmits a connection request packet. Here, the index number which can take the place of IP address is assigned and transmitted. In the example, it assigned to '0'. The shipboard acquiring a transmission of the connection request packet transmits the response packet.

The example which transmits the IP packet after finishing the connection request was shown in Figure 13. An air-fighter sets the header type for the IP packet transmission to 001. After confirming the fragmentation of a packet, the More Fragment field is set. The index number assigned in the connection request is stored and transmitted. At this time, since the sequence number is increased from '0' by one, data recovery using the block ACK is made. The sequence number is one of 0 to 127. 127 packet transmissions were finished, or if the transmission of the fragmented packet is completed, the block ACK Request packet is transmitted (a header type of 100). By using the sequence number, a receiver makes the error check. If the block ACK request packet is transmitted, by using the bit map of 128 bits, it transmits the error location. In the example, 6 packets were transmitted. The second and the fifth packet are erroneous. Therefore, the block ACK bit map is transmitted to 010010.



(a) Transmission procedure



(b) Reception procedure

Figure 9. Transmission and reception procedure of tactical data link message

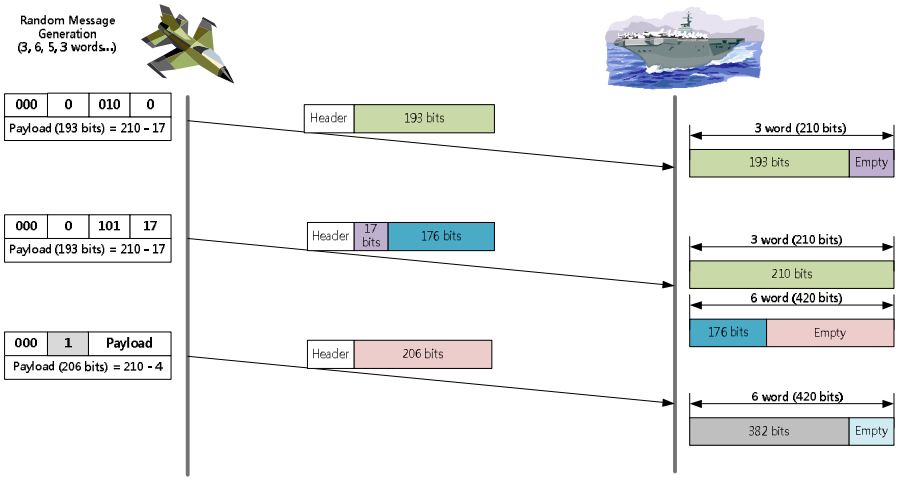
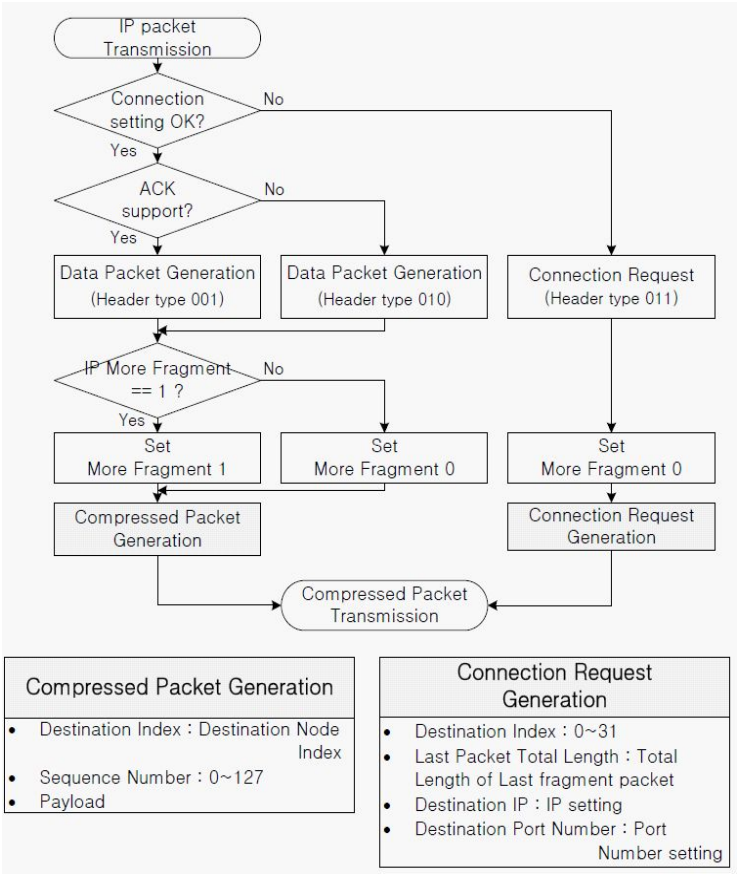
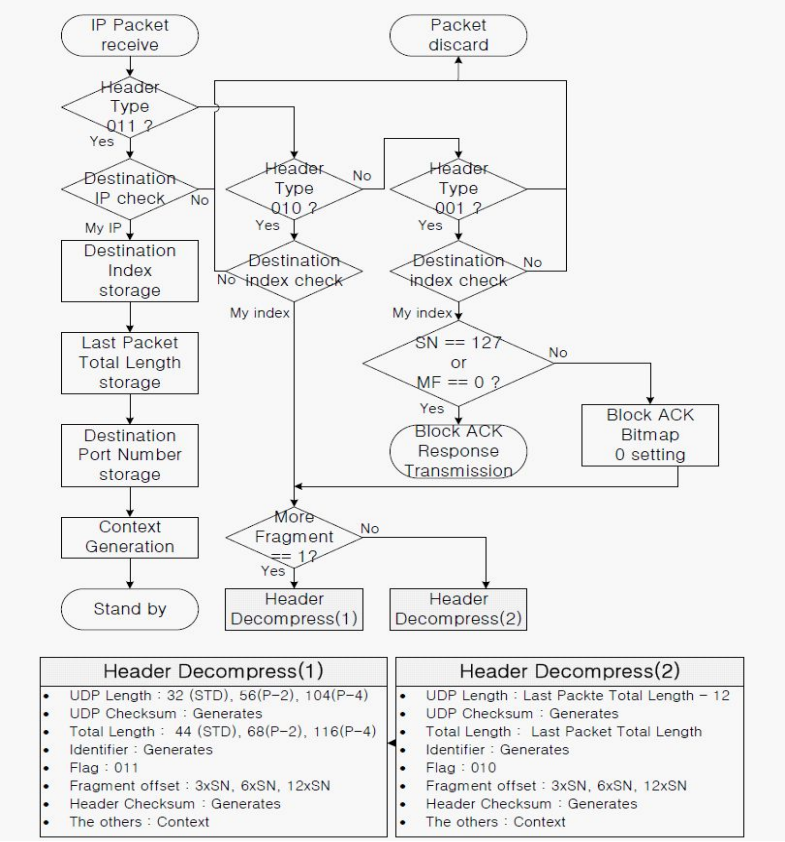


Figure 10. Tactical data link message transmission scheme at the intra network



(a) Transmission procedure



(b) Reception procedure

Figure 11. Transmission and reception procedure of an IP packet

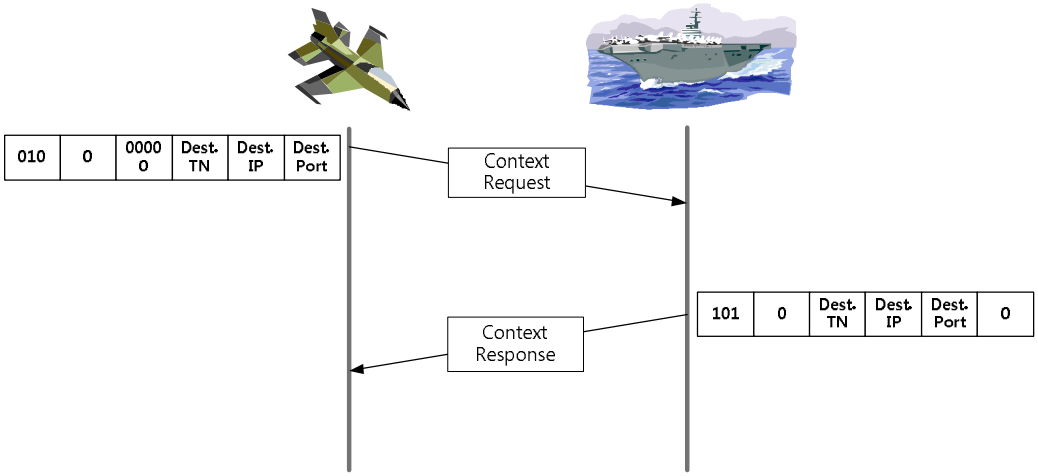


Figure 12. Connection request and response procedure for an IP packet

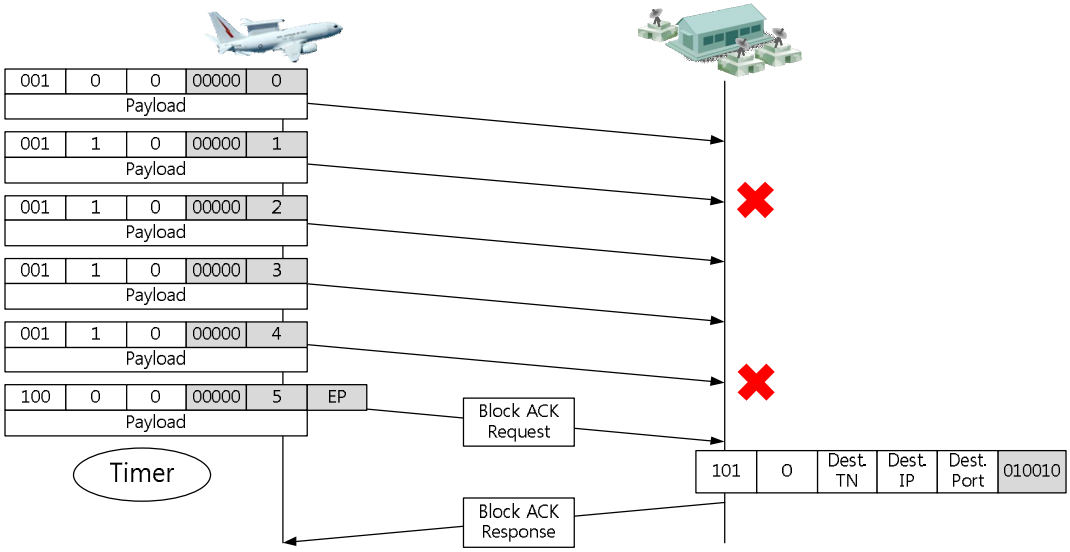


Figure 13. Internet protocol packet transmission and block ACK operation process

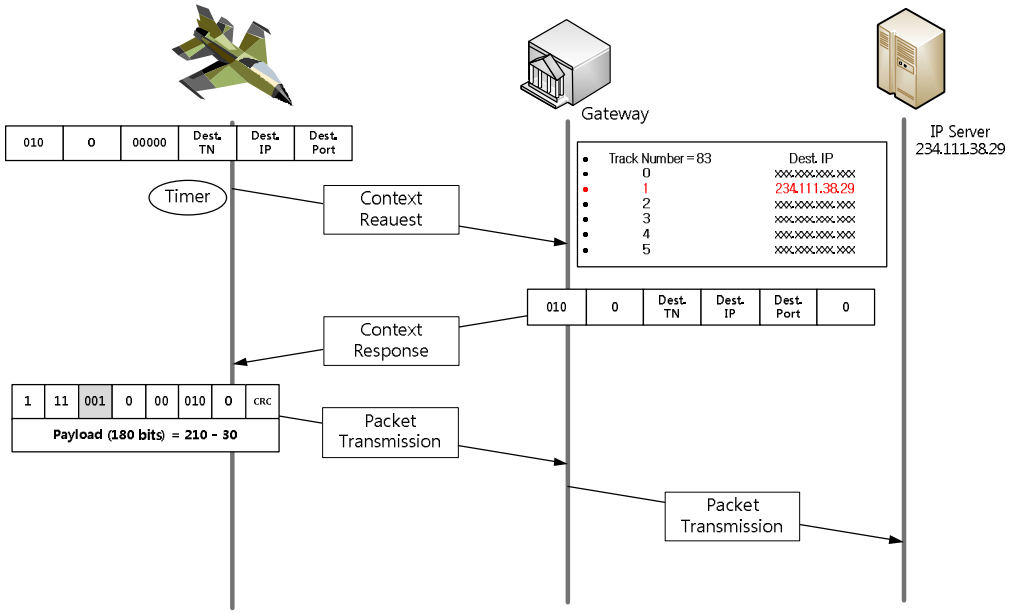


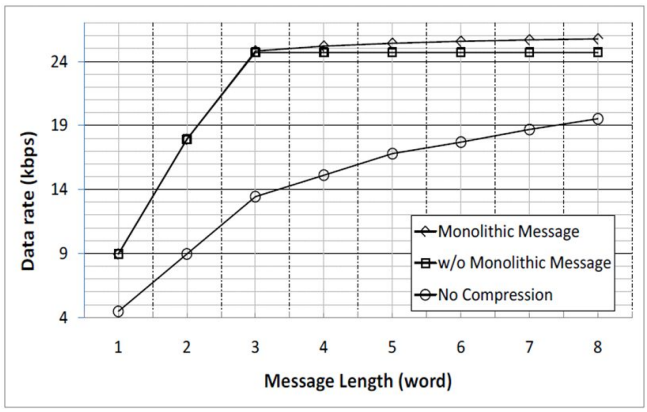
Figure 14. Inter-network connection request and response procedure

Figure 14 shows the IP packet transmission example for the inter-network case. After a unit desiring data transmission to the server in foreign network sets the destination information, a connection request packet is transmitted to a gateway. After a transmission of this packet, the gateway composes a table between the index number and the destination location IP server, and makes the inter-network communication possible.

5. Simulation Results

The maximum data rate of Link-16 using the proposed header compression method is evaluated. Figure 15(a) shows the transmission data rate when the tactical data link message of one to eight words is transmitted. In case that the compressed header is not used, the UDP and IP headers are transmitted in a time slot. If a message containing three words is transmitted, the UDP and IP headers are transmitted to two time slot intervals. This reduces the maximum data rate (26.88 kbps) of STDP mode. The difference of the data rate in case that the Monolithic Message field is used is shown. As the Monolithic Message transmits message containing more words, the relative size of a header is decreased. The data rate is larger because the message size is relatively larger.

Figure 15(b) describes the Energy efficiency according to Monolithic message field of header compression method. STDP of link-16 transmits 3 words at a time. Therefore, it has two times transfer efficiency compared to uncompressed mode. Average transmission efficiency is 164.57% with Monolithic message and 161.561% without Monolithic message.



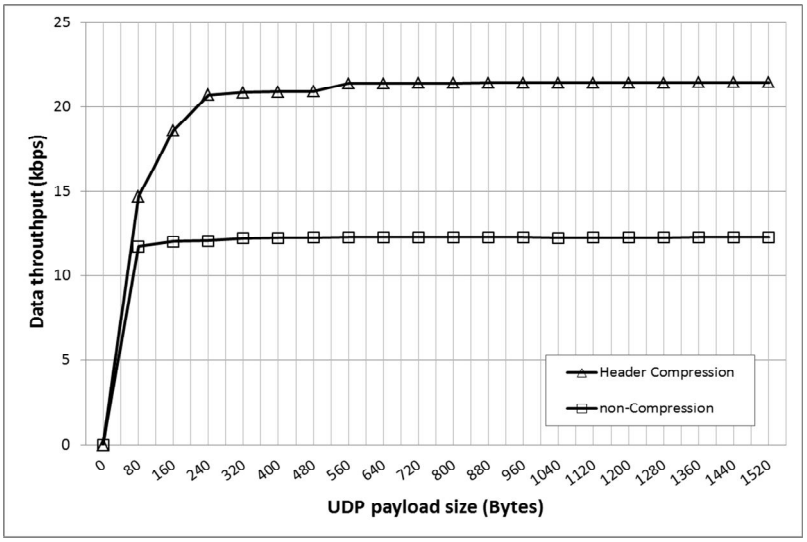
(a) Data rate vs. length of fixed J-series message format

(b) Energy efficiency vs. length of fixed J-series message format

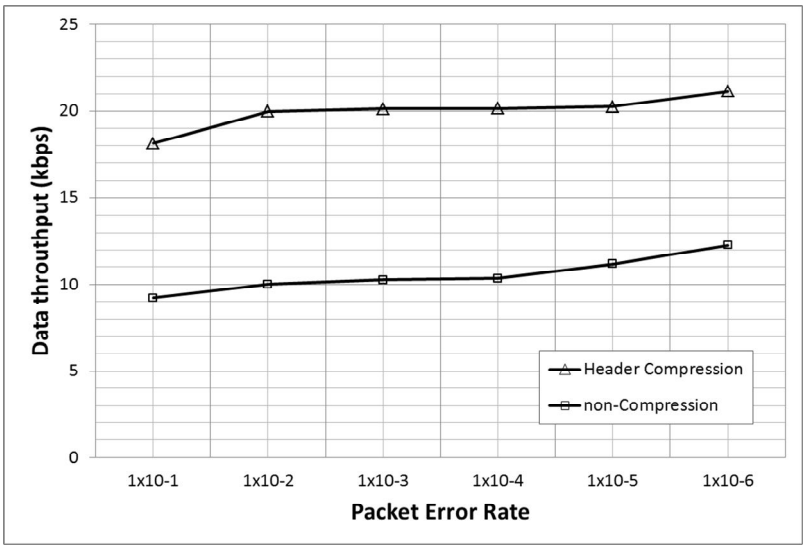
Figure 15. Performance for a fixed J-series format message

Table 2. Data rate for IP packet transmission

	IP Addressing (IP and UDP)	Proposed Indexing (Connection setting)
Preparation process	None	2 time slots
Header Length	45 bits	18 bits
Data rate	16.26 kbps (ST) 40.64 kbps (P2) 97.54 kbps (P4)	24.38 kbps (ST) 48.77 kbps (P2) 97.54 kbps (P4)



(a) Data throughput vs. UDP payload size



(b) Data throughput vs. packet error rate

Figure 16. Data throughput performance for IP packets

Table 2 shows the IP packet transmission rate for two addressing methods. One is the IP addressing, and the other is the proposed indexing scheme. The IP addressing does not need the preparation for data transmission. The proposed indexing method needs the preparation during 2 time slots. For the IP addressing method, data rate is smaller because of the large size of header. In Table 2, the data transmission rate is the same for Packed-4 (P4) because transmitting data size is the same as IP fragmentation based on the MTU (Message Transfer Unit) of Link-16.

Figure 16 is the data throughput performance for IP packets. Figure 16(a) shows data throughput for various sizes of UDP payload. If the proposed header compression method is used, data throughput is increased by average 58.72%. Figure 16(b) shows data throughput for erroneous channels. The data throughput can be different if packet errors are happened and packet retransmission is used.

6. Conclusions

Header compression is necessary for IP over tactical data link such as Link-16. This paper proposed a novel header compression method for IP over Link-16. And the Monolithic Message was also proposed for the efficient IP packet transmission of the tactical data link message. An indexing method was used for transmission of typical IP packets. In addition, the function of transmitting ACK to the compressed header was added in order to compensate the disadvantage of the UDP application.

For monolithic message, 90.7% for IP packet transmission and maximum 95.8% for tactical data link message can be achieved by using the proposed header compression method compared to existing Link-16.

As a further study, a research including physical layer issues for efficient IP application over Link-16 will be considered.

References

[1] US DoD, “Network Contric Warfare Report To Congress”, July . 2001

[2] S.B.Jee, “An Analysis for Efficient Appliance of TDL Protocol and IP on Link-K System” Agency of Defence Development(in Korean)

[3] W.J.Wilson, “Applying Layering Principles to Legacy Systems; Link-16 as a case study” , IEEE MILCOM 2001, pp 526-531

[4] Understanding Link-16: A Guidebook for New User, Northrop Grumman Corporation, San Diego, CA, September 2001.

[5] EFFNET, "An Introduction to IP Header Compression.",Effnet WhitePaper, Febrary ,2004

[6] M.Degermark, B.Nordgren, S.Pink, "IP Header Compression", RFC 2507, Febrary 1999

[7] S.Casner,V.Jacobson,"Compressing RTP/UDP/IP Headers for Low-SpeedSerialLinks", RFC 2508, Febrary 1999.

[8] C.B,Ed.,"RobustHeaderCompression(ROHC)" RFC 3095, June 2001

[9] H.J. Woo, J.Y. Kim M.J. Lee, “Performance analysis of Robust Header Compression over Mobile WiMAX”, ICACT 2008, pp. 311-313

[10] Y.Yoon, S.Park, H.Lee, J.S.Kim, S.B.Jee, “Header Compression for Resource and Energy Efficient IP over Tactical Data Link” FGIT 2010, LNCS 6485, pp. 180-190, 2010

Acknowledgments
The research is supported by the Agency for Defense Development (ADD) of Korea.

Authors

Yongkoo Yoon received B.S. degree in Electronic and Communication Engineering from Kwangwoon University, Seoul, Korea, in 2009. He is now a Ph.D. candidate in Kwangwoon University. His research interests include wireless communication, header compression, and tactical communication networks.

Suwon Park received the B.S. degree in electrical engineering and mathematics (double major) in 1994, the M.S. degree in electrical engineering in 1996, and the Ph.D. degree in the Department of Electrical Engineering and Computer Science (EECS), all from the Korea Advanced Institute of Science and Technology (KAIST), Daejeon, Korea, in 2003. From 1994 to 1998, he was a Research Engineer in Telecommunication R&D Center of Samsung Electronics, where he worked for the standardization of International Mobile Telecommunications (IMT)-2000. From 1999 to 2002, he was a Research Assistant in the Department of EECS, KAIST, and a Part-Time Researcher with the Electronics and Telecommunications Research Institute (ETRI), Daejeon, Korea. In 2002, he rejoined the Telecommunication R&D Center of Samsung Electronics as a Senior Research Engineer, where he worked for the development of terminal modems based on software-defined radio (SDR). In 2006, he joined the faculty of the Kwangwoon University, Seoul, Korea, where he is currently an Assistant Professor with the Department of Electronics and Communications Engineering. His research interests include mobile communication systems, statistical multiplexing, radio resource management, communication theory, and SDR.

Hyungkeun Lee received B.S. degree in Electronic Engineering from Yonsei University, Seoul, Korea, in 1987, and M.S. and Ph.D. degree in Computer Engineering from Syracuse University in 1998 and 2002, respectively. He worked in Samsung Electronics and Bell Atlantic. He joined the Department of Computer Engineering at Kwangwoon University, Seoul, Korea in 2003. His research interests include wireless multihop communication, sensor networks and tactical communication networks.

Jongsung Kim is a Division Chief in JTDLS PMO(Joint Tactical Data Link System, Program Executive Office) at ADD(Agency for Defense Development). He received B.A. and M.A. degrees in Computer Network from Soongsil University in 1984 and 1986, Ph.D. degree in Computer Engineering from POSTECH in 1997. He did his post doctoral work at University of California, Irvine(2006-2007). His research interests include Tactical Data Links, Distributed Systems, Network Modeling & Simulation

Seungbae Jee is a senior researcher in JTDLS PMO(Joint Tactical Data Link System, Program Executive Office) at ADD(Agency for Defense Development). He received B.S. degree in Electronic Engineering from Sogang University in 2001, and M.A. degree in Electrical Engineering from KAIST in 2003. Research interest: Tactical Data Links, Broadband Converged Network, System modeling and simulation