A Reliable and Secure Distributed In-network Data Storage Scheme in Wireless Sensor Networks

Authors:Abdullahi, M.B. ; Sch. of Inf. Sci. & Eng., Central South Univ., Changsha, China ; Guojun Wang ; Musau, F.

Abstract

In a battlefield surveillance scenario, data readings and events emerging from a wireless sensor network deployed that may not be used immediately by or simply impossible to transmit to an authorized user (a Soldier) in real time are stored in the network. Without proper protection for the sensitive data generated in this setting, a compromised storage node (by an enemy soldier) may divulge its stored sensitive data about the monitored environment, and even worse, it may alter the data. In this paper, we integrate an elliptic curve cryptography scheme and an erasure coding scheme to provide reliable and secure distributed in-network data storage for sensor networks. The main idea is to distribute each erasure coded fragment appended with a fingerprint to different storage nodes. The fingerprint is to allow each coded data fragment to be independently verified as a valid and correct subset of a specific data item. So, the scheme achieves localization of data error. The proposed scheme is resilient to collusion attack, pollution attack, and data dropping attack, and guarantees forward and backward data secrecy as well. The security of the proposed scheme relies on the intractability of the elliptic curve discrete logarithm problem. Different from the existing solutions, the uniqueness of our method comes from the use of lightweight encryption scheme, which is well suited for resource constrained wireless sensors.

Published in:

Trust, Security and Privacy in Computing and Communications (TrustCom), 2011 IEEE 10th International Conference Date of Conference:16-18 Nov. 2011,Page(s):548 - 555,Print ISBN:978-1-4577-2135-9

Author keywords:

Wireless sensor network,distributed in-network storage,energy,consumption,reliability,resiliency,security