A

Project Report

On

KEY UPDATING FOR LEAKAGE RESILIENCE WITH APPLICATION TO AES MODES OF OPERATION

Submitted to

Department of

Computer Science and Engineering

By

REDDY VYSHNAVI	(206Y1A6646)
AKULA RUSHIKA MAITHI	(206Y1A6601)
SIRISHETTY SREEJA	(206Y1A6647)
BOMMAGANI BHAVANI	(206Y1A6606)

Under the guidance

Of

Mrs.T.SHRAVANTHI
Asst.Professor

Department of Computer Science & Engineering

SUMATHI REDDY INSTITUTE OF TECHNOLOGY for WOMEN

(Approved by AICTE, New Delhi; Affiliated to JNTU, Hyderabad)

Ananthasagar(Vill), Hasanparthy(M), Warangal – 506 371 (A.P.), Website : www.sritw.org

2022-2023

PRINCIPAL
Sumathi Reddy Institute of Technology for Women
Ananthasagar (V), Hasanparthy (M)
WARANGAL - 506 371 (T.S.)

SUMATHI REDDY INSTITUTE OF TECHNOLOGY for WOMEN

(Approved by AICTE, New Delhi; Affiliated to JNTU, Hyderabad)

Ananthasagar(Vill), Hasanparthy(M), Warangal – 506 371 (A.P.), Website : www.sritw.org

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

CERTIFICATE

This is to certify that the project entitled **"KEY UPDATING FOR LEAKAGE RESILIENCE WITH APPLICATION TO AES MODES OF OPERATION"** is submitted by REDDY VYSHNAVI(206Y1A6646), AKULA RUSHIKA MAITHI(206Y1A6601), SIRISHETTY SREEJA(206Y1A6647) and BOMMAGANI BHAVANI(206Y1A6606) to the department of Computer Science and Engineering during academic year 2022-23.

Mrs.T.SHRAVANTHI
Project Guide

Dr.E.SUDARSHAN
Head of the Department

PRINCIPAL
Sumathi Reddy Institute of Technology for Women
Ananthasagar (V), Hasanparthy (M)
WARANGAL - 506 371 (T.S.)

S.R.I.T. FOR WOMEN * WARANGAL *

ABSTRACT

File sharing applications in mobile ad hoc networks (MANETs) have attracted more and more attention in recent years. The efficiency of file querying suffers from the distinctive properties of such networks including node mobility and limited communication range and resource. An intuitive method to alleviate this problem is to create file replicas in the network. However, despite the efforts on file replication, no research has focused on the global optimal replica creation with minimum average querying delay. Specifically, current file replication protocols in mobile ad hoc networks have two shortcomings. First, they lack a rule to allocate limited resources to different files in order to minimize the average querying delay. Second, they simply consider storage as available resources for replicas, but neglect the fact that the file holders' frequency of meeting other nodes also plays an important role in determining file availability. Actually, a node that has a higher meeting frequency with others provides higher availability to its files. This becomes even more evident in sparsely distributed MANETs, in which nodes meet disruptively. In this paper, we introduce a new concept of resource for file replication, which considers both node storage and meeting frequency. We theoretically study the influence of resource allocation on the average querying delay and derive a resource allocation rule to minimize the average querying delay. We further propose a distributed file replication protocol to realize the proposed rule. Extensive trace-driven experiments with synthesized traces and real traces show that our protocol can achieve shorter average querying delay at a lower cost than current replication protocols.