Elliptic Curve Cryptography in Vehicle Security

Erin Manson
Department of Physics and
Computer Science
Wilfrid Laurier University
Waterloo, Canada

Ryan Mood
Department of Physics and
Computer Science
Wilfrid Laurier University
Waterloo, Canada

ARTICLE INFO

ECC
VANET
Smart Cities
Security
Authentication

ABSTRACT

Vehicular Ad-Hoc Networks (VANETs) are connected networks of vehicles and infrastructure that allow for communication between parties. VANETs are ever changing now that technology in and around vehicles is rapidly changing as well. Sensors, personal devices, and autonomously driving vehicles all pose new security threats to smart cities. Elliptic Curve Cryptography (ECC) can offer increased security and lowered computational effort in many of these scenarios. Our work will systematically review how ECC is being applied in real world scenarios and how it can be applied in the future to improve vehicle security in VANETs.

1. INTRODUCTION

As vehicles become more advanced the need for cryptographic security measures has also increased. Vehicular Ad-Hoc Networks (VANETs) enable communication between vehicles (V2V) and vehicles to roadside assistance, infrastructure, and other sources (V2I) [5]. As smart cities continue to evolve vehicles need to communicate with other entities such as sensors, personal devices, and pedestrians [9]. VANETs are evolving and so are the threats to the rapidly increasing number of communications vehicles must perform.

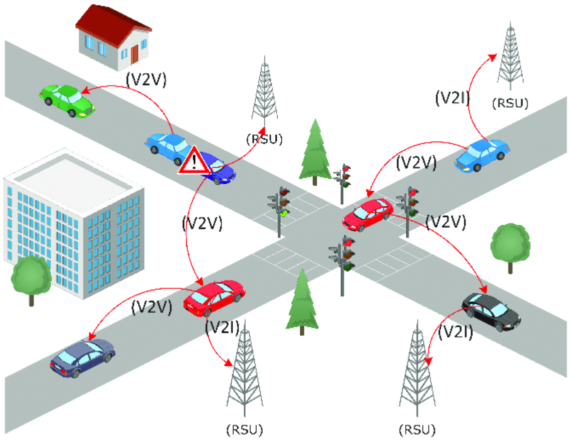

Fig. 1. Communication in VANETs [11]

Previously asymmetric cryptographic schemes like RSA (Rivest-Shamir-Adleman) were used in vehicle security but as the need for bandwidth and security has increased Elliptic Curve Cryptography (ECC) has shown to have an edge over RSA and similar schemes especially on embedded platforms [4]. ECC reduces computational effort needed in other asymmetric schemes like RSA, it implementation involves using points on a curve rather than integers. Elliptic curves are said to have approximately the same number of points as the prime p used in the equation of the curve. For example, an elliptic curve created with p = 11 would have about eleven points. ECC requires a significantly smaller key size for the equivalent security in RSA. This is due to the larger amount of points available on the curve. Parameters are significantly smaller for ECC algorithms opposed to RSA, which decreases storage needs and computational effort as mentioned above [4]. This is of great importance for VANET security because storage space will be limited on small and embedded devices, and it will offer greater security relative to key size. Security is of utmost importance in vehicle security because of the sensitive nature of vehicle security related to personal safety.

1.1 Threats and Disadvantages

While encryption time is faster using ECC compared to other common choices, RSA offers faster decryption time [4]. This is a downside of using ECC however, security concerns related to RSA are too prominent to ignore. Factors such as resource usage and bandwidth savings must also be taken into account, which leaves ECC at a clear advantage [4].

Successful attacks to ECC are much less common than those against RSA. The most successful attacks on ECC are Baby-Step Giant-Step and the Pollard-Rho Method [1]. Baby-Step Giant-Step aims to solve the discrete logarithm problem by dividing the problem up into baby steps where values are computed and stored in a hash table based on the square root of the group size or number of points, and giant steps where a calculation is performed to receive a value [1]. If a match is found in the hash table after the giant step value is computed the discrete logarithm problem has been solved and the system is susceptible to threats. ECC schemes aim to have such a large number of points that the square root of p (prime used in creating the elliptic curve) cannot be computed. If the prime used is too small the curve is again susceptible to Baby-Step Giant-Step attacks. The other main attack on ECC is the Pollard Rho method which again aims to solve the discrete logarithm problem. The Pollard Rho method essentially searches for collisions on the curve (where two inputs give the same output) which are inevitable because of the finite field [1]. This is much faster than a brute force attack and given infinite time would be unbeatable. Elliptic curves with small primes again are much more susceptible to these attacks because collisions will be found faster. Both of these attacks do pose a threat to ECC however, the risks can be easily mitigated by increasing the prime which the elliptic curve was based on.

1.2 Research Goals and Layout

While there is much existing research on vehicle security in regard to cryptographic methods as well as Elliptic Curve Cryptography, we wish to find practical applications of ECC in terms of vehicle security. We will systematically review the current research available in applying ECC to VANETs as the need for vehicle security continues to evolve in smart cities. Studies on secure message communication between vehicles, privacy-preserving authentication schemes, how to increase security in VANETs, and how to evade inclusion of fake vehicles in VANETs by utilizing ECC will be examined. We will be guided by three main research questions in order to uncover the challenges, applications, and advantages of ECC in real life scenarios.

Table 1.

Research Questions (RQ)
RQ1: How can ECC enhance the security of VANETs and prevent attacks in smart cities?
RQ2: What advantages does ECC have over current cryptographic security measures?
RQ3: What challenges will arise in the implementation of ECC in VANETs?

In this paper section 2 will detail our findings and outline the current relevant research regarding ECC and VANET security. Section 3 will cover our methodology and the techniques we used to review the current research. Section 4 will offer suggestions for future research based on our findings. Section 5 will draw conclusions on our work, summarize our findings, and recommendations.

2. RESULTS

Elliptic Curve Cryptography presents itself as a newly emerging tool with the responsibility of addressing rapidly growing security concerns in vehicular technology. As vehicles become more advanced, they present a variety of new challenges including but not limited to vehicle-to-vehicle communications, secure sensor communication, and on-board systems. ECC has been shown by various studies to be very effective in securing vehicular networks through offering robust encryption with small key sizes and low computational cost. The table below clearly outlines findings from various research papers, showcasing the capabilities of ECC and its various applications for vehicular security.

Table 2.

Study	Key Findings	Application
[2]	ECC can be used to address authentication and distribution of messages among smart vehicles. It’s small key length and strong encryption make it effective and efficient for modern vehicle security challenges.	VANET Security
[8]	A novel encryption method, AHOA-EECC is shown to improve VANETs through identifying and isolating malicious nodes. It was shown to reduce time complexity, although it requires further performance optimization to	VANET Trust Systems

	counteract delays and collisions.	
[9]	This paper introduces a modified ECC solution through dynamic cryptographic secure elliptic curve selection stored on on-board devices. This method offers improved performance, a flexible and scalable design, although it does require additional storage compared to a traditional ECC scheme.	On-Board Embedded Devices
[14]	This paper proposes a three-party authentication and key agreement protocol based on elliptic curve public cryptography. They propose this as a solution to address existing challenges with identity authentication and key agreements between the On-Board Unit and Roadside Unit in VANETs, including impersonation attacks, RSU impersonation and vehicle privacy leakage. The use of ECC allowed for efficient storage utilization and computing efficiency, allowing for implementation in vehicles with limited computing power.	On-Board Unit and Roadside Unit Security in VANETs
[3]	Goudarzi et al, 2022, proposed a scheme in which a Quotient Filter is used for node authentication while Elliptic Curve Cryptography is used for message authentication within VANETs. The ECC-based authentication scheme can	Vehicle Node Security

	ensure authenticity of messages from the vehicle node before initiating data sharing. This successfully allows them to identify illegitimate vehicle nodes and invalid messages when the fog-enabled VANET is possibly exposed to outside attacks.	
[10]	In VANETs, there are plenty of security and privacy threats due to its wide-open nature and in this study, they aim to address them with an enhanced Elliptic Curve Cryptography-based certificate-less signature aggregation scheme. This proposal alleviates certificate management, while maintaining privacy, anonymity and security.	Highly Dynamic and Volatile VANETs

	Furthermore, resource demands are minimized through not employing bilinear pairing operation or map-to-point hash functions which also increase suitability for highly volatile and resource constrained VANET environments.	
[7]	The Weighted Average Sandpiper Coot Optimal (WASCO) routing protocol was designed using Elliptic Curve Cryptography and is proposed to address challenges and vulnerabilities within vehicle occupancy privacy and safety. This protocol was shown to decrease authentication delay while also increasing the packet delivery ratio (*figures 1, 2 and 3)*	Vehicle Occupancy Privacy and Safety

	compared to other popular methods.	

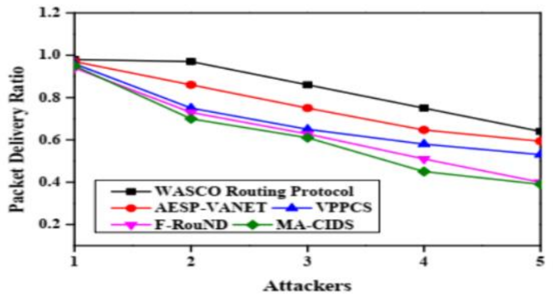

Fig. 2. [7]

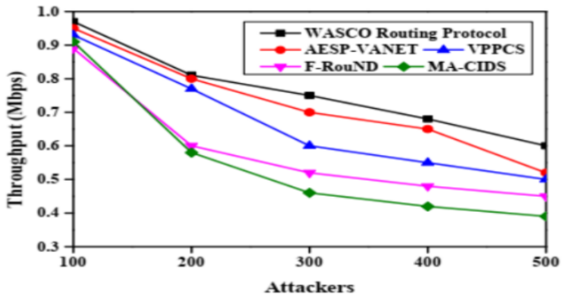

Fig. 3. [7]

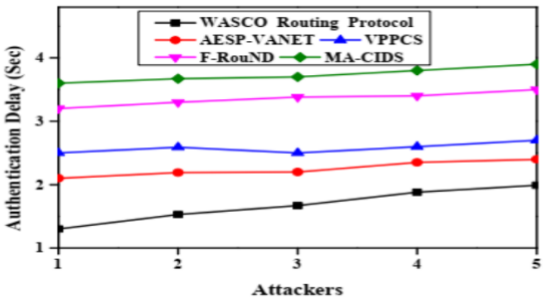

Fig. 4. [7]

The findings of the articles viewed, can be directly applied to our research questions presented earlier.

RQ1: How can ECC enhance the security of VANETs and prevent attacks in smart cities?

The literature discussed prior demonstrates that ECC offers significant enhancements towards VANETs. ECC boasts a wide range of applications including message authentication (Goudarzi et al., 2022) three-party authentication protocols [14]. These in combination help to address critical issues in smart cities including impersonation, vehicle privacy leakage and malicious node detection.

RQ2: What advantages does ECC have over current cryptographic security measures?

ECC is able to distinguish itself from alternative cryptographic security measures due it its smaller key size while not reducing security levels. This plays a particularly important role within vehicular security as there is often strict computational and storage constraints in place. Dua et al. (2016) showed ECC increases efficiency in authentication processes, while Patil & Adhiya (2023) demonstrated improved time complexity through AHOA-EECC [2, 8]. The combination of these factors as shown by Rajkumar & Kumar (2023), demonstrate the computational requirements are virtually eliminated due to the lack of resource-intensive operations being performed with ECC [10].

RQ3: What challenges will arise in the implementation of ECC in VANETs?

While ECC demonstrates promising solutions to many current problems within VANETs, there are some challenges posed with implementation. Certain implementation of ECC, including dynamic cryptographic protocols, will require additional storage [13], and may face limitations from specific devices. Furthermore, protocols like AHOA-EECC [8], may face issues with delays and packet collisions on crowded networks, requiring further configuration as a possible solution. Addressing these challenges, through further research and designing is critical for the implementation of ECC in VANETs.

3. DISCUSSION

The use of Elliptic Curve Cryptography has emerged as a viable solution for addressing modern day vehicular network security challenges including authentication, secure communication and data privacy. The studies reviewed helped to highlight the strengths and weaknesses of ECC, providing an objective perspective on the viability of this solution as the vehicle network security needs continue to grow. Elliptic Curve Cryptography offers large potential boasting low computational overhead, efficient storage utilization and smaller key sizes with robust encryption making it suitable for all vehicular environment demands.

The studies discussed in the results section were sourced through a systematic literature search. The primary source for this search was Google Scholar through using key words including Elliptic Curve Cryptography and VANET to guide the search. Examining the abstract and keyword sections of papers from reliable sources like Google Scholar was essential before proceeding to read papers to ensure relevancy. Papers were then read in their entirety, only those directly related to ECC and its applications in VANETs were included. Additionally, references within selected papers were reviewed for foundational knowledge and related studies to further support our research questions. This approach allowed for comprehensive and objective reporting of current findings in the field regarding our topic.

The results of this review demonstrate the immense potential of Elliptic Curve Cryptography for addressing the ever-growing concerns of vehicular security. Through viewing key research regarding applying ECC to VANETs, we examined several key themes across them.

i. Authentication and Trust in VANETs:

Elliptic Curve Cryptography has outstanding potential for addressing the rapidly evolving multifactored security concerns emerging within vehicle technology. Dua et al., (2016), highlighted how ECC excels in efficiency for VANET security while Goudarzi et al. (2022) demonstrates its resiliency in preventing unauthorized nodes and messages [2, 3].

ii. Addressing Privacy and Key Management Challenges:

Innovations such as certificate-less signature aggregation schemes from Rajkumar and Kumar (2023) help to address key management issues while maintaining anonymity [10]. These methods help to further reduce computational demands, demonstrating its applicability to specifically vehicular security environments.

iii. Enhanced Protocol Design:

WASCO routing as demonstrated by Patil and Mallapur (2024), illustrates how ECC is able to optimize routing while being able to simultaneously maintain vehicle privacy [7]. Alongside that, they demonstrated that ECC lead to improved performance metrics including decreasing authentication delay while also increasing the packet delivery ratio.

iv. Integration:

The flexibility of ECC leads to improved integration with limited computational and storage capacities within vehicular devices. Yu et al. (2024) further demonstrates this integration potential with an ECC-based protocol providing efficient authentication and limited storage requirements [14].

Vulnerabilities were also reviewed in depth to ensure all aspects of the application of ECC in vehicular security were examined fairly. Despite the key themes mentioned above, some challenges remain. The primary limitations mentioned revolve around increased storage requirements and potential delays as noted in Wang et al. (2019) and Patil & Adhiya (2023) respectively [13, 8]. It is important to note that this can be minimized with optimization as noted in many studies including Yu et al. (2024), leading to ECC being a viable choice to implement in VANET security [14].

After gaining an in depth understanding of ECC and VANET fundamentals we chose to discuss two main areas where we believe ECC would be a good fit for security improvements and innovation in Section 4.

4. RECOMMENDATIONS

As previously mentioned ECC is still emerging in the field of vehicle security. While the above articles explore some applications in VANETs, we must acknowledge that VANETs and vehicles are rapidly evolving. Cars are now equipped with features like keyless entry, and soon we will see more autonomous driving on roads. Small devices with high security concerns like car keys that require repeated and quick authentication is largely unexplored. Autonomous driving will present a variety of threats; one topic of interest is V2V communication between autonomous vehicles to coordinate key tasks like braking and lane changing. These two topics are of great interest for future research and below we will explore the limited existing research in these two areas.

4.1 Keyless Entry Using ECC

Keyless entry is a seemingly perfect fit for ECC due to the small, embedded nature of car keys devices. Heyszl & Stumpf (2010) propose a novel approach for Efficient One-Pass Entity Authentication based on ECC for Constrained Devices [6]. Mentioned in the study is how this protocol can be applied in real life scenarios like keyless entry to buildings and remote keyless entry for vehicles [6]. The use of ECC in this context would be a good fit due to the repeated authentication needed by systems such as car keys. Constrained remote devices with high security needs are a great fit for ECC however there is limited research available on real world applications. This article highlights the lack of research done on the topic of keyless entry with ECC because the protocol developed by Heyszl & Stumpf was published in 2010 with no research to follow. No other articles seemed to come to the same conclusion on the topic of keyless entry and ECC being a good fit for one another which leaves room for future research opportunities.

4.2 Autonomous V2V Communication

Vehicle to vehicle (V2V) communication in VANETs is changing alongside vehicular technology which offers opportunities for new research to be conducted. Smart cities will soon have technology such as autonomous vehicles as a new norm and security concerns will rise. We wished to explore new ideas related to ECC being applied to V2V communications in VANETs but limited research is currently available. Vybornova (2024) discusses secure communication protocols for V2V communication specifically regarding autonomous vehicles [12]. The article explores modern threats which many studies lack such as quantum computing and their threat to using ECC and other protocols for securing communication. As autonomous vehicles gain in popularity security must be held to a high standard due to passenger and pedestrian safety, there is no room for error. Not many studies have addressed modern threats as this study does, the fact that this lone study was published in August of 2024 also illustrates the lack of research in this area. New concepts such as using Machine Learning and Artificial Intelligence to analyze security risks in autonomous vehicles more effectively were also discussed and have limited existing research available.

Research Agenda 1: Remote entry for vehicles and buildings offers a great opportunity for ECC to innovate security as mentioned above. There is limited existing research and the existing research that does exist on the topic is not recent. Again, high security needs and constrained device size is a good fit for ECC to be applied, which leaves room for future research to be conducted on real life applications and results.

Research Agenda 2: V2V communication in autonomous vehicles is a major concern as smart cities continue to evolve. There is minimal research available in this area which offers a great opportunity for future research to be conducted.

5. CONCLUSION

Our work has outlined applications of Elliptic Curve Cryptography in terms of vehicle security. VANETs are ever changing as technology in and around vehicles changes as well. Security needs will also change as new technology makes its way into our world. ECC offers improved security from other asymmetric cryptography protocols like RSA. This is due to the smaller key size and reduced computational effort. We conducted an in-depth review of scholarly sources which discussed real world applications of ECC in vehicle security. Our research questions were answered while taking into account threats against and drawbacks of using ECC. ECC offers improved security to vehicle security and there is plenty of research to be done as new technologies arise specifically in regard to keyless entry and V2V communication amongst autonomous vehicles as discussed above. Overall ECC will continue to make an impact on vehicle security in VANETs as they evolve.

REFERENCES

[1] Aung, T. M., & Hla, N. N. (2017). A Study of General Attacks on Elliptic Curve Discrete Logarithm Problem Over Prime Field and Binary Field. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3269714

[2] Dua, A., Kumar, N., Singh, M., Obaidat, M. S., & Hsiao, K.-F. (2016). Secure message communication among vehicles using elliptic curve cryptography in smart cities. *IEEE*. https://doi.org/10.1109/cits.2016.7546385

[3] Goudarzi, S., Soleymani, S. A., Anisi, M. H., Azgomi, M. A., Movahedi, Z., Kama, N., Rusli, H. M., & Khan, M. K. (2022). A privacy-preserving authentication scheme based on Elliptic Curve Cryptography and using Quotient Filter in fog-enabled VANET. *Ad Hoc Networks*, *128*, 102782. https://doi.org/10.1016/j.adhoc.2022.102782

[4] Gupta, K., & Silakari, S. (2011). ECC over RSA for Asymmetric Encryption: A Review. *International Journal of Computer Science Issues*, *8*(3), 370. 2. https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=49e1b49d6c34e6395017f733073ee262480a73f0

[5] Hasrouny, H., Samhat, A. E., Bassil, C., & Laouiti, A. (2017). VANet security challenges and solutions: A survey. *Vehicular Communications*, *7*, 7–20. https://doi.org/10.1016/j.vehcom.2017.01.002

[6] Johann Heyszl, & Stumpf, F. (2010). *Efficient one-pass entity authentication based on ECC for constrained devices*. https://doi.org/10.1109/hst.2010.5513107

[7] Patil, A. N., & Mallapur, S. V. (2024). WASCO Routing Protocol: Enhancing Security in Vehicular Adhoc Networks (VANETs) using Weighted Average Sandpiper Coot Optimal Approach. *2024 4th International Conference on Innovative Practices in Technology and Management (ICIPTM)*, 1–8. https://doi.org/10.1109/iciptm59628.2024.10563935

[8] Patil, M. J., & Adhiya, K. P. (2023). An Enhanced Elliptic Curve Cryptography Scheme for Secure Data Transmission to Evade Entailment of Fake Vehicles in VANET. *Cybernetics and Systems*, 1–35. https://doi.org/10.1080/01969722.2022.2157601

[9] Paul, A., Naveen Chilamkurti, Daniel, A., & Rho, S. (2017). Vehicular network (VN) model. *Elsevier EBooks*, 43–75. https://doi.org/10.1016/b978-0-12-809266-8.00003-x

[10] Rajkumar, Y., & Kumar, S. (2023). An elliptic curve cryptography based certificate-less signature aggregation scheme for efficient authentication in vehicular ad hoc networks. *Wireless Networks*, *30*(1), 335–362. https://doi.org/10.1007/s11276-023-03473-8

[11] Shah, S. S., Malik, A. W., Rahman, A. U., Iqbal, S., & Khan, S. U. (2019). Time Barrier-Based Emergency Message Dissemination in Vehicular Ad-hoc Networks. *IEEE Access*, *7*, 16494–16503. https://doi.org/10.1109/access.2019.2895114

[12] Vybornova, Dr. E. (2024). Secure Communication Protocols for Vehicle-to-Vehicle Communication in Autonomous Vehicles. *Distributed Learning and Broad Applications in Scientific Research (DLBASR)*, *10*. https://dlabi.org/index.php/journal/article/view/77/76

[13] Wang, J., Li, J., Wang, H., Leo Yu Zhang, Cheng, L.-M., & Lin, Q. (2019). Dynamic Scalable Elliptic Curve Cryptographic Scheme and Its Application to In-Vehicle Security. *IEEE*, *6*(4), 5892–5901. https://doi.org/10.1109/jiot.2018.2869872

[14] Yu, W., Zhang, R., Ma, M., & Wang, C. (2024). A Noval and Efficient Three-Party Identity Authentication and Key Negotiation Protocol Based on Elliptic Curve Cryptography in VANETs. *Electronics*, *13*(2), 449–449. https://doi.org/10.3390/electronics13020449