Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

An Efficient Pairing-free Batch Verification Scheme for VANET

Yan-Ming Lai (d05922014@csie.ntu.edu.tw)
NTU: National Taiwan University https://orcid.org/0000-0001-7621-7159
Pu-Jen Cheng
NTU: National Taiwan University

Research

Keywords: Ad hoc networks, Elliptic curves cryptography, Intelligent transportation systems, Message authentication, Vehicle

Posted Date: April 9th, 2021

DOI: https://doi.org/10.21203/rs.3.rs-291819/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License.
Read Full License

Abstract

An intelligent traffic system, which can flexibly allocate traffic resources, serves as a good assistant to help us improve traffic safety and efficiency of controlling traffic volume, providing instant traffic information and giving priority to ambulances. Although such system is powerful, it could be misused without prop er protection. For example, malicious drivers might forge the message of the ambulance so that they can quickly pass through intersections. In addition, because traffic information is huge and needs to be processed immediately, traditional schemes that pro cess the information one by one are not competent. For this issue, a lot of batch schemes have been proposed. Most of them adopt the algorithm of Bilinear pairing while the others tries to avoid it since pairing operations are complex. However, such pairin g - free schemes are not applicable because their calculation time will explode when there are more data waiting to be processed. In this article, we briefly describe those schemes and propose a more effective one to solve the problems mentioned above.

Full Text

This preprint is available for download as a PDF.

Figures

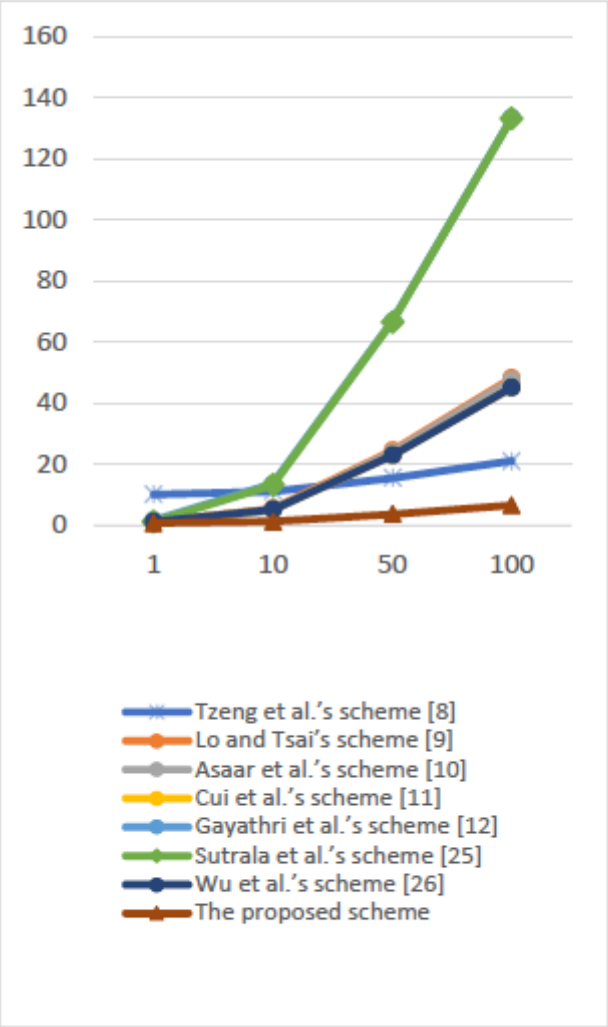

Figure 1

Execution time for m verified messages. *x-coordinate: the number of verified messages (1 to 100) *y-coordinate: execution time of verified messages (unit: ms)