IJMRT: Volume (6), Issue 5, 2024
International Journal of Multidisciplinary Research Transactions
(*A Peer Reviewed Journal*)
www.ijmrt.in

ISSN (Print):2663-2381
ISSN (Online):2663-4007

Strengthening Security and Privacy in VANETs: Advancements in Ring Signcryption Based Protection

S Sheela Angel[1*], K Suthika[2], S Yahitha[3], D Sruti[4], Dr. S A Arunmozhi[5]

[1]*Student, Department of Electronics and Communication Engineering, Saranathan College of Engineering, Trichy, India.*
[2]*Student, Department of Electronics and Communication Engineering, Saranathan College of Engineering, Trichy, India.*
[3]*Student, Department of Electronics and Communication Engineering, Saranathan College of Engineering, Trichy, India.*
[4]*Student, Department of Electronics and Communication Engineering, Saranathan College of Engineering, Trichy, India.*
[5]*Associate Professor, Department of Electronics and Communication Engineering, Saranathan College of Engineering, Trichy, India.*

[*]Corresponding author

DoI: https://doi.org/10.5281/zenodo.11184337

Abstract

Vehicular ad hoc networks (VANETs) offer various benefits such as driving safety, data communication, traffic management, and entertainment, but they are vulnerable to attacks. Conditional privacy protection (CPP) schemes aim to secure VANET communication. In 2021, Cai et al. proposed a CPP scheme based on ring signcryption for VANETs. However, their scheme has flaws regarding message retrieval, sender anonymity, and malicious user detection. We present an improved scheme addressing these issues, with security proofs and performance analysis, offering enhanced security and efficiency for VANETs.

Keywords: Vehicular adhoc networks (VANETs), Conditional privacy protection (CPP), Ring signcryption, Security flaws, Message retrieval, Sender anonymity, Malicious user detection, Improved scheme, Security proofs, Performance analysis.

1. Introduction

Vehicular Ad-hoc Networks (VANETs) play a critical role in facilitating communication between vehicles and Road Side Units (RSUs), fostering safety and informational exchanges

within Intelligent Transportation Systems (ITS). These networks integrate fixed infrastructures and mobile vehicles, serving as dynamic nodes for data exchange. However, VANETs face specific security threats, such as message interception and unauthorized data alteration by attackers, which could lead to catastrophic outcomes. Despite these challenges, the evolution of VANETs from basic ad hoc networks to specialized systems within inter-vehicle communication underscores their paramount importance in enhancing road safety and navigation.

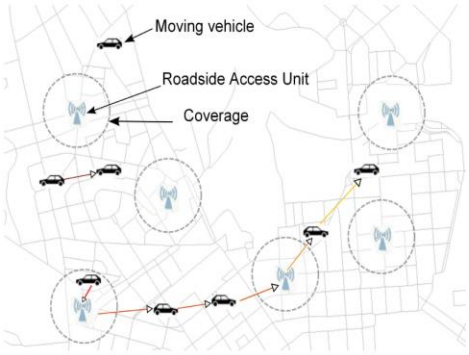

Figure.1. Vehicular Communications in ITS

2. Related Work

Researchers have devised several security mechanisms to bolster Vehicular Ad Hoc Networks (VANETs). Wasef and Shen introduced EMAP, a protocol that expedites message authentication in VANETs [1]. Yang et al. proposed an ADS-B authentication framework using hierarchical identity-based signatures to secure aircraft communication [2]. He et al. developed ICPPA, an authentication scheme ensuring privacy while authenticating vehicles efficiently [3]. Omar, Zhuang, and Li designed VEMAC, a MAC protocol enhancing broadcast reliability in VANETs [4]. Jo, Kim, and Lee devised a cooperative authentication mechanism for improved security in vehicular networks [5]. Ni et al. presented a privacy-preserving smart parking navigation system for VANETs [6]. Weng et al. introduced BENBI,

a scalable access control mechanism for SDN-based VANETs [7]. Zhang et al. proposed DAPPA, ensuring authentication privacy in VANETs [8]. Cheng et al. explored big data-driven approaches in vehicular networks [9]. Tzeng et al. enhanced an identity-based batch verification scheme to bolster security and privacy in VANETs [10].

3. Proposed Algorithm

3.1. Proposed Architecture for VANET

The primary objective of our work is to enhance message delivery reliability within a Vehicular Ad-Hoc Network (VANET) by identifying suitable relay nodes. We introduce a predictive model to forecast the future movement trajectories of vehicles based on their historical mobility data. Subsequently, a set of relay nodes is selected, prioritizing those with a higher likelihood of reaching the intended destination vehicle. We then establish routing metrics and present a routing algorithm to determine relay nodes for packet forwarding, along with corresponding routing paths.

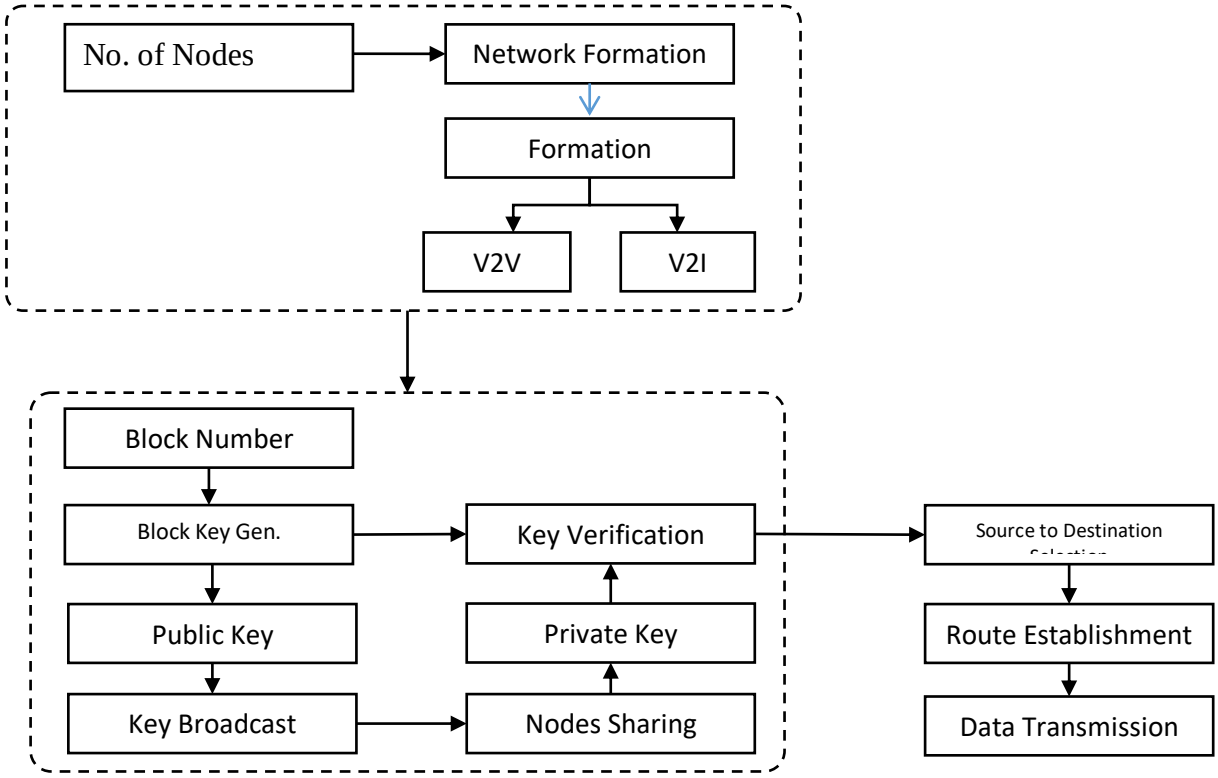

Figure.2. Configuration

The illustration depicts a typical VANET configuration, consisting of a Trusted Authority (TA), numerous vehicles, and Roadside Units (RSUs). RSUs are interconnected with the Internet to facilitate infotainment services while engaging with vehicles through wireless communication protocols compliant with the IEEE 802.11p standard.

Trusted Authority (TA): Responsible for registering RSUs and vehicles, the TA generates system parameters and distributes secret keys among members (RSUs and vehicles). It is assumed to possess ample computational and storage capabilities to prevent compromise by adversaries.

Roadside Units (RSUs): Serving as VANET infrastructure, RSUs communicate with vehicles to offer services such as information dissemination. Each RSU handles resource access

requests from vehicles within its communication range, acting as a proxy to retrieve corresponding resources from the Internet. Due to the limited bandwidth of the wireless communication channel allocated to VANETs, each RSU can only serve a limited number of vehicles within a specific timeframe.

Vehicles: Equipped with On-Board Units (OBUs), vehicles communicate with RSUs and other vehicles. Drivers or passengers can access infotainment services through OBU-RSU and OBU-OBU communications.

3.2. General Structure of Register-Based Distance Bounding Protocol

Initialization Phase: During this phase, the verifier (V) and the prover (P) may exchange messages such as random nonces and pre-generate all necessary materials for the distance-bounding phase. This minimizes processing delays during the time-critical distance-bounding phase, reducing the impact on distance calculation.

Distance-Bounding Phase: Comprising multiple rounds, each round involves V sending a challenge to P, who computes a response. V records the time difference between sending the challenge and receiving the response.

Verification Phase: V verifies the correctness of received responses and checks if the recorded round-trip times are within a predefined bound. If satisfied, V concludes that P is physically nearby and authenticated.

3.3. Performance Analysis

The performance analysis of TCP-SET in VANETs involves two scenarios: Static Row and Random Placement. Simulation parameters are provided, including source-destination pairs and attacker positions, with results averaged over ten simulations to reduce bias.

The SGKP-VANET protocol focuses on secure communication by

1. Cluster Head Selection based on adjacent nodes.
2. Temporary Public Key Distribution within clusters.
3. Verification and distribution of keys.
4. Secret Key Verification and computation.
5. Cluster Key Computation and merging.
6. Joining and Leaving Participant steps for group key updates.

RSU Selection involves broadcasting RREQ-Route Requests and generating ACK RREP, with cluster heads selected based on adjacency. Non-clustered participants join for data transmission.

Software and Simulation: The simulation utilizes MATLAB 8.3 R2014a, chosen for its robust simulation capabilities and extensive support for algorithm development and system modeling. Performance metrics like throughput and packet delivery ratios are evaluated under various attack scenarios to demonstrate the protocol's effectiveness.

4. Results

we're testing how secure our proposed protocols are against different kinds of attacks in VANETs. We're also looking at how adding extra security measures affects things like energy use and how long the network stays up. We're doing this by running simulations with

sensor networks, where we've set up a bunch of sensors in a field, each with its own energy and ability to communicate. We're seeing how well they transmit data over time and how they respond to potential security threats like impersonation or eavesdropping.

The comparison between the Conditional Privacy Protection (CPP) scheme and the Secure and Efficient Transmission (SET) protocol reveals distinct impacts on various performance metrics in VANETs. While CPP indirectly affects throughput through additional processing overhead for policy enforcement, the SET Protocol may introduce overhead due to cryptographic operations, albeit with efforts to maintain relatively high throughput. The impact of CPP on network lifetime depends on enforcement frequency and policy complexity, potentially shortening it if inefficiently implemented, whereas the SET Protocol aims to enhance security without significant network lifetime impact. In terms of energy consumption, CPP's impact is indirect, relying on access control policies that may require additional computational resources, while the SET Protocol primarily involves cryptographic operations, which can be energy-intensive but subject to modern optimizations. Lastly, neither CPP nor the SET Protocol directly affects total distance, although encryption choices in the SET Protocol may influence transmission distances due to computational requirements.

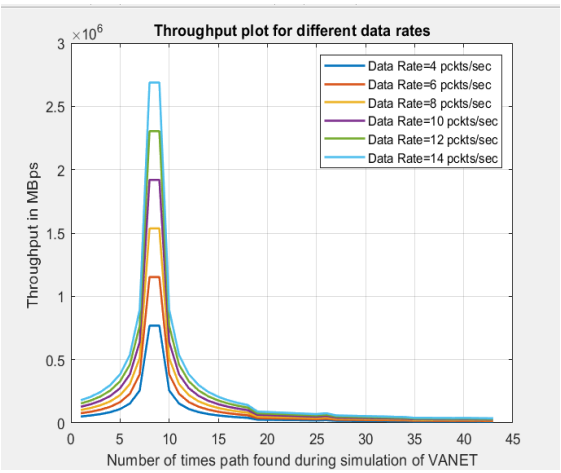

Figure.3. Throughput Plot

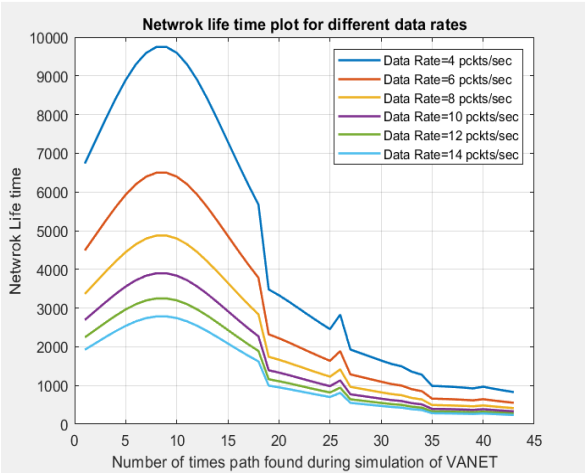

Figure.4. Network Lifetime

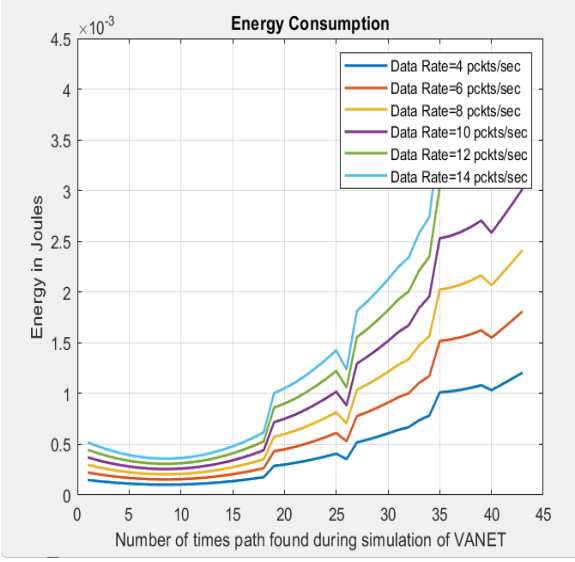

Figure.5. Energy Consumption

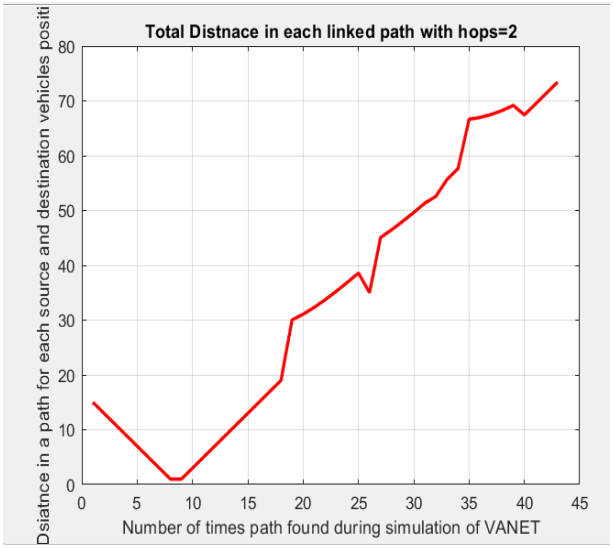

Figure.6. Total Distance

5. Conclusion

In this paper, we developed a novel routing and security framework for Secure and Efficient Transmission (SET) in Vehicular Ad-hoc Networks (VANETs). This framework prioritizes route stability alongside minimizing travel time, employing an incremental packet allocation scheme for efficient routing. By routing packets through multiple stable paths, including source routing-based Forwarding Information (FI) operation, we ensure reliable transmission. Our hybrid vehicular routing scheme leverages both Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communication for enhanced transmission performance. Through SET-based prediction of vehicle trajectories and relay selection, we optimize delay and forwarding probability. Simulation results demonstrate significant improvements over existing schemes in multi-hop data transmission metrics.

REFERENCES

[1]. A. Wasef and X. Shen, "Emap: Expedite message authentication protocol for vehicular ad hoc networks," IEEE Transactions on Mobile Computing, vol. 12, no. 1, pp. 78–89,(2013).

[2]. A. Yang, X. Tan, J. Baek, and D. S. Wong, "A new ADS-B authentication framework based on efficient hierarchical identity-based signature with batch verification," IEEE Transactions on Services Computing, vol. 10, no. 2, pp. 165–175, (2017).

[3]. D. He, S. Zeadally, B. Xu, and X. Huang, "An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks," IEEE Transactions on Information Forensics and Security, vol. 10, no. 12, pp. 2681–2691, (2015)

[4]. H. A. Omar, W. Zhuang, and L. Li, "Vemac: A tdma-based mac protocol for reliable broadcast in vanets," IEEE Transactions on Mobile Computing, vol. 12, no. 9, pp. 1724–1736, (2013).

[5]. H. J. Jo, I. S. Kim, and D. H. Lee, "Reliable cooperative authentication for vehicular networks," IEEE Transactions on Intelligent Transportation Systems, vol. 19, no. 4, pp. 1065–1079,(2018).

[6]. J. Ni, K. Zhang, Y. Yu, X. Lin, and X. Shen, "Privacy-preserving smart parking navigation supporting efficient driving guidance retrieval," IEEE Transactions on Vehicular Technology, vol. 67, no. 7, pp. 6504–6517, (2018).

[7]. J. Weng, J. Weng, Y. Zhang, W. Luo, and W. Lan, "Benbi: Scalable and dynamic access control on the northbound interface of sdn-based vanet," IEEE Transactions on Vehicular Technology, vol. 68, no. 1, pp. 822–831, (2019).

[8]. L. Zhang, Q. Wu, J. Domingo-Ferrer, B. Qin, and C. Hu, "Distributed aggregate privacy-preserving authentication in vanets," IEEE Transactions on Intelligent Transportation Systems, vol. 18, no. 3, pp. 516–526, (2017).

[9]. N. Cheng, F. Lyu, J. Chen, W. Xu, H. Zhou, S. Zhang, and X. Shen, "Big data driven vehicular networks," IEEE Network, vol. 32, no. 6, pp. 160–167, (2018).

[10]. S. Tzeng, S. Horng, T. Li, X. Wang, P. Huang, and M. K. Khan, "Enhancing security and privacy for identity-based batch verification scheme in vanets," IEEE Transactions on Vehicular Technology, vol. 66, no. 4, pp. 3235–3248, (2017).