Abstract
IEEE 802.16e supports EAP (Extensible Authentication Protocol) for authentication, but do not specify the EAP method required for authentication. EAP-SPEKE and EAP-SRP are the strongest password based EAP methods. This paper examines these EAP methods and proposes an efficient password based authentication protocol for WiMAX. Proposed protocol is an improvement of EAP-SPEKE protocol and supports mutual authentication and key derivation. Protocol is verified using Automated Validation of Internet Security Protocols and Applications (AVISPA) which is a push button tool for the automated validation of security protocol and result shows that it does not have any security flaws. Proposed protocol uses only three message exchange for authentication and key derivation. Therefore, the number of exchanged message decreases by one and two compared with the EAP-SRP and EAP-SPEKE respectively.

Reference

- Su Jung Yu and Joo Seok Song, “An Improved Password Authentication Key Exchange Protocol for 802.11 Environments”, V. Kumar et al. (Eds.): ICCSA 2003, LNCS2668, pp. 201–209, 2003
An Improved Password Based EAP Method for WiMAX with Formal Verification

2000.
- Anjani K. Rai, Vimal Kumar, Shivendu Mishra, "An Efficient Password Authenticated Key Exchange Protocol for WLAN and WiMAX" International Conference and Workshop on Emerging Trends and Technology (ICWET), 2011 proceedings by ACM at Mumbai Maharashtra. (Accepted)
- David Q. Liu, Mark Coslow, “Extensible Authentication Protocols for IEEE Standards 802.11 and 802.16”.

Index Terms
Computer Science Wireless

Key words Authentication AVISPA
EAP-SPEKE EAP-SRP