A Comprehensive Approach to Combat GPS Spoofing and Ensure Security Positioning in Autonomous Vehicles

Laid Kenioua
AI Laboratory and its Applications
University of Eloued, Algeria
Kenioua-laid@univ-eloued.dz

Brahim Lejdel
Computer Science Department
University of Eloued, Algeria
Brahim-lejdel@univ-eloued.dz

Mohamed Abdelhamid Nedioui
Computer Science Department
University of Eloued, Algeria
nedioui-abdelhamid@univ-eloued.dz

Abstract: *The emergence of Autonomous Vehicles (AVs) marks a significant turning point in the future of transportation and reflects radical advancements in artificial intelligence, edge computing, advanced sensing systems, and advanced control. These vehicles have sophisticated sensors, artificial intelligence systems, and computing capabilities that enable them to drive and operate without human intervention. They rely on various technologies such as cameras, radar, and Devices Satellite Locations (GPS) to obtain precise information about their surroundings and make real-time decisions. However, AVs face several unique challenges. They depend on accurate and reliable location information to drive and operate, ensuring safe driving and real-time decision-making. One of the major challenges is that central positioning systems are vulnerable to attacks, security breaches, spoofing attacks, and signal jamming, which can tamper with vehicle command systems. The significance of accurately determining the vehicle's location lies in improving driving precision, efficient decision-making, enhanced mobility in different environments, and ensuring constant communication among vehicles for better collective performance. In this research, we propose an engineering model based on mixed collaboration for secure measurement in autonomous vehicle positioning. This collaboration enhances cooperation among vehicles, where the leader obtains its location through satellite identification, and the rest of the group members depend on the leader's location to determine their positions in a highly reliable and immune manner against GPS spoofing, signal jamming, and fraudulent attacks. Additionally, to ensure secure communication among different vehicles, a strong encryption system has been adopted to send messages within the proposed framework, ensuring higher reliability. The technique used is lightweight and robust because it uses only one operation of multiplication and only one exponential operation. Moreover, network traffic analysis and the complexity of different algorithms have been assessed to ensure the efficiency and effectiveness of the proposed framework.*

Keywords: *Autonomous vehicles, positioning security, secure communication, semi-decentralized collaboration architecture, edge computing, data collection, consensus.*

Received January 31, 2024; accepted July 15, 2024
https://doi.org/10.34028/iajit/21/4/7

1. Introduction

One of the results of technological development is the emergence of self-driving vehicles, which are seen as a revolution in transportation systems, monitoring, disaster management, and search operations. As it gives solutions and guarantees for safer, safer, and more efficient transportation through self-driving using smart systems. With the development of computing processes, Autonomous Vehicles (AVs) have become dependent on edge computing, and each vehicle crosses an edge unit [5]. Self-driving vehicles do not run directly from the vehicle but rather need an administrator to monitor them from a wireless station in a remote location. The official intervenes only in dangerous or critical cases or emergency situations to avoid disasters [27].

During research, monitoring, and disaster management processes, the importance of teamwork forself-driving vehicles are highlighted. Where they form together a portable sensor network that enables them to communicate and coordinate while performing tasks. Airborne Communication Networks (ACNs) provide rapid response for emergency communications and accurate surveillance services [16], and this is what gave it great importance and interest from researchers, one of which is the characteristics of the network distinguished by its high dynamic network topology, which is What gave power to vehicles and their communication in difficult tasks in large and remote geographical areas.

In small distances and in limited geographical areas, self-driving vehicles can be controlled by radio waves and several controls, but this is not possible in open and remote geographical areas and even remote areas that are hundreds of kilometers away from the main monitoring and control station, where they do not work Radio waves in these large distances, but the work is through satellite technology [28], which is characterized by the strength of the signal and the lack of interruptions, the locations of self-driving vehicles are determined on the ground

through the data collected from the various technologies attached to the vehicle such as the compass, the speed measuring device, radar devices, and determining Devices Satellite Locations (GPS).

To coordinate and control teamwork between self-driving vehicles in terms of communication and task planning, coordination between them is done in two ways (Figure 1). The first one is the central method, where the group is controlled by one party. The main advantage of this method is speed and the minimum network traffic. However, it has many defects, the most important of which is the failure of the controller. The second is decentralized with the interaction between the vehicles depending on the communication between them, where education is the basis of work between the vehicles on several levels to achieve clear goals such as exchanging information, sharing tasks, and collective decision-making. It can adapt to its environment safely, and the whole group is able to manage the task of monitoring a large area more quickly and efficiently, even in the absence of direct communication with the central station.

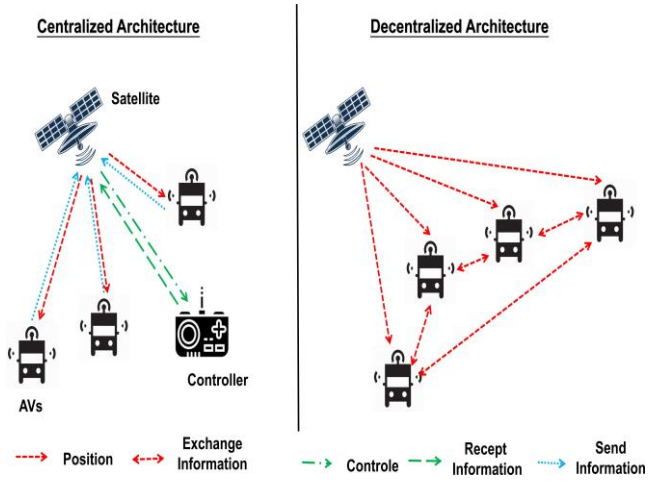

Figure 1. Centralized and decentralized architectures.

Through our proposed model, we combined the central and decentralized methods, where we define a leader for the group, the leader will determine his location using positioning via GPS satellites, and the rest of the team members are determined based on the information sent from the leader, where all the team is linked by radio waves to A special communication vehicle road in the middle in case of large distances.

The rest of the paper is organized as follows: Section 2 discusses security risks and spoofing attacks on AVs; the section treats two points, some related works, and secure data exchange. Section 3 presents the proposed architecture. Section 4 explains how the proposal secures AVs communication. In section 5, we show the secure collection of data at the cloud level. Section 6 discusses the performance of our approach. Lastly, the paper presents the conclusion and future work in section 7.

2. Security Technology in AVs: Addressing Security Risks and Spoofing Attacks

The field of AVs systems technology is rapidly advancing within the realm of the Internet of Things. AVs are being increasingly utilized in all sectors for various goals, including recreational, commercial, and military applications [23]. However, with the increased adoption of AVs comes an escalation in associated risks, particularly in terms of security. The potential compromise of sensitive data, such as photos, videos, GPS locations, and other private information, poses a significant threat as these become prime targets for hackers. The ability to remotely control AVs opens up avenues for electronic attacks, including denial of service and unauthorized takeover. If this part is not adequately addressed, it could lead to the potential exploitation of commercially available and widely used vehicles.

This work aims to address these challenges, primarily focusing on two key aspects. The first part centers on establishing secure communication between vehicles. While this aspect will not be extensively covered in this discussion, as it typically relies on encryption methods for exchanging information between peers, it remains a crucial component of AV security. The second part, which holds significant importance, revolves around mitigating spoofing attacks (Figure 2). In this regard, we will explore various studies and contributions found in the existing literature.

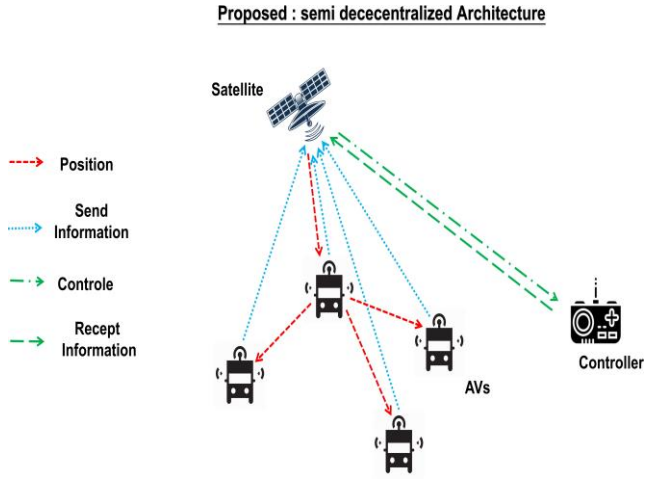

Figure 2. Proposed semi-decentralized architecture for measurement of position.

2.1. Related Work

Cui *et al.* [7] provided a comprehensive review of current research on safety failures and security attacks in AVs, along with an examination of the existing safety and security countermeasures. Nanda *et al.* [24] presented the communication layers of self-driving vehicles, their characteristics, and potential security risks are the main topics of this article. They also gave a summary of the recent research developments and future

research challenges in this field. Xu *et al*. [29] talked about how ultrasonic sensors, which are widely used for obstacle detection in AVs, can be attacked by spoofing or jamming their signals. The attacks can cause the vehicles to stop or fail to stop when they should not, resulting in accidents. The work also proposed two defense strategies based on physical shift authentication [19] and multiple sensor consistency checks to improve the security and synchronization [14] of ultrasonic sensors and AVs.

Dutta *et al*. [12] showed that safety and security are important design goals for automotive systems, particularly in the event of electronic attacks or sensors that could compromise the operation of the vehicle. The work introduced the concept of Security for Safety's sake and presented a system-level security solution that combined a modified Kalman filter and a chi-square detector to detect and mitigate sensor attacks while maintaining integrity constraints which consists of a modified Kalman filter and a Chi-squared detector. The work demonstrated the effectiveness of the proposed solution by studying a vehicle tracking case where the slave vehicle has an adaptive cruise control unit.

Cui *et al*. [8] work was about proposing a framework for analyzing both safety and security issues in AVs, which combines an integrated Safety and Security (S-S) method with ISO 26262 and SAE J3061 standards. The work demonstrated the framework application to a typical autonomous vehicle model and how it can help identify and address vulnerabilities that affect vehicle safety and security. Almeaibed *et al*. [3] discussed the digital transformation and digital twins that enable more intelligent and autonomous systems for smart manufacturing transportation but also pose new challenges and solutions for safety and security functions.

Chen *et al*. [6] proposed a novel method for anomaly detection and mitigation against GPS attacks, utilizing onboard cameras and high-precision maps to ensure accurate vehicle localization. Initially, lateral direction localization within driving lanes is determined through both camera-based lane detection and map matching. Subsequently, a real-time detector for GPS spoofing attacks is developed to evaluate the localization data. Upon detecting an attack, a multi-source fusion-based localization method employing an unscented Kalman Filter is implemented to mitigate the GPS attack and enhance localization accuracy.

Abrar *et al*. [1] introduced a GPS Intrusion Detection System (GPS-IDS), an Anomaly Behavior Analysis (ABA)-based framework designed to detect GPS spoofing attacks on AVs. The framework incorporated a novel physics-based vehicle behavior model, integrating a GPS navigation model into the conventional dynamic bicycle model for precise AV behavior representation. Temporal features derived from this behavior model are analyzed using Machine Learning (ML) to identify normal and abnormal navigation behavior.

Shabbir *et al*. [26] described a novel approach using Deep Learning (DL) algorithms, such as Convolutional Neural Networks (CNN), and ML algorithms to protect CAVs from GPS location spoofing attacks. Their work was validated using real-time simulations in the CARLA simulator, utilizing training and test data that included GPS coordinates, fake coordinates, and positioning algorithm values.

Dasgupta *et al*. [9] presented a system and research method for developing a covert spoofing attack against AVs. They explored the relationship between the original pseudo-range and the manipulated pseudo-range to establish an efficient defense. The gradual divergence from the genuine route further conceals the attack and impedes swift detection.

To address the drawbacks illustrated in Table 1, we introduced a new encryption and consensus based technique defense.

Table 1. Disadvantages of some proposed works in literature.

Work	Drawback
[7]	Proposed for particular use
[11]	Needs of an onboard camera and high-precision map
[12]	Physics-based vehicle behavior which implies additional processing time
[13]	Machine and deep learning algorithms are still slow
[14]	Time complexity equals $O(n^2)$

2.2. Securing Data Exchange in AVs

Several positioning systems are available, including two systems for Global Navigation Satellite Systems abbreviated by (GNSS), the first is United States (GPS) and the second is GLONASS (Russia). We can cite two other systems, the first is European Galileo System and the other is Chinese Beidou-2 System, they are in the development of becoming global. Most general designs for all GNSS variants are quite similar. The weakest point is the GPS receiver for AVs, which rely on unencrypted civilian GPS.

But in military GPS signals that keep the used key secret, unlike civilian GPS signals that are not coded or authenticated. The signals are broadcast using known spread symbols. In AV equipment, the receiver cannot distinguish the spoofed signal from the original signal. Dasgupta *et al*. [11], focused on the vulnerabilities of GNSS used by AVs and proposed a prediction-based spoofing attack detection strategy. GNSS, which provides Positioning, Navigation, and Timing (PNT) services, is susceptible to spoofing attacks due to factors like lack of encryption and open-access codes.

The study utilizes a recurrent neural network model called the Long Short-Term Memory (LSTM) model. Alheeti *et al*. [2] discussed the importance of detecting 3D objects for AVs to drive safely and responsibly. AVs use LiDAR sensors to detect objects quickly and accurately in various conditions. However, LiDAR sensors may face spoofing attacks via laser satirizing, which can mislead AVs by providing false information. To protect AVs from such attacks, the paper proposes a model utilizing ML (i.e., decision trees) that can detect

LiDAR spoofing attacks. Komissarov *et al*. [22], the authors presented a system to attack FMCW mmWave radar in automotive applications. Using a single rogue radar, it spoofs distance and velocity measurements simultaneously, creating coherent phantom measurements.

A proof-of-concept hardware-based system is built and two real-world scenarios are demonstrated successfully. Countermeasures to mitigate the described attack are also discussed. Paper Dasgupta *et al*. [10] developed a deep RL-based method for detecting turn-by-turn spoofing attacks in AVs using low-cost in-vehicle sensor data. The proposed method aims to ensure a resilient PNT system for AV navigation even in the presence of compromised GNSS signals.

3. The Proposed Model

Identifying a secure method for measuring position is a complex challenge. The proposed approach (Figure 3) involves relying on the GPS position of a designated team member, referred to as the leader. Before transmission, the leader has to encrypt its position and shares it with all other members through a wireless network. Each receiving vehicle forwards the leader's position to other connected vehicles, excluding the sender. Upon receiving the information, the recipient vehicle decrypts it to obtain the leader's position. Using the leader's position and additional data such as radio signal propagation time, each vehicle calculates its own current position. A consensus process is employed to select a new leader for a specified time interval (e.g., ten seconds). This interval, denoted as *Tc*, depends on factors like connection quality, communication speed, and task importance. The leader has to be related to at least one vehicle to transmit its position. If it fails to transmit a position signal, an additional short period is granted, after which a new leader is selected by the team. If one vehicle loses connection with others, it resorts to GPS to determine its position while attempting to establish communication with the group periodically.

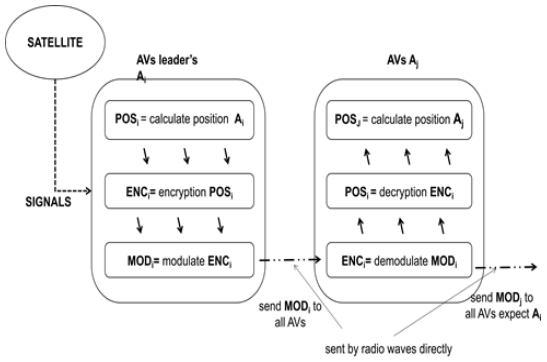

Figure 3. The general phases in our approach.

Algorithm 1: Get Position

Require: Tc: time period of a consensus, Pr: period of reception
Ensure: my position
1: function Get Pos
2: $p_1 \leftarrow 0$ ▷ p_1 : denotes period 1
3: while (p_1 < Tc)
4: increment p_1
5: end while
6: consensus()
7: $p_1 \leftarrow 0$
8: if 'I am the leader' then
9: each Pr of time
10: Pn ← calculate position (GPS info)
11: En ← encrypt (Pn)
12: Md ← modulate (En)
13: send (Md) to all connected vehicles
14: else ▷ means that I am not a leader
15: each Pr of time
16: receive (Md) ▷ from other members of the group
17: send (Md) to other connected vehicles, except me
18: En ← demodulate (Md)
19: Pn_leader ← decrypt(En)
20: Pn_my ← compute position (Pn_leader and AF) ▷ AF: additional (other) information such as the signal propagation
21: end if
22: return my position
23: end function

When executing Algorithm (1), the vehicle needs two periods of time *Tc* and *Pr*, and the variable p_1 must be initialized by 0. Each *Tc* of time, the group performs a new consensus in order to select a new leader. After the consensus process, the variable p_1 takes the value 0. During this period (between Tc_i and Tc_{i+1}), the leader has to compute its position each *Pr* of time using GPS info as shown in the line 10. Then he broadcasts it as a ciphertext (line 13). If the vehicle is not a leader, we will go to line 14. The vehicle must receive position info from the leader in each *Pr*, decrypt it, and exploit it The vehicle must receive position info from the leader in each *Pr*, decrypt it, and exploit it to determine safely its own position ((Algorithm 1), lines 16-20).

3.1. Consensus Algorithm

A consensus algorithm is a process in computer science employed to reach an agreement on a single data value among many distributed users. These algorithms are developed to attain reliability in a network involving multiple users or nodes. As they solve a consensus concern, consensus algorithms consider some participants will be unavailable and that only a portion of the nodes will reply. They also consider some communications will be lost during the transmission. There are various consensus algorithms available for selecting a leader, but we need to utilize lightweight algorithms to conserve energy in autonomous vehicle environments [3].

Algorithm 2: Do Consensus

Require: Nv: # of vehicles, p: prime number,
Ensure: who is the leader
function Do Cons
generate random value v_i
generate sk_i
$c_{1i} \leftarrow v_i \times sk_i \mod p$

$c_{2i} \leftarrow sk^{sk} \mod p$
broadcast (c_{1i}, c_{2i})
while (number of received $c_j < Nv$*)*
receive (c_{1j}, c_{2j})
end while
broadcast sk_i
while (number of received $sk_j < Nv$*)*
receive sk_j
end while
$d_i \leftarrow$ *decrypt* (c_{1i}) *using* (sk_i), ▷ *all* c_{1i}
$v \leftarrow Sum(d_i) \mod (Nv+1)$
select the new leader by using the value v
return leader
end function

To ensure the exclusion of external parties from the consensus process, we employ a technique involving two phases (Algorithm 2). The first one involves the "creation of a list of encrypted values", where each vehicle V_i generates a random temporary number v_i and a random temporary secret key sk_i. With each consensus operation, a new pair (v_i , sk_i) is created by everyone in the team. The value v_i is then encrypted using the corresponding sk_i according to Equation (1). (1)

$$c1i = vi \times ski \mod p$$

Equation (1) involves a secret prime number p, and the condition is set such that $0 < v_i < p$. This condition is put in place to ensure the correct retrieval of each v_i later. Because if v_i is greater than p, then the initial value of v_i cannot be recalculated. Equation (1) shows at the same time lightweight and hard encryption because both values v_i and sk_i are unknown. The purpose of encrypting the generated v_i is to prevent any malicious AVs from influencing the outcome of the selection algorithm. To enhance the robustness of the process because each vehicle can modify the secret key sk_i or manipulate the selection value in order to be a leader, we introduced another parameter c_{2i} computed by Equation (2). Besides c_{1i}, each AVs must share c_{2i}.

$$c2i = skiski \mod p \quad (2)$$

Once the encrypted list is created i.e., all c_{1i} and c_{2i} are broadcast, AVs can start the second step, known as the selection process. In this step, each vehicle V_i has to share its secret key sk_i with the other vehicles in the team. Using these shared keys, each vehicle can calculate all other v_i values by decrypting the c_{1i} values using the shared secret keys sk_i as shown in Equation (3).

$$vi = c1i \times sk - 1 \mod p \quad (3)$$

where sk_i^{-1} denotes the multiplicative inverse of sk_i which shows in Equation (4):

$$ski \times ski - 1 \mod p = 1. \quad (4)$$

After getting all v_i values, all vehicles can calculate the same value v based on the following Equation (5):

$$v = (\Sigma\, i = 1, N\, vi) \mod N + 1 \quad (5)$$

where N denotes the vehicle's total number. The last operation at this stage is to identify the leader. Upon computing v the sum of all v_i (mod N + 1), the rest is very simple; the leader is the vehicle whose v_i is the closest to v.

We note here that no adversary can impersonate any vehicle or join the group and participate in the consensus process for the purpose of being the leader and then mislead the team by providing them with false positions. How is that? the adversary can easily produce a pair (c_{1a} , c_{2a}), but since the number p is secret, he will use another number, let it be p_a, so he will compute $c_{2a} = sk_a^{ska} \mod p_a$. After revealing its secret key sk_a, each member of the team will check the value c_{2i} and we will definitely get the following Equation (6):

$$c2a = skaska \mod pa \neq c'2a = skaska \mod p \quad (6)$$

The team will then discover that this is a false value even with a forged signature [20], and not enter it into the calculation, so waiting for the correct value to arrive.

4. Securing AVs Communication

In Figure 4, it is evident that vehicle 3 falls within the control zone of the adversary, which represents the range affected by the jamming signal used to spoof the signal of GPS. However, the adversary is unaware that vehicle 3 does not rely on GPS for positioning, but rather computes its position using the leader's location, which lies outside the jamming zone. Consequently, vehicle 3 remains unaffected by the interference signal. It is important to note that the adversary cannot control the whole (entire) area where the AV group is situated. To mitigate the impact of a large jamming range, team members must maintain a safe distance between them, ensuring that the two farthest vehicles are beyond the attacker's range. This guarantees that at least only one vehicle remains outside the jamming area. When some team members are under the attacker's control, the rest of the team will adjust their positions based on the vehicle that is outside the danger zone. To enhance signal robustness during radio transmission modulation and prevent attacks, the leader's position transmitted from vehicle 3 to vehicle 4 is encrypted. This operation of encryption serves to safeguard against interference, as well as protect against distance enlargement attacks as well as against distance reduction attacks from both internal or external threats.

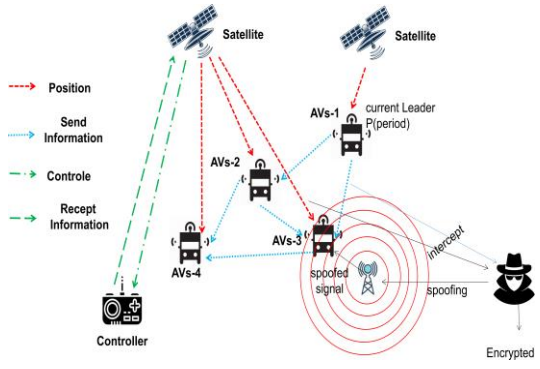

Figure 4. Secure position demonstration in our proposal.

5. Secure Data Collection and Processing

To leverage modern technologies like Internet of Things (IoT) and emerging cloud computing, data collection can be achieved through the utilization of AVs. For instance, individual vehicles can calculate specific information values within their designated areas. These values are then encrypted using an additive scheme [18] before being transmitted to the cloud for storage. Once the encrypted data is received by the cloud server, it can conduct operations on them by utilizing homomorphic encryption [21]. In our model, the additive technique allows the cloud to make the addition operations on received data from individual vehicles, even if they originate from different locations or were collected at different moments. The additive technique adheres to the equation verification Equation (7):

$$Dec(Enc(v) + Enc(v')) = v + v' \quad (7)$$

By employing homomorphic addition, the cloud has the capability to perform computations on encrypted corporate data without getting the original values. As a result, the privacy of the data owner who utilizes the cloud is preserved. The owner is able to subsequently retrieve the data content after decrypting them using its secret key. The purpose of the scheme is to conceal the data splitting them at random into two components, v_1 and v_2, such that $v = v_1 + v_2$. This fragmentation makes it challenging for an attacker to determine either v_1 or v_2 individually. Consequently, the proposed encryption can be represented the following Equation (8):

$$c = (v1 + v2 \times sk + r \times p) \ mod \ pk \quad (8)$$

In this scheme, the symbol *sk* represents the private key, r is a randomly generated number, p is a prime number, and *pk* denotes a public key. This approach ensures the security of information during its transmission to the cloud, preventing hacking attempts, as well as safeguarding it from access by the calculation provider within the cloud. Additionally, the encryption technique enables the performance of additional operations on cipher data without requiring decryption. This technique is classified as a lightweight scheme in comparison to other existing approaches mentioned in the literature [17], indicating its suitability for the Unmanned Aerial Vehicle (UAV) environment.

6. Preferences

In this Section, we will show two points, network traffic and algorithm complexity.

6.1. Network Traffic and Scalability

Network traffic refers to the data packets exchanged between devices connected to a network. It includes all digital communications flowing over the network, such as file transfers and more. Understanding network traffic is of utmost importance as it contributes to improving network performance by monitoring and analyzing network traffic to identify bottlenecks, congestion points, and potential areas for improvement. By optimizing network performance, businesses and individuals can ensure faster and more reliable data transmission, reduce latency, and enhance the user experience [25].

Moreover, network traffic analysis plays a crucial role in ensuring security and detecting potential threats. By monitoring abnormal patterns or suspicious activities, security professionals can quickly identify potential cyberattacks, malware, or unauthorized access attempts, allowing them to respond promptly to safeguard the network [14]. Network traffic analysis is an integral part of maintaining a stable, secure, and efficient network infrastructure. A comprehensive understanding of data flow enables informed decision-making, improved performance, enhanced security measures, and an overall enhancement of the user experience [13]. To know how data is transmitted within the network, let us have a group of AVs equipped with sensors and communication modules. They communicate with each other V2V and with a central traffic management system V2C. Vehicles transmit sensor data, and location updates, communicate with each other, and receive commands from the central system [15].

To calculate the transmitted data in our approach, we take into account some values; each vehicle transmits sensor data (such as LiDAR and camera) every *Ts* (send-Time), site updates are sent every P (period), site update package size: sus(site-update-size).

We put *n* denotes the number of vehicles, with regard to determining the location, a consensus algorithm is executed to determine the leader, $n \times (n-1)$ messages will be sent to share (c_1, c_2), and then the same number of messages to share the secret keys, finally, the same number to confirm the gotten result (leader). After that, the leader sends his location to all vehicles, through which the locations of the vehicle paths are determined. Therefore, *n-1* messages will be sent from the leader to the rest of the vehicles each period of updating position time. Thus, the total traffic can be shown by Equation (9).

$$sus = 3 \times (n \times (n - 1)) \quad (9)$$

Regarding scalability, the proposed protocol is effective because it relies only on linear encryption and lightweight arithmetic operations. Of course, this is not an absolute statement, but rather a proportion must be established between the number of AVs and the period to conduct a consensus. As we have seen, every consensus process needs $3\times(n\times(n-1))$ messages, so increasing the number of AVs will inevitably affect the traffic. This proportion is determined by calculating the probability of losing a single message, as this probability increases by increasing the number of AVs, thus increasing the probability of failure of the consensus process. Determining the percentage of the probability of losing a single message needs a field test, which we

intend to do in future work.

The proposed model is based on consensus, which is carried out by exchanging messages encrypted with a secret key *p*. There are two basic rounds to complete the consensus process, sharing (c_1, c_2) and sharing *sk*; then a third round in order to confirm the result obtained, which gives us three rounds with $3\times(n\times(n\text{-}1))$ exchanged messages. In each round, each vehicle must receive n-1 messages where n denotes the number of team members. If this is not done due to environmental factors, this round will be repeated again, which could delay the consensus process, and consequently the updating position process.

6.2. Algorithms Complexity

Algorithm complexity refers to the analysis of how the efficiency of an algorithm changes as the input size increases. It quantifies the amount of time and resources an algorithm requires to solve a problem, helping us understand its scalability and performance characteristics [4]. The importance of algorithm complexity lies in its role in guiding the selection of the most efficient algorithms for specific tasks. By comparing and evaluating different algorithms based on their complexity, we can make informed decisions to optimize computational processes, reduce execution time, and conserve valuable resources.

Understanding algorithm complexity is crucial in the design and optimization of software and systems. It enables developers and engineers to strike a balance between computational power and practicality, ensuring that applications can handle large-scale data and real-time demands efficiently. In summary, algorithm complexity provides valuable insights into the efficiency of algorithms, enabling us to build faster, more responsive, and resource-efficient solutions that meet the demands of modern computing environments [4].

In our proposal, we have two algorithms, one for positioning and the other for leader selection. In the first algorithm, we have elementary instructions which give us $O(1)$. In the second algorithm, there are two 'while' loops, sending (c_1, c_2) and sending sk. Therefore, the complexity of the second algorithm equals $O(n)$. Thus the final complexity of the proposal is shown by the following Equation (10):

$$C = O(n)$$

Table 2. Execution time comparison, with 10 AVs, * denotes that each arithmetic operation is estimated by 0.001 s, and LSTM for Long Short-Term Memo.

work	Delay (s)
[6], 2023	0.2 (LSTM Algorithm)
[26], 2023	1 (DNN, CNN)
[9], 2024	0.4 (*)
Ours	0.13 (*)

Table 2 shows that the time complexity is reduced in our proposed model.

7. Conclusions

In this paper, we present a new approach to address the problem of GPS spoofing attacks for AVs, which constitutes one of the major challenges to the advancement and adoption of AVs and their operation and widespread adoption. Through the study and analysis, we noticed that the current solutions are either complex in implementation, ineffective, or restricted by environmental restrictions. Therefore, in our proposed method, we presented solutions through which the attacker cannot influence the vehicles unless he has control over the entire group of vehicles. The process of Jamming requires all team members to be within the attacker's jamming zone, which is a hard process to implement. We presented the performance of our proposal by illustrating two aspects which are traffic network and algorithm complexity.

In the future, we plan to perform field tests of our protocol to show real results against GPS attacks namely spoofing. Furthermore, we aim to empirically evaluate the timing of our scheme in terms of delay and thus evaluate the feasibility and practicality of this method.

References

[1] Abrar M., Islam R., Satam S., Shao S., and Hariri, S., "GPS-IDS: An Anomaly-based GPS Spoofing Attack Detection Framework for Autonomous Vehicles," *arXiv Preprint*, vol. arXiv:2405.08359, 2024. https://doi.org/10.48550/arXiv.2405.08359

[2] Alheeti K., Alzahrani A., and Al-Dosary D., "LiDAR Spoofing Attack Detection in Autonomous Vehicles," *in Proceedings of the IEEE International Conference on Consumer Electronics*, Las Vegas, pp. 1-2, 2022. Doi:10.1109/ICCE53296.2022.9730540

[3] Almeaibed S., Al-Rubaye S., Tsourdos A., and Avdelidis N., "Digital Twin Analysis to Promote Safety and Security in Autonomous Vehicles," *IEEE Communications Standards Magazine*, vol. 5, no. 1, pp. 40-46, 2021. DOI:10.1109/MCOMSTD.011.2100004

[4] Belin A., Myers R., Ruan S., S´arosi G., and Speranza A., "Complexity Equals Anything II," *Journal of High Energy Physics*, vol. 1, no. 154, pp. 1-79, 2023. https://doi.org/10.1007/JHEP01(2023)154

[5] Chen L., Wu P., Chitta K., Jaeger B., and Geiger A., "End-to-End Autonomous Driving: Challenges and Frontiers," *arXiv Preprint*, vol. arXiv:2306.16927, 2023. https://doi.org/10.48550/arXiv.2306.16927

[6] Chen Q., Liu P., Li G., and Wang Z., "GPS Attack Detection and Mitigation for Safe Autonomous Driving Using Image and Map-based Lateral Direction Localization," *arXiv Preprint*, vol. arXiv:2310.05407, 2023.

https://doi.org/10.48550/arXiv.2310.05407

[7] Cui J., Liew L., Sabaliauskaite G., and Zhou F., "A Review on Safety Failures, Security Attacks, and Available Countermeasures for Autonomous Vehicles," *Ad Hoc Networks*, vol. 90, pp. 101823, 2019. https://doi.org/10.1016/j.adhoc.2018.12.006

[8] Cui J., Sabaliauskaite G., Liew L., Zhou F., and Zhang B., "Collaborative Analysis Framework of Safety and Security for Autonomous Vehicles," *IEEE Access*, vol. 7, pp. 148672-148683, 2019. DOI:10.1109/ACCESS.2019.2946632

[9] Dasgupta S., Ahmed A., Rahman M., and Bandi T., "Unveiling the Stealthy Threat: Analyzing Slow Drift GPS Spoofing Attacks for Autonomous Vehicles in Urban Environments and Enabling the Resilience," *arXiv Preprint*, arXiv:2401.01394, 2024. https://doi.org/10.48550/arXiv.2401.01394

[10] Dasgupta S., Ghosh T., and Rahman M. "A Reinforcement Learning Approach for Global Navigation Satellite System Spoofing Attack Detection in Autonomous Vehicles," *Journal of the Transportation Research Board*, vol. 2676, no. 12, pp. 318-330, 2022. https://doi.org/10.1177/03611981221095509

[11] Dasgupta S., Rahman M., Islam M., and Chowdhury M., "Prediction-based GNSS Spoofing Attack Detection for Autonomous Vehicles," *arXiv Preprint*, vol. arXiv:2010.11722, 2020. https://doi.org/10.48550/arXiv.2010.11722

[12] Dutta R., Yu F., Zhang T., Hu Y., and Jin Y., "Security for Safety: A Path Toward Building Trusted Autonomous Vehicles," *in Proceedings of the IEEE/ACM International Conference on Computer-Aided Design*, San Diego, pp. 1-6, 2018. DOI:10.1145/3240765.3243496

[13] Gu Z., Wang Z., Liu Z., and Saberi M., "Network Traffic Instability with Automated Driving and Cooperative Merging," *Transportation Research Part C: Emerging Technologies*, vol. 138, pp. 103626, 2022. https://doi.org/10.1016/j.trc.2022.103626

[14] Habib A., Laouid A., and Kara M., "Secure Consensus Clock Synchronization in Wireless Sensor Networks," *in Proceedings of the International Conference on Artificial Intelligence for Cyber Security Systems and Privacy*, El Oued, pp. 1-6, 2021. DOI:10.1109/AI-CSP52968.2021.9671225

[15] Han H., Yan Z., Jing X., and Pedrycz W., "Applications of Sketches in Network Traffic Measurement: A Survey," *Information Fusion*, vol. 82, pp. 58-85, 2022. https://doi.org/10.1016/j.inffus.2021.12.007

[16] Hazmy I., Hawbani A., Wang X., Al-Dubai A., and Ghannami A., "Potential of Satellite-Airborne Sensing Technologies for Agriculture 4.0 and Climate-Resilient: A Review," *IEEE Sensors Journal*, vol. 24, no. 4, pp. 4161-4180, 2023. DOI:10.1109/JSEN.2023.3343428

[17] Hidalgo C., "Economic Complexity Theory and Applications," *Nature Reviews Physics*, vol. 3, no. 2, pp. 92-113, 2021. https://doi.org/10.1038/s42254-020-00275-1

[18] Kara M., Karampidis K., Papadourakis G., Laouid A., and AlShaikh M., "A Probabilistic Public-Key Encryption with Ensuring Data Integrity in Cloud Computing," *in Proceedings of the International Conference on Control, Artificial Intelligence, Robotics and Optimization*, Crete, pp. 59-66, 2023. DOI:10.1109/ICCAIRO58903.2023.00017

[19] Kara M., Karampidis K., Sayah Z., Laouid A., and Papadourakis G., "A Password-Based Mutual Authentication Protocol via Zero-Knowledge Proof Solution," *in Proceedings of the International Conference on Applied CyberSecurity*, Dubai, pp. 31-40, 2023.

[20] Kara M., Laouid A., and Hammoudeh M., "An Efficient Multi-Signature Scheme for Blockchain," *Cryptology ePrint Archive*, 2023. https://eprint.iacr.org/2023/078

[21] Kara M., Laouid A., Hammoudeh M., and Bounceur A., "One-Digit Checksum for Data Integrity Verification of Cloud-Executed Homomorphic Encryption Operations," *Cryptology ePrint Archive*, 2023.

[22] Komissarov R. and Wool A., "Spoofing Attacks Against Vehicular FMCW Radar," *in Proceedings of the 5th Workshop on Attacks and Solutions in Hardware Security*, New York, pp. 91-97, 2021. https://doi.org/10.1145/3474376.3487283

[23] Lee S., "Opinions of Active Transportation Users on Policies to Ensure their perceived safety in the Era of Autonomous Vehicles," *Case Studies on Transport Policy*, vol. 12, pp. 101002, 2023. https://doi.org/10.1016/j.cstp.2023.101002

[24] Nanda A., Puthal D., Rodrigues J., and Kozlov S., "Internet of Autonomous Vehicles Communications Security: Overview, Issues, and Directions," *IEEE Wireless Communications*, vol. 26, no. 4, pp. 60-65, 2019. DOI:10.1109/MWC.2019.1800503

[25] Papadogiannaki E. and Ioannidis S., "A Survey on Encrypted Network Traffic Analysis Applications, Techniques, and Countermeasures," *ACM Computing Surveys*, vol. 54, no. 6, pp. 1-35, 2021. https://doi.org/10.1145/3457904

[26] Shabbir M., Kamal M., Ullah Z. and Khan M., "Securing Autonomous Vehicles Against GPS Spoofing Attacks: A Deep Learning Approach," *IEEE Access*, vol. 11, pp. 105513-105526, 2023. DOI:10.1109/ACCESS.2023.3319514

[27] Xiong S., Li B., Zhu S., Cui D., and Song X., "Spatial Pyramid Pooling and Adaptively Feature Fusion based Yolov3 for Traffic Sign Detection," *The International Arab Journal of Information*

Technology, vol. 20, no. 4, pp. 592-599, 2023. DOI:10.34028/iajit/20/4/5

[28] Wiseman Y., *Autonomous Vehicles*, IGI Global, 2022. DOI:10.4018/978-1-6684-3694-3.ch043

[29] Xu W., Yan C., Jia W., Ji X., and Liu J., "Analyzing and Enhancing the Security of Ultrasonic Sensors for Autonomous Vehicles," *IEEE Internet of Things Journal*, vol. 5, no. 6, pp. 5015-5029, 2018. DOI:10.1109/JIOT.2018.2867917

Laid Kenioua received a state engineer's degree in computer science, specializing in advanced information systems, from the University of M'sila, Algeria, 2006, then obtained a Master's degree in Artificial Intelligence from the University of El Oued, Algeria, 2016. He is a candidate for a Doctorate in Artificial Intelligence from the University of El Oued, Algeria, interested in Big Data Analysis, Advanced Computing, And Machine Learning.

Brahim Lejdel is currently a full Professor at the Faculty of Exact Sciences, University of El Oued, Algeria. He obtained his Magister Degree in Computer Science from the University of Ouargla in 2009, and completed his Ph.D. in Computer Science in 2015. Dr. Lejdel has authored over 120 articles published in refereed journals and international conferences, and has authored more than 10 books within his research domain. He serves as the chair of numerous international conferences and contributes as an invited editor and reviewer for various journals and conferences. Dr. Brahim Lejdel supervises several students pursuing degrees in Computer Science at the undergraduate, master's, and doctoral levels.

Mohamed Abdelhamid Nedioui is an associate Professor in the Faculty of Exact Sciences, University of EL-Oued (Algeria). He has held a Magister Degree in Computer Science from University of Biskra since 2015. He held his Ph.D. in Computer Science in 2021.