Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 2, Issue. 9, September 2013, pg.184 – 190

RESEARCH ARTICLE

A Framework Based Integrated Dynamic Data Storage Scheme Based on Network Coding and Homomorphic Fingerprinting

K. Jothimani[1], N.Hema[2]

[1]Research Scholar, Department of Computer Science, Vivekanandha College, Elayampalayam, Tiruchengode, Tamil Nadu, India

[2]Assistant Professor, Department of Computer Science, Vivekanandha College, Elayampalayam, Tiruchengode, Tamil Nadu, India

[1] kjothimani88@gmail.com; [2] hemaguna_80@gmail.com

ABSTRACT: - Recently, distributed data storage has gained increasing popularity for efficient and robust data management in wireless sensor networks (WSNs). The distributed architecture makes it challenging to build a highly secure and dependable yet lightweight data storage system. On the one hand, sensor data are subject to not only Byzantine failures, but also dynamic pollution attacks, as along the time the adversary may modify pollute the stored data by compromising individual sensors. On the other hand, the resource-constrain nature of WSNs precludes the applicability of heavyweight security designs. To address the challenge, in this article we propose framework based integrated dynamic data storage scheme with dynamic integrity assurance. Based on the principle of secret sharing and erasure coding, we first propose a hybrid share generation and distribution scheme to achieve reliable and fault-tolerant initial data storage by providing redundancy for original data components. To further dynamically ensure the integrity of the distributed data shares, we then propose an efficient data integrity verification scheme exploiting the techniques of algebraic signature and spot-checking. The proposed scheme enables individual sensors to verify in one protocol execution the correctness of all the pertaining data shares simultaneously in the absence of the original data. Extensive security analysis shows that the proposed scheme has strong resistance against various data pollution attacks.

Keywords ---- Clustering Algorithm; Aggregation

Full Text: http://www.ijcsmc.com/docs/papers/September2013/V2I9201355.pdf