ECC based Lightweight Authentication Protocol against Multi-Attack in Vehicular Communication

Ali Abbas

College of Information Technology, Al-Furat Al-Awsat Technical University, Technical Institute, Samawa, Iraq;
ali.abbas.isa@atu.edu.iq.

Abstract:

Vehicular ad-hoc networks (VANET) are the subset of mobile network and the major mode of communication of the vehicles are inter-vehicular communication and infrastructure based communication. This technology aims to provide high security at the time of data transmission among the devices. Due to the high speed of the devices certain malfunctions can occur in terms of multiple attacks which increase the data loss and delay among the devices in the network. To attend high quality in communication it is very essential to provide authentication for each data packet which is transmitted among the devices in the network. For that purpose in this article Elliptical Curve Cryptography (ECC) based lightweight authentication protocol (ECC-LMV) is developed which is able to provide high accuracy in data transmission.

Index Terms: Vehicular ad-hoc networks (VANET)

1 Introduction

In recent times vehicular communication and intelligent transmission system and this goes a fast advancement which provides the way to a time high quality communicative in the urban traffic with densely populated area [1]. In this technology, the cars in the network may connect with one another via communication messages delivered by the trusted authority (TA) [2]. The process of data sharing with improved traffic safety among the vehicles is the primary concentration of the network and it also provides emergency data transmission without any collision occurrences [3]. The roadside units transmit a warning message to each vehicle to avoid the traffic accident at the time of travel [4].

In general the devices which are present in the vehicular network communicate [5] with the external entities using several interfaces [6]. Through this interface there is a possibility for malfunction so that it becomes very essential to improve the security of transmitted packets using private information transmission among the devices [7]. That is able to secure the data from several abs dropping attacks and other denial of service attacks in the network [8]. Secondly the transmitted data needs to get its destination without any judgments and it is very essential to avoid traffic accidents [9]. With the presence of rapidly changing topology among the vehicles it needs an efficient security model to face the difficulty of data transmission in a highly efficient model [10]. This paper focuses on an ECC-based, light-weight authentication system to secure the network from numerous threats.

The major contribution of this article is described below. The sub sections of this article include an effective system model, threads model and lightweight authentication protocol. This process is able to improve the quality of service of the devices which are present in the network. The organization of the paper includes earlier research study, proposed model elaboration and experimental demonstration with conclusion.

2. Related Works:

In [41], proposd an efficient scheme addressing authorization, privacy, and source validation, validated through experiment with disadvantage of high power consumption. In [42], proposes a context-aware security quantification approach for VANET that overcomes obstacles from dynamic connections. Using a Homogeneous Continuous-Time Markov Chain (HCTMC), the approach enables adaptive defense strategies based on the environment and the drawback is high delay. In [43], Improved road safety utilizing the Trust Cascading-based Emergency Message Dissemination (TCEMD) concept. This model efficiently incorporates trust values for disseminating emergency messages during events, showing superior performance in theoretical analysis and highway simulations. In [44], proposed VANETs are crucial for intelligent traffic systems (ITS) but face security challenges in high-mobility

scenarios, such as Location-Based Services (LBS). Our blockchain-based trust model ensures privacy during LBS requests, resilient against trust model attacks but the disadvantages are high delay.

In [45], describes VANETs were the protocol selects junctions efficiently with real-time traffic updates and addresses security by monitoring vehicle duration under Roadside Units (RSUs), the disadvantage here is considerable packet loss. In [46], plained resources by relaying authentication exchanges without relaying subsequent services. Simulations confirm practicality, prompting the design of a cross-layer relay-resistant authentication protocol for effective mitigation and the drawback here is high overhead. In [47] explained Vehicular Ad-hoc Networks (VANETs) which enable efficient vehicle communication. This paper proposes a secure group mobility management scheme based on blockchain for fast authentication with enhanced security functionalities and the disadvantage are high overhead.

In [48], suggested SEMA protocol combines pseudonyms-based and group-based approaches to provide mutual authentication in (VANETs), proving resilience, computational efficiency, and practicality; nevertheless, the downside is excessive latency In [49], presents a fog computing-based solution, combining Decoy Technology (DT) and User Behavior Profiling (UBP) to enhance data security, privacy, and trust in vehicular cloud servers, here the disadvantage is high delay. In [50], explained BTCPS, a blockchain-based trust model which ensures VANET privacy through anonymous announcements and guarantees message reliability via RSUs and blockchain offering a secure and efficient solution. however, the downside is substantial packet loss..

In [51], implemented F–RouND, a Fog-based Rogue Node Detection scheme that dynamically identifies rogue nodes in VANETs with reduced processing delays, overhead, and False–Positive Rate (FPR) and the disadvantages are high delay. In [52], focuses on enhancing security in VANET Cloud by proposing an adaptable machine learning-based framework to counter DDoS attacks here the disadvantage is high power consumption. In [53], focuses on the security of the AODV protocol against Black Hole Attacks in VANET. It proposes a method for detection as well as prevention to boost security in Intelligent Transportation Systems, however the negative is substantial packet loss. The earlier model analysis with its merits and demerits are discussed in table 1.

3. Proposed ECC-LMV Network

This ECC-LMV is mainly developed to achieve high security among the high speed vehicles. The core modules which are present in the ECC-LMV are system model creation, threads model and light weight authentication protocol construction. The work flow of the ECC-LMV is described in figure 1.

3.1 System model:

We analyze a typical VANET consisting of many vehicles, RSUs, and a Trusted Authority (TA)In order to deliver entertainment services, RSUs are linked to the Internet. They communicate with automobiles using IEEE 802.11p-compliant wireless protocols.

1) TA: This trusted entity is in charge of registering RSUs and vehicles, particularly creating system settings and assigning members' secret keys (RSUs and vehicles). It is presumed that TA has enough processing power and storage capacity to prevent compromise by an attacker.

3.2 Treads Model:

This section outlines the security assumptions that characterize the attacker's and all system entities' capabilities. It also highlights system security threats that the attacker may use to carry out the planned assault. The TA is reliable and impervious to outside interference. RSUs are somewhat truthful; that is, they adhere to protocol while occasionally showing interest in private vehicle data. Vehicles have the potential to be malicious in that they may appear to be closer to RSUs in order to get access to the services; these attackers are known as insiders.

3.3 Lightweight Authentication Protocol

ECDSA, or elliptically equivalent to DSA, is a public key cryptography. Only authorized nodes should be able to access the vehicle's privacy; unauthenticated users should remain anonymous. By adding a digital signature to every

message, ECDSA serves the same function of message security. The algorithm is utilized to include more strength into the vehicle's safety. It is safer than the other available RSA and DSA algorithms because of its most advantageous feature—the comparatively short key length in comparison to other algorithms—which ensures that no other third party can access the private information shared between the two communicating parties.

Three phases make up the ECDSA classification:

4. Results and Discussion:

The implementation of this ECC-LMV is carried out in the software NS3 and the vehicles are moving condition and its mobility is generated using the additional software called sumo. To achieve the real time traffic open street map maps are taken into consideration. The parameters which are calculated to measure the performance of the network are data accuracy, data loss, routing overhead, throughput and average delay. To perform comparative analysis the ECC-LMV is compared with certain earlier works and they are SAES [51], SRML [52] and PDPS [53] and as well the input parameters which are present in this simulation experimentation are given in table 2.

4.1 Data Accuracy: The data accuracy of the devices is calculated according to the data success rate at the time of data transmission among the source and the destination in the network. Achieving maximum data accuracy is a primary goal of the ECC-LMV and in the figure 2 the accuracy calculation of the ECC-LMV is given and it is compared with the earlier works like SAES, SRML and PDPS. With the presence of ECC based authentication process the data security is highly increased that leads to increase the data accuracy among the devices. The success rate of the ECC-LMV is around 4% higher than the other methods.

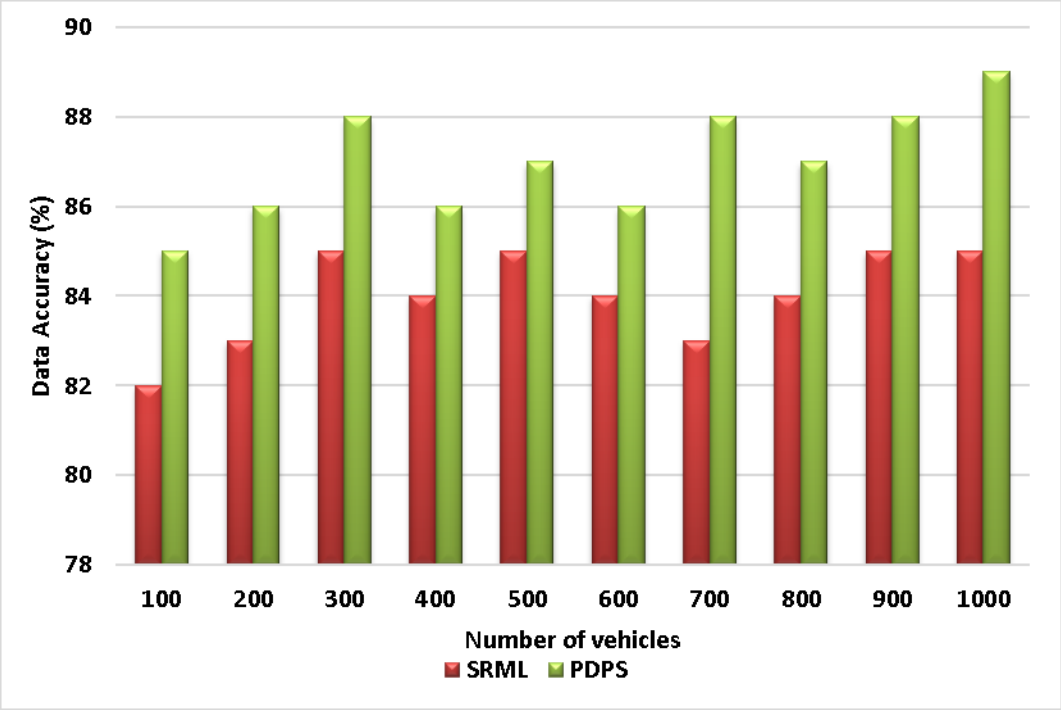

Figure 2 - Data Accuracy

4.2 Data Loss: It is the amount of data which gets lost at the time of high speed communication among the vehicles. To reduce the packet loss in the article efficient authentication models are constructed. In figure 3 the loss of packet calculation of the ECC-LMV illustrated and it is compared with the other methods like SAES, SRML and PDPS. The calculated result proves that the ECC-LMV performed lower loss which is around 15 percent lower than the other methods.

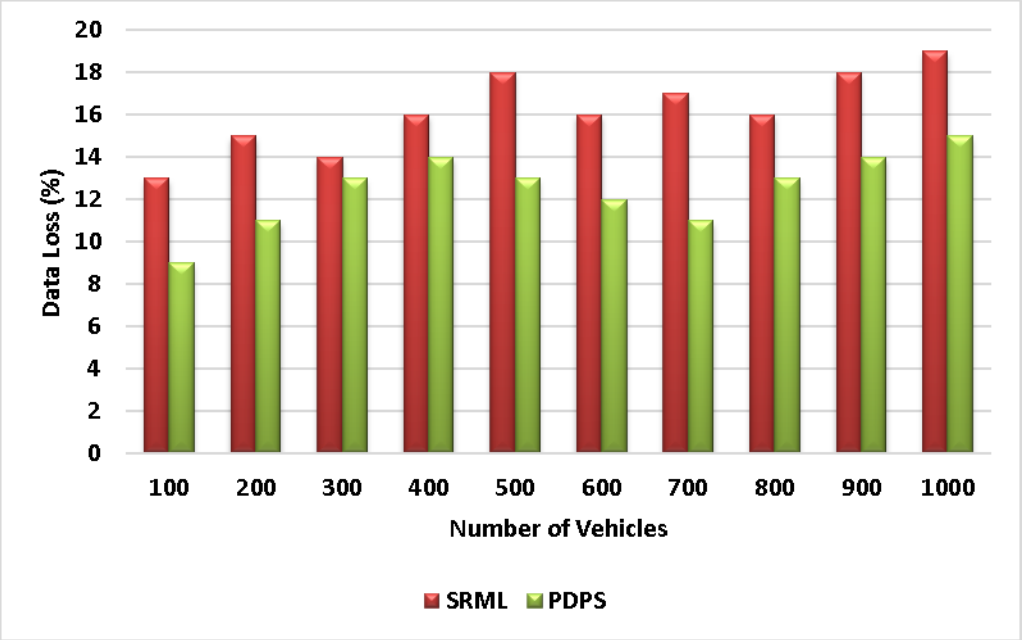

Figure 3 - Data Loss

4.3 Routing Overhead: It is the calculation of data forward packets which are generated at the time of data transmission among the high speed vehicles. In figure 4 the routing overhead calculation is performed among the ECC-LMV and the other methods like SAES, SRML and PDPS. From this calculated result it is understood that the ECC-LMV generates lower routing overhead which is around 300 packets lower than the other methods.

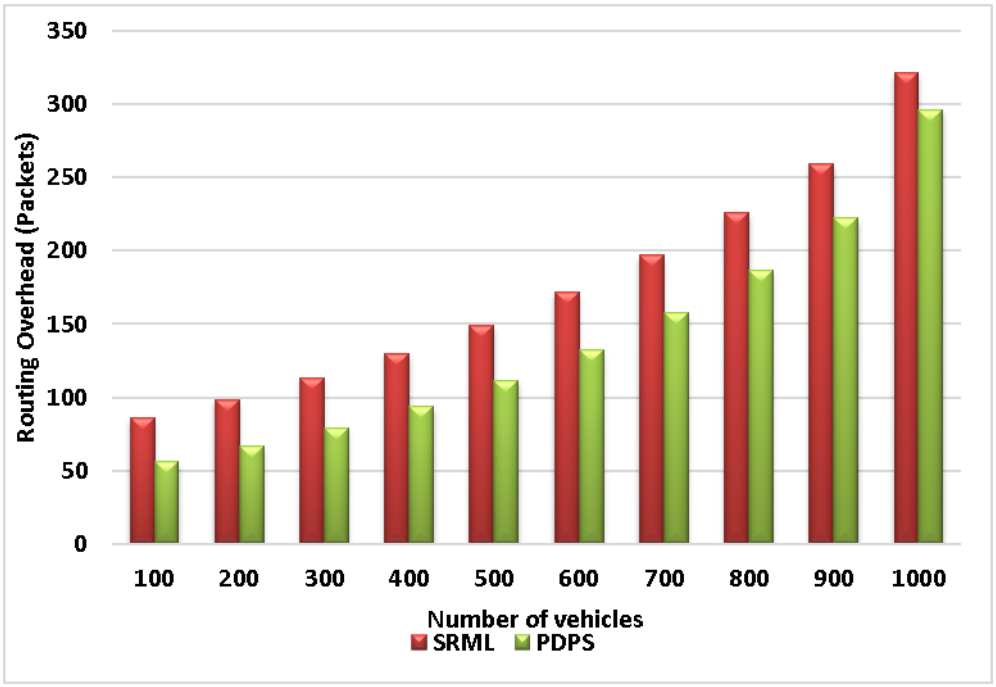

Figure 4 - Routing Overhead

4.4 Throughput: It is defined as the amount of generated packages among the source vehicles in the network. In order to achieve better performance it is very essential to maximize the throughput level of the network. In figure 5

the throughput analysis illustrated among the ECC-LMV and the earlier methods like SAES, SRML and PDPS. From this result it is identified that the ECC-LMV generates maximum throughput which is around 200kbps higher than other methods.

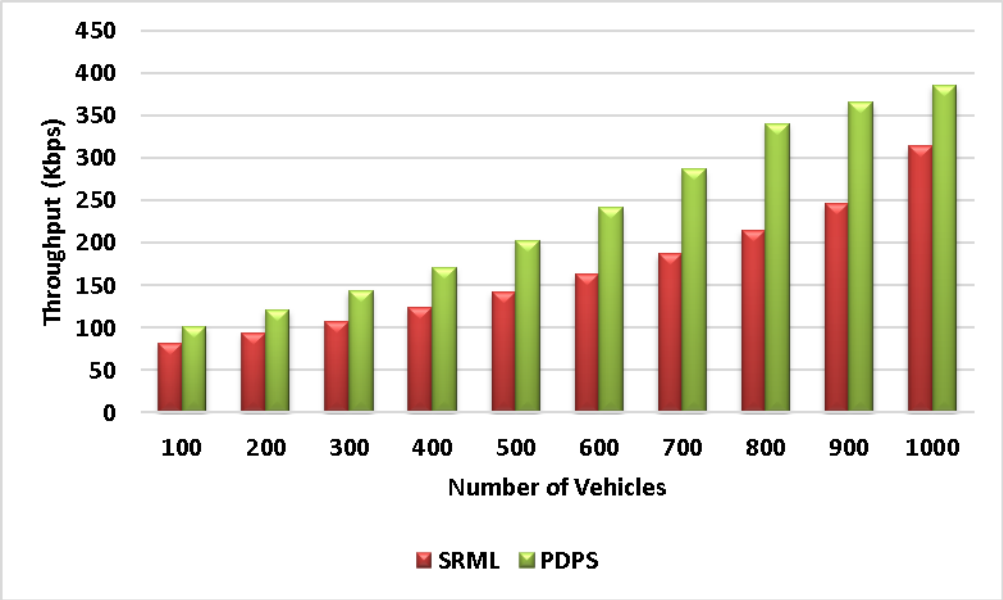

Figure 5 - Throughput

4.5 Average Delay: It is defined as a time difference between the allocated time and the received time of the data from the source to the destination. Reduction of delay leads to better efficiency among the vehicles in the network. In figure 6 the delay calculations are described. It proves that the ECC-LMV produce lower delay when compared with the other methods like SAES, SRML and PDPS.

5. Conclusion:

The aim of this ECC-LMV model is to provide high authentication among the vehicles at the time of data transmission between one another. To protect the data from the multiple attacks it is very essential to provide authentication among the devices. An improved authentication model is required to concentrate on the high speed vehicle data transmission. For that purpose in this article ECC based lightweight authentication protocol is developed. This concept is implemented in the software ns3 and the result shows that it is better than earlier baseline methodology in terms of data accuracy and throughput. In the future, trust model is concentrated to provide high accuracy in the densely populated area.

6. References:

[1] R. Q. Malik, K. N. Ramli, Z. H. Kareem, M. I. Habelalmatee, A. H. Abbas, and A. Alamoody, "An Overview on V2P Communication System: Architecture and Application

[2] M. I. Habelalmateen, A. H. Abbas, L. Audah, and N. A. M. Alduais, "Dynamic multiagent method to avoid duplicated information at intersections in VANETs," Telkomnika

[3] M. K. Hasan, M. M. Ahmed, N. F. Wani, A. H. Abbas, L. M. Alkwai, S. Islam, A. K. M. A. Habib, and R. Hassan, "Dynamic load modeling for bulk load-using

[4] F. Abedi, S. R. M. Zeebaree, Z. S. Ageed, H. M. A. Ghanimi, A. Alkhayyat, M. A. M. Sadeeq, S. N. Mahmood, A. S. Abosinnee, Z. H. Kareem, A. H. Abbas, W. K. Al-

[5] A. H. Kadhim, A. M. Razaq, M. A. Jubair, N. F. Abdulsattar, A. H. Abbas, M. H. Hassan, A. Jamal Ahmed, S. AbdulJabbar Rashid, and M. I. Habelalmateen, "A Real-Time Low-Cost

[6] A. H. Abbas, A. J. Ahmed, S. A. Rashid, M. A. Jubair, N. F. Abdulsattar, H. S. Mansour, and M. I. Habelalmateen, "Hybrid ANT Based Continuous Cuckoo Search Optimization

[7] F. Abedi, H. M. A. Ghanimi, M. A. M. Sadeeq, A. Alkhayyat, Z. H. Kareem, S. N. Mahmood, A. H. Abbas, A. S. Abosinnee, W. K. Al-Azzawi, M. M. Jaber, and M. Dauwed,

[8] A. H. Abbas, H. Mansour, and A. Al-Fatlawi, "Self-Adaptive Efficient Dynamic Multi-Hop Clustering (SA-EDMC) Approach for Improving VANET's Performance

[9] I. Ahmad, S. Hussain, S. N. Mahmood, H. Mostafa, A. Alkhayyat, M. Marey, A. H. Abbas, and Z. Abdulateef Rashed, "Co-Channel Interference Management for

[10] A. H. Abbas, N. F. Abdulsattar, H. S. Mansour, M. H. Mutar, M. I. Habelalmateen, L. Audah, N. A. M. Alduais, and A. Mohammed, "A New Hybrid Approach Cluster-

[11] F. Abedi, H. M. A. Ghanimi, A. D. Algarni, N. F. Soliman, W. El-Shafai, A. H. Abbas, Z. H. Kareem, H. M. Hariz, and A. Alkhayyat, "Computational Intelligence Driven Secure

[12] A. M. Abdulkarem, F. Abedi, H. M. A. Ghanimi, S. Kumar, W. K. Al-Azzawi, A. H. Abbas, A. S. Abosinnee, I. M. Almaameri, and A. Alkhayyat, "Robust Automatic Modulation Classification Using Convolutional

[13] A. H. Abbas, A. J. Ahmed, and S. A. Rashid, "A Cross-Layer Approach MAC/NET with Updated-GA (MNUG-CLA)-Based Routing Protocol for VANET

[14] H. S. Mansour, M. H. Mutar, I. A. Aziz, S. A. Mostafa, H. Mahdin, A. H. Abbas, M. H. Hassan, N. F. Abdulsattar, and M. A. Jubair, "Cross-Layer and Energy-Aware

[15] M. A. Jubair, S. A. Mostafa, D. A. Zebari, H. M. Hariz, N. F. Abdulsattar, M. H. Hassan, A. H. Abbas, F. H. Abbas, A. Alasiry, and M. Turki-Hadj, "A QoS Aware Cluster Head

[16] M. I. Habelalmateen, A. J. Ahmed, A. H. Abbas, and S. A. Rashid, "TACRP: Traffic-Aware Clustering-Based Routing Protocol for

[17] S. A. Rashid, M. I. Habelalmateen, A. J. Ahmed, A. H. Abbas, M. A. Jubair, M. H. Hassan, A. Abdulhadi, S. Hammed, and L. Audah, "Congestion Aware Genetic Q-learning Based RPL Routing Protocol

[18] A. H. Abbas, A. J. Ahmed, S. A. Rashid, N. F. Abdulsattar, M. H. Hassan, M. A. Jubair, and M. I. Habelalmateen, "Predictive Hybrid Routing with Multi Objective Optimization Model for

[19] A. H. Najim, A. H. Abbas, K. Al-sharhanee, and H. M. Hariz, "Reinforcement Learning-based Topology-Aware Routing Protocol with Priority Scheduling for Internet of Drones in Agriculture Application," Inte

[20] A. H. Alwan, A. A. Aziz, M. A. Jubair, A. H. Abbas, M. H. Hassan, S. Alheejawi, N. F. Abdulsattar, A. S. Mustafa, and M. I. Habelalmateen, "Monitoring the Impact of the Nodes Density on