MUQAMI: A Locally Distributed Key Management Scheme for Clustered Sensor Networks

[1]Syed Muhammad Khaliq-ur-Rahman Raazi, [1]Adil Mehmood Khan, [2]Faraz Idris Khan, [1]Sung Young Lee,[3]Young Jae Song, [1]Young Koo Lee†
[1]Ubiquitous Computing Lab, Department of Computer Engineering, Kyung Hee University, 449-701 Suwon, South Korea {raazi, adil, sylee, yklee}@oslab.khu.ac.kr
[2]Internet Computing and Security Lab, Department of Computer Engineering, Kyung Hee University, 449-701 Suwon, South Korea {faraz}@khu.ac.kr
[3]Software Engineering Lab, Department of Computer Engineering, Kyung Hee University, 449-701 Suwon, South Korea, {yjsong}@khu.ac.kr

Abstract. In many of the sensor network applications like natural habitat monitoring and international border monitoring, sensor networks are deployed in areas, where there is a high possibility of node capture and network level attacks. Specifically in such applications, the sensor nodes are severely limited in resources. We propose MUQAMI, a locally distributed key management scheme for resilience against the node capture in wireless sensor networks. Our scheme is efficient both in case of keying, re-keying and node compromise. Beauty of our scheme is that it requires minimal message transmission outside the cluster. We base our Scheme on Exclusion Basis System (EBS).

1 Introduction

Wireless Sensor Networks (WSN) differs from other distributed systems in a way that they have to work in real-time with an added constraint of energy. They are mostly data centric and are used to monitors their surroundings, gather information and filter it [1]. A sensor network will typically consist of a large number of sensor nodes

† Corresponding author.

Please use the following format when citing this chapter:

Raazi, S. M. K., Khan, A. M., Khan, F. I., Lee, S. Y., Song, Y. J. and Lee, Y. K., 2007, in IFIP International Federation for Information Processing, Volume 238, Trust Management, eds. Etalle, S., Marsh, S., (Boston: Springer), pp. 333–348.