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.

References

- Jesus Arango, Stephen Pink, Procito, &quot;HEADER COMPRESSION FOR AD-HOC NETWORKS,&quot; in Proc. IEEE Military Communications Conference, MILCOM 2005
- Tang Zhi-ling, Yang Xue-zhou, Xiong Chang-wei, Li Si-min, &quot;The Encrypted Traffic Adaptive Wireless Image Sensor Network Based on 6LoWPAN,&quot; in Proc. Communications and Mobile Computing (CMC), 2010
- Sangheon Pack, Joo-Chul Lee and Jung-Soo Park, &quot;Hybrid Robust Header Compression in Proxy Mobile IPv6 over Wireless Mesh Networks,&quot; in Proc. Communications Workshops, 2008.
- Priyanka Rawat, Jean Marie Bonnin, Laurent Toutain, and Yanghee Choi, &quot;ROBUST HEADER COMPRESSION OVER LONG DELAY LINKS,&quot; in Proc. IEEE Vehicular Technology Conference, 2008. VTC Spring 2008
- Kaddoura, M.; Schneider, S., &quot;ROBUST HEADER COMPRESSION TECHNIQUE FOR AD-HOC NETWORKS,&quot;
- Alkiviadis Yiannakoulias, Dr. Theodore Kotsilieris2, Dr. Stavros Stavroyiannis, &quot;Theoretical evaluation of header compression schemes for IP based wireless access systems,&quot; in Proc. Wireless Conference 2006 - Enabling Technologies for Wireless Multimedia Communications.
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.

Index Terms

Computer Science  Security

Keywords

IPV6Lowpan  ROHC  Encryption  DES  TDES  Kasumi