Power Efficient and Secure IPV6 Robust Header Compression Technique for Low Power Wireless Personal Area Networks

Shumaila Khan, Syed M. Anwar, Sobia Arshad
Department of Computer Engineering
University of Engineering & Technology Taxila

Asjad Amin
Department of Electrical Engineering, King Fahad University of Petroleum & Minerals

ABSTRACT
A power efficient & secure ROHC scheme has been presented in this paper. This scheme is designed to work efficiently for IPV6 based low power wireless personal area networks. The proposed scheme first implements ROHC followed by a suitable encryption scheme. ROHC can greatly reduce the size without adding too much complexity to the system. This in result improves the data rate without costing too much power. IPV6 lowpans have a number of applications in military and emergency scenarios. Therefore providing high data rate with security is the prime requirement especially for military applications. For our design we have tested three different encryption schemes. DES gives the best power efficiency as compared to TDES but it is less secure and information can be cracked. TDES is three times computationally more expensive but gives more secure option. Kasumi gives a middle solution. A computer simulation for the whole system has been tested to verify the data rate & power efficiency. The result clearly suggest that proposed system gives a higher data rate with better security and power efficiency.

Keywords
IPV6Lowpan;ROHC; Encryption; DES; TDES; Kasumi

1. INTRODUCTION
Header Compression techniques are used to compress the header of data packets before transmission, saving the network bandwidth from packet overheads, thereby providing an efficient utilization of network resources. Traditional compression techniques used in wireless networks are generally a tradeoff between enhanced network utilization and low complexity. Algorithms with better compression ratios consume a lot of resources in terms of memory, power and time. On contrary to this simplified algorithms does not always give an optimum level of compression.

In recent years the idea of efficient spectrum utilization has become one of the most researched field in wireless communication. Recent survey [1][4][5] indicates that 50% of total packets transmitted over internet have a size equal or less than 80 bytes with header contributing 40 bytes which is 50% of the actual packet. The average packet size is found even more less in low power wireless networks e.g. military GPS based on adhoc network.

The shortage of current Internet Protocol (IP) addresses has become an issue due to the recent increase in the number of computer terminals and users. The main advantages of IPv6 over the current IP version, IPv4, are that IPv6 supports billions of users, reduces the size of the routing tables, provides better security, and supports mobility[2]. However, these advantages come at a cost of increased header size, further depleting the efficiency [1]. This makes Header compression even more critical problem in IPV6 based networks.

State of the art header compression techniques such as ROHC [9] reduces the size of header significantly but at an expense of computationally complex algorithms. These algorithms cannot be implemented in low power networks where efficient power utilization is the prime priority.

Low power networks provides a reliable platform for information exchange during emergency and military scenarios. Such networks have proved to be of vital importance during emergency situations such as forest fires, quakes and hurricanes (Sandy is the latest example). The military applications involve strategic formation during war or locating missing personnel. Since a large number of low power networks are used in military applications therefore it is essential to design a power efficient and secure header compression scheme suited for the mentioned applications.

Providing broadcast encryption is an essential service in distributed networks. It turns out to be a challenging. Particularly for some special types of networks, such as Ad hoc networks and Wireless Sensor Networks (WSN), it is not easy to provide a practical and secure broadcast scheme. Public-key-based encryptions, which are typically used for broadcast authentication in traditional networks, are too expensive to be used in sensor networks, due to the intensive computation involved in signature verification and the resource constraints on sensor nodes.

In this paper we have implemented a robust header compression technique based on lempel ziv algorithm followed by an encryption algorithm. For encryption, we have tested Kasumi, DES & TDES schemes. We have compared the different schemes based on efficiency and power consumption.

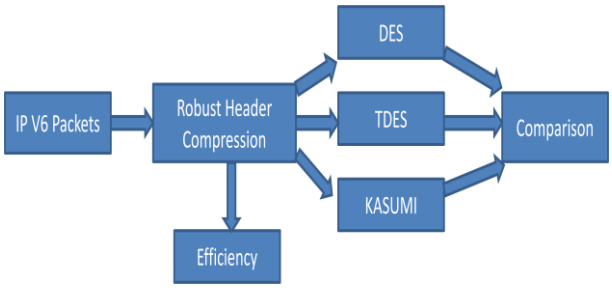

Fig 1: Architecture for proposed ROHC scheme for lowpans with efficient security

The paper is organized as follows: Section II presents Robust Header Compression technique for lowpans , Section III presents implementation of DES, TDES and Kasumi for lowpans, Section IV presents an IPV6 lowpan model with ROHC and encryption together, Section V presents Conclusion remarks.

2. Robust Header Compression for IPV6 Lowpan

For the past two decades header compression has been an active topic for people working in field of computer science. Many header compression schemes have been proposed for the IPV4 and IPV6. Robust Header Compression protocol ROHC [5] was developed by the IETF in 2001. ROHC is well suited for protocols such as IPV4, IPV6, UDP and TCP. ROHC is designed to work well on multilink as well as point to point link. ROHC is known to be able to reduce the header size and performs well over wireless links where the packet loss rate is high. The IP/UDP/RTP profile of ROHC compresses the overhead of 20 bytes for IPv4 or 40 bytes for IPv6 into 2-3 bytes.

ROHC mechanism works by removing the redundant header fields and the redundant information in the packet flow. Each ROHC entity consists of a compressor and decompressor. The compressor and decompressor maintain a context for each flow to store the information about the header fields.

The ROHC compressor has three compression levels: Initialization and Refresh (IR), First Order (FO), and Second Order (SO). In the IR compression level there is no context for compression available. Thus the compressor sends a ROHC packet containing all the static and dynamic header fields information to establish the context. In the FO compression level it sends the change pattern of dynamic fields. In the last compression level SO, it sends encoded values of the RTP Sequence Number (SN) and Timestamp (TS) forming the minimal size packets. In case of some updates or errors in a stream, the compressor goes back to the lower compression levels. It returns to the SO level, which is the highest compression level after retransmitting the updated information and establishing again the change pattern at the decompressor. The decompressor decompresses the headers based on the header fields' information of the context. In order to ensure correct decompression the context should be synchronized all the time.

Fig 2: Point to point link to test ROHC performance

To verify the performance of ROHC we first begin by considering a point to point link as shown in figure 2. Node A is transmitting data to node B. The data set for this case consists of 5 different random files with different size. Figure 3 shows the amount of data with and without ROHC, amount of compression and systems efficiency in each case using ROHC.

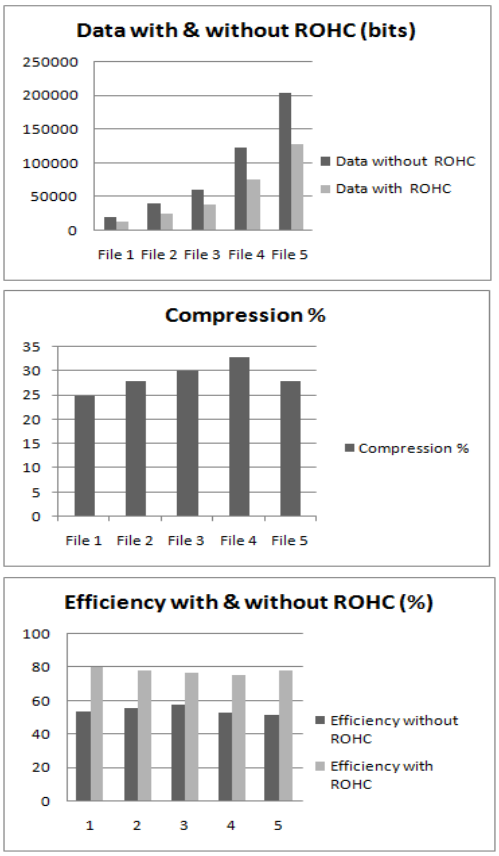

Fig 3: Comparison of Data, Compression & Efficiency with & without ROHC

To analyze the advantage of ROHC in Lowpan consider the scenario as shown in figure 4 with 6 low power nodes. Each node transmits a 1000 packets to any random destination using any random path. With maximum transmitting capability of each node restricted to 10kbps we analyze the result without ROHC first.

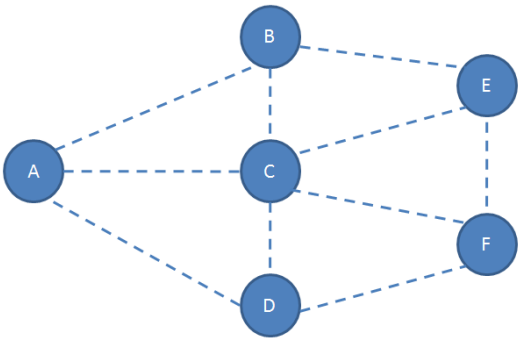

Fig 4: IPV6 Lowpan with 6 Nodes

With average packet size equal to 80 bytes as discussed earlier we get the transmission performance for each node as shown in figure. Figure 5 and figure 6 clearly illustrates that maximum data rate achieved by any node is less than 6kbps that makes the maximum efficiency of system slightly over 50%.

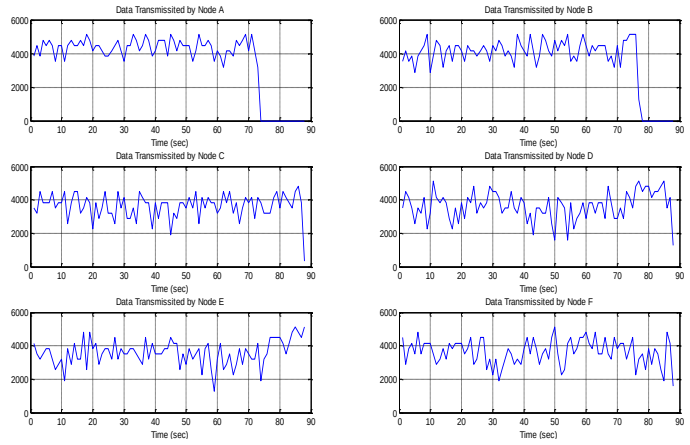

Fig 5: Data transmitted by each node without ROHC

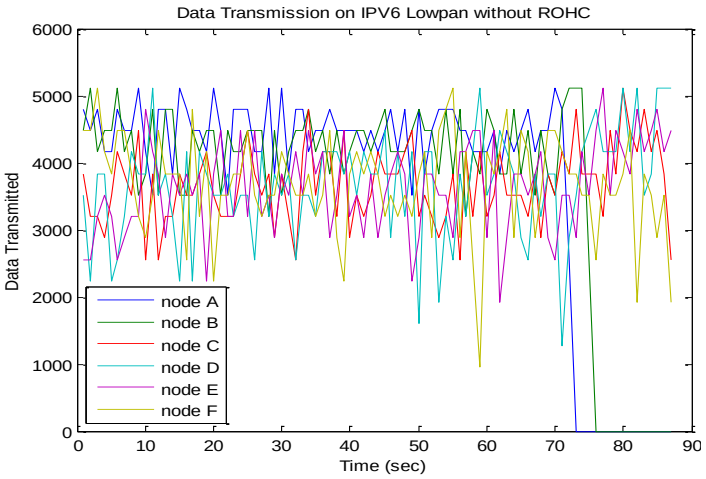

Fig 6: Combined analysis of data transmitted at each node without ROHC

Figure 7 shows the result for the same Lowpan but with introduction of ROHC. ROHC clearly improves the data rate by a significant margin.

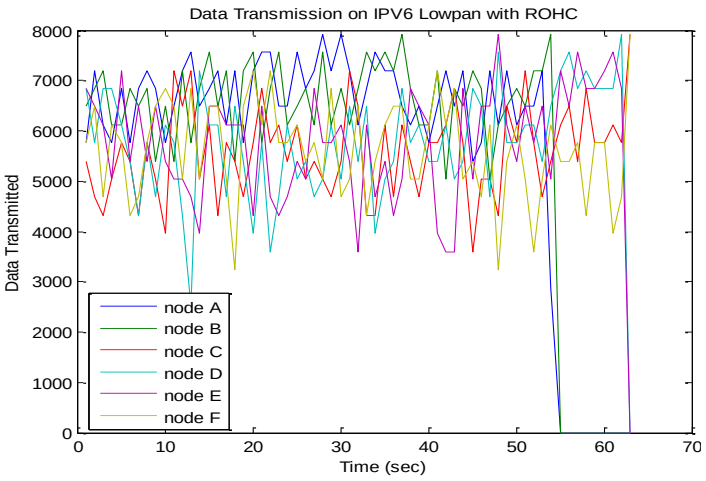

Fig 7: Data transmitted at each node in IPV6 Lowpan using ROHC

The data rate has climbed to 8kbps. The transmission time which was 88 sec in the previous case has also been reduced to 63 sec. Efficiency has been improved from 54% to almost 80%.

3. Encryption Schemes for IPV6Lowpans (DES, TDES, KASUMI)

3.1 Data Encryption Standard DES

The DES (Data Encryption Standard) algorithm, developed in 1976, is the most widely used encryption algorithm in the world. DES works by encrypting groups of 64 message bits, which is the same as 16 hexadecimal numbers. A DES key consists of 64 binary digits of which 56 bits are randomly generated and used directly by the algorithm. The other 8 bits, which are not used by the algorithm, may be used for error detection. The 8 error detecting bits are set to make the parity of each 8-bit byte of the key odd, i.e., there is an odd number of "1"s in each 8-bit byte. In DES algorithm 8 S-boxes are used in each entries is 6 bits and p- boxes in which each value is 32 bit. Figure 8 shows the block diagram of working of DES.

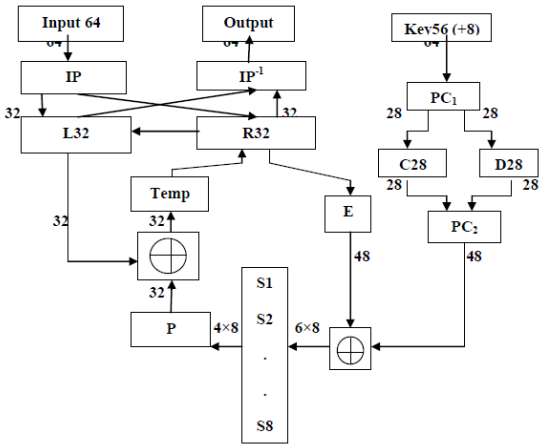

Fig 8: Working of DES algorithm

3.2 Triple DES

Triple DES is another mode of DES operation. It takes three 64-bit keys, for an overall key length of 192 bits. The procedure for encryption is exactly the same as regular DES, but it is repeated three times. Hence the name Triple DES. The data is encrypted with the first key, decrypted with the second key, and finally encrypted again with the third key. Figure 9 shows the working of TDES.

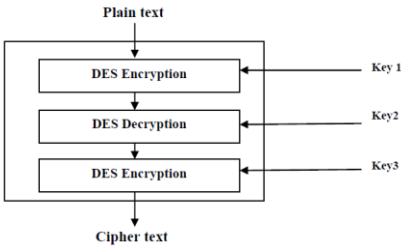

Fig 9: Working of TDES algorithm

3.3 KASUMI

KASUMI has a Feistel structure comprising eight rounds, operates on 64-bit data blocks, and a 128-bit encryption key K controls its processing. The encryption key K is used to generate a set of round keys {KLi, KOi, KIi} for each round i, each round computes a different function as long as the round keys are different, and the same algorithm is used both for

encryption and decryption. For odd rounds the round-function is computed by applying the FL function followed by the FO function. For even rounds the FO function is applied before FL. FL & FO are a 32-bit function made up of simple AND, OR and XOR. Each round's output is twisted before being applied as input to the following round. After completing eight rounds KASUMI produces a 64-bit long cipher text block corresponding to the plaintext input block. Figure 10 shows the first three rounds of KASUMI.

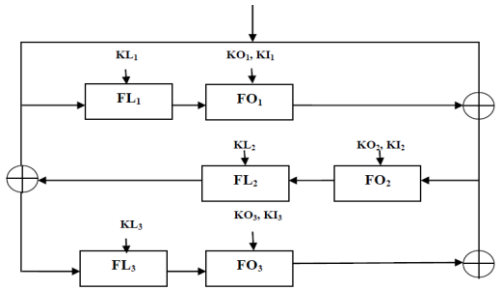

Fig 10: Operation of KASUMI

4. Power Efficiency of IPV6 Lowpan

4.1 Power Efficiency of IPV6 LowPAN using DES

To compute power efficiency of IPV6 lowpans we consider the same network as described in figure 4. The maximum transmission capability of each node is 10 kbps. Each node has 2000 power units. Consider the scenario where all the nodes are transmitting data randomly to other nodes. Simulation results as given in figure 11 for the above network shows that all the nodes consume their 2000 power units before 50 sec and stop working when using DES.

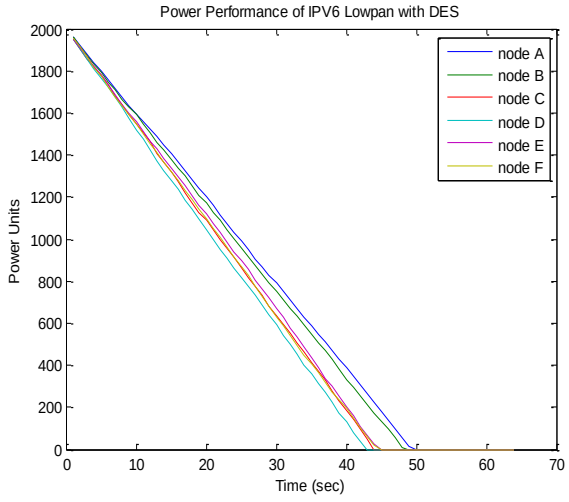

Fig 11: Power Efficiency of IPV6 lowpan with DES (all the nodes transmitting)

For comparative analysis consider a simple scenario for the above network where only node A is transmitting 2000 packets to all the other nodes using DES. Figure 12 shows the results. It can be seen clearly that node A has almost consumed all of its power units since it was the only node that was generating packets & transmitting. Node B,C & D have more than 1000 power units left and node E & F have more than 1600 power units left.

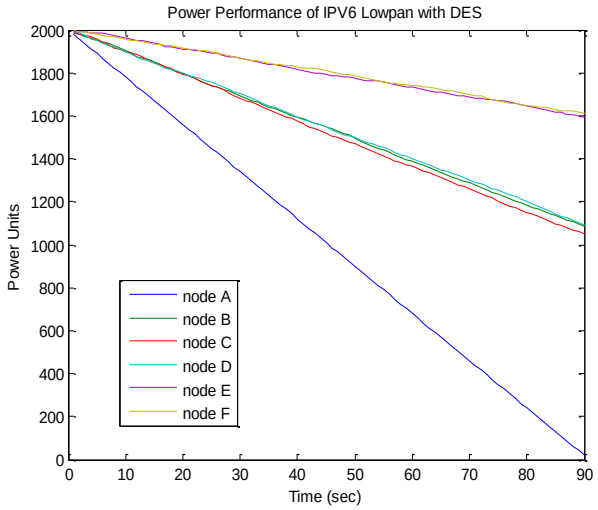

Fig 12: Power Efficiency of IPV6 lowpan with DES (Node A transmitting)

4.2 Power Efficiency of IPV6 LowPAN using TDES

Consider the same scenario where node A is transmitting 2000 packets to all the other nodes but now using TDES. Figure 13 shows that node A consumes all of its power units before 50 sec since it was the only node that was transmitting. Node B,C & D have less than 200 power units left and node E & F have more than 1000 power units left. The results clearly suggest that TDES requires a lot more power as compared to DES.

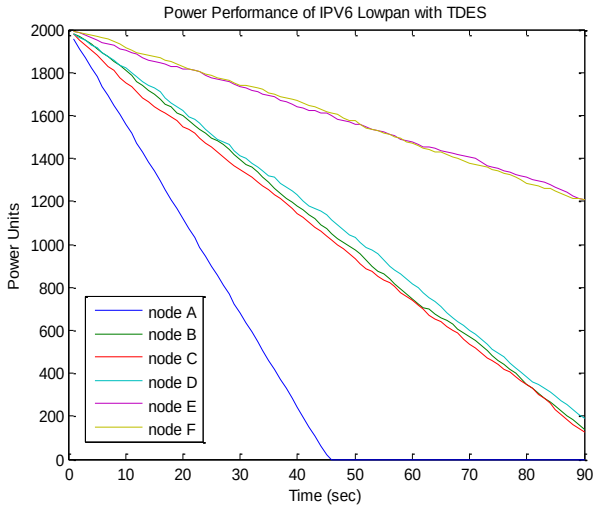

Fig 13: Power Efficiency of IPV6 lowpan with TDES (Node A transmitting)

4.3 Power Efficieny of IPV6 LowPAN using KASUMI

Figure 14 shows the result for same scenario with node A transmitting to all other nodes using KASUMI as encryption scheme. The result suggests that node A consumes all its power units in just over 60 sec. Node B, C & D have almost 600 power units left and node E & F have more than 1500

power units left. This shows that KASUMI is a moderate option if compared to DES & TDES.

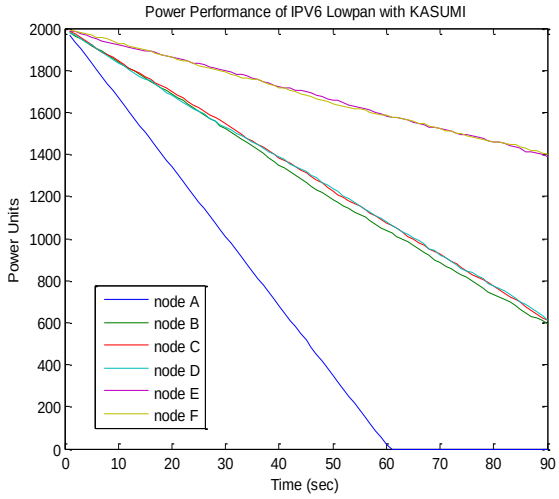

Fig 14: Power Efficiency of IPV6 lowpan with KASUMI (Node A transmitting)

4.4 Comparitive Power Analysis of IPV6 LowPAN using DES, TDES & KASUMI

Figure 15 shows the result of each node when using DES, TDES & KASUMI. It can be clearly seen that in terms of power TDES consumes the most and DES the least for the same amount of data. KASUMI is in between. It consumes more power than DES but fairly low power than TDES.

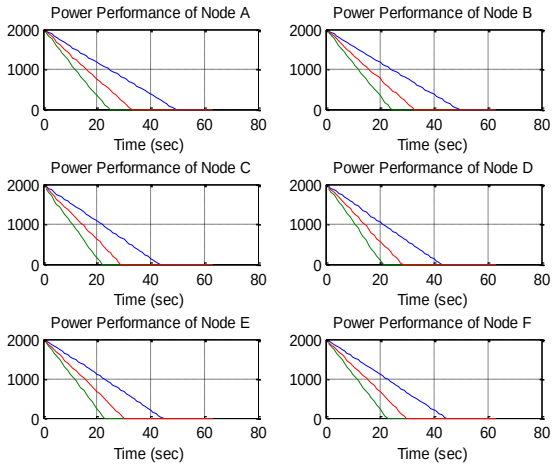

Fig 15: Power Efficiency of IPV6 lowpan with DES, TDES & KASUMI (all the nodes transmitting)

5. Conclusion

A secure power efficient ROHC scheme suitable for IPV6Lowpan has been presented in this paper. To ensure the security of data, three different encryption schemes have been discussed and compared. Simulations have been performed on a 6 node IPV6lowpan network. The results clearly suggest that the proposed scheme provides a secure ROHC solution and it is also power efficient.

6. REFERENCES

[1] Jesus Arango, Stephen Pink, Procito, " HEADER COMPRESSION FOR AD-HOC NETWORKS," in Proc. IEEE Military Communications Conferenc,. MILCOM 2005

[2] Jae D. Lim, Harold P. Stern, " IPv6 HEADER COMPRESSION ALGORITHM SUPPORTING MOBILITY IN WIRELESS NETWORKS," in Proc. IEEE Southeastcon 2000.

[3] Tang Zhi-ling, Yang Xue-zhou, Xiong Chang-wei, Li Si-min, " The Encrypted Traffic Adaptive Wireless Image Sensor Network Based on 6LoWPAN," in Proc. Communications and Mobile Computing (CMC), 2010

[4] Sprint. "IP Monitoring Project". Feb. 6, 2004. http://ipmon.sprint.com/packstat/packetoverview.php

[5] CAIDA. "Packet Length Distributions", 4 Aug 2004, http://www.caida.org/analysis/AIX/plen_hist

[6] Changli Jiao, Loren Schwiebert, Golden Richard, " Adaptive Header Compression for Wireless Networks," in Proc. IEEE Conference on Local Computer Networks, 2001.

[7] Sangheon Pack,Joo-Chul Lee and Jung-Soo Park, " Hybrid Robust Header Compression in Proxy Mobile IPv6 over Wireless Mesh Networks," in Proc. Communications Workshops, 2008.

[8] Yu Wu, Han-Chieh Chao, and Chi-Hsiang Lo, " Providing Efficient Secured Mobile IPv6 by SAG and Robust Header Compression," Journal of Information Processing Systems, Vol.5, No.3, September 2009

[9] Priyanka Rawat, Jean Marie Bonnin, Laurent Toutain, and Yanghee Choi, " ROBUST HEADER COMPRESSION OVER LONG DELAY LINKS," in Proc. IEEE Vehicular Technology Conference, 2008. VTC Spring 2008

[10] Kaddoura, M.; Schneider, S, " ROBUST HEADER COMPRESSION TECHNIQUE FOR AD-HOC NETWORKS,"

[11] C6dric Westphal, " A User-based Frequency-dependent IP Header Compression Architecture," in Proc. IEEE Global Telecommunications Conference, 2002. GLOBECOM '02.

[12] M.Sief, Y.Dakroury, " GAURANTEED END· TO· END QoS FOR VoIP OVER CELLULAR LINKS BASED ON IPv6 COMPRESSION," in Proc. IEEE Conference on 3G Mobile Communication Technologies, 2004.

[13] Alkiviadis Yiannakouliast, Dr. Theodore Kotsilieris2, Dr. Stavros Stavroyiannis, " Theoretical evaluation of header compression schemes for IP based wireless access systems," in Proc. Wireless Conference 2006 - Enabling Technologies for Wireless Multimedia Communications.

[14] Yang Xue-Zhou, Tang Zhi-Ling, Li Si-Min, " A Novel Mobile IPv6 Header Compression Algorithm of Wireless Sensor Network ," in Proc. International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, 2009. CyberC '09.

[15] Shahid Raza, Simon Duquennoy, Tony Chung†, Dogan Yazar, Thiemo Voigt, and Utz Roedig," Securing Communication in 6LoWPAN with Compressed IPsec" Distributed Computing in Sensor Systems and Workshops (DCOSS), 2011 International Conference.