DISTRIBUTED AGGREGATE PRIVACY-PRESERVING AUTHENTICATION IN VANETs

A project report submitted in partial fulfillment of the requirements for the award of the Degree of

BACHELOR OF TECHNOLOGY

In

COMPUTER SCIENCE AND ENGINEERING

Submitted By

N. SAIDUTT
Regd.No:14811A0544

P.S.P. VINEETHA
Regd.No:14811A0552

V.H.S. KAMESH
Regd.No:14811A0572

R. GEETHA DEVI
Regd.No:14811A0560

Under the esteemed guidance of

Mr N. Swaroop
Assistant Professor

Dept of Computer Science and Engineering

AVANTHI INSTITUTE OF ENGINEERING AND TECHNOLOGY
(Approved by AICTE, New Delhi & Permanently affiliated to JNTU Kakinada)
(Accredited by NAAC, UGC & NBA, AICTE)
MAKAVARAPALEM, NARSIPATNAM
VISAKHAPATNAM DIST
(2014-2018)

Scanned with CamScanner

AVANTHI INSTITUTE OF ENGINEERING AND TECHNOLOGY
(Approved by AICTE, Permanently affiliated to JNTU Kakinada)
(Accredited by NAAC, UGC & NBA, AICTE)
MAKAVARAPALEM, NARSIPATNAM
VISAKHAPATNAM-531113

CERTIFICATE

This is certify that this project work entitled "DISTRIBUTED AGGREGATE PRIVACY-PRESERVING AUTHENTICATION IN VANETs" in partial fulfillment for the degree of Bachelor of Technology in Computer Science and Engineering, at AVANTHI INSTITUTE OF ENGINEERING AND TECHNOLOGY, MAKAVARAPALEM, VISAKHAPATNAM is the bonafied work carried out by N. SAIDUTT (14811A0544), V.H.S. KAMESH (14811A0572), P.S.P. VINEETHA (14811A0552), R. GEETHA DEVI (14811A0560) under the guidance and supervision during 2017-2018.

Project Guide

6/4/18
External examiner

Head of the Department
Computer Science and Engineering
Avanthi Institute of Engg. & Technology
Tamaram (Vill), Makavarapalem (MD)
Narsipatnam, Visakhapatnam-531113

Scanned with CamScanner

ABSTRACT

Now-a-days, there is a tremendous growth in the graph of accidents on roads. This is due to lack of safety precautions like speed alerts, road blocks... etc. Although there are sign boards available on the roadside the driver need to check it every time he/she enter in to a new area, it is a bit difficult task to check the sign boards on the road repeatedly.

In order to reduce the rate of accidents the vehicles need to be alerted at every new zone about the speed limits to maintain and about the other safety related precautions. To alert the vehicles at every new zone there must be a communication between the vehicles to share safety related messages, communication between vehicles can be done through an adhoc network, such type of adhoc network for vehicle to vehicle communication is called Vehicular Adhoc Network(VANET).

In VANETs, to communicate with the vehicles the network uses the Road Side Units(RSUs) and Tamper Proof Devices(TPDs) embedded in vehicles. These RSUs are distributed along the road side with an equal distance of separation. Each RSU consists of a frequency range in which a vehicle can communicate with a RSU and also it can communicate with other vehicles. A vehicle can communicate through network only when it has an ideal tamper-proof device (TPD) embedded in it. Using those TPDs each vehicle has to register with its credentials to root Trusted Authority(TA) which generates public and private keys for a secure communication between these RSUs and vehicles. Each vehicle broadcasts a message to nearby vehicles and RSUs every few hundreds of milliseconds A vehicle or an RSU may receive hundreds of messages in a short period. If the messages cannot be processed in time, traffic jams and even accidents may ensue. Hence, it is critical to devise security and privacy mechanisms that do not lead to an unaffordable reaction delay.