JAUES

Journal of Al-Azhar University Engineering Sector

Vol.16, No. 61, October, 2021,1184-1198

# VANET Applications Vulnerability and Attacks Detection and Avoidance

**Manal S. Gamal [1], Abdurrahman A. Nasr [2], Sayed A. Nouh [2]**

[1]Department of Electrical Engineering, Faculty of Engineering, 6th of October University, Giza, Egypt
[2]Department of Computers and Systems Engineering, Faculty of Engineering, Al-Azhar University, Cairo, Egypt

* Corresponding Authors' Email: Manal.shehab@gmail.com

## ABSTRACT

Vehicular ad-hoc network (VANET) are designed to aid in avoiding many of the traffic problems, such as accidents, traffic jams, traffic status broadcast, etc. This article proposes two possible configurations as VANET applications to aid in solving two traffic issues namely, parking, and after-accident management. These two models of VANET are designed with the objective of improving traffic fluidity.
However, VANETs are special types of Mobile Ad Hoc Networks (MANETs) with moving nodes (Vehicles) and stand still nodes Roadside Units (RSUs). Likewise, all MANETs. The network nodes can move freely within the network coverage yet stay connected. Therefore, VANETS are subject to vulnerable attacks. Sybil attacks are the most threatening VANET attacks that may lead to death.
Therefore, this article proposes a three-stage technique for detection, prevention, and avoidance of Sybil attacks. It also presents a methodology for analyzing the algorithms of VANET applications to identify predictive security holes and hence suggests a method for closing these threatening gaps, which are exemplified on the two sample applications for explanation.

**KEYWORDS:** Vehicular ad-hoc networks; VANETs Applications; VANETs Security; VANETs Sybil Avoidance; VANETs Sybil Attacks.

## تطبيقات على الشبكات اللاسلكية للمركبات لكشف الهجمات وتجنبها

**منال س. جمال[1]، عبد الرحمان أ. نصر[2] ، سيد أ. نوح[2]**

[1] قسم الهندسة الكهربيه - كلية الهندسه - جامعة 6 أكتوبر – الجيزة – جمهورية مصر العربية
[2] قسم الهندسة النظم و الحاسبات - كلية الهندسه - جامعة عين شمس – القاهرة – جمهورية مصر العربية

*البريد *الالكتروني للباحث الرئيسي:* Manal.shehab@gmail.com

**الملخص**

تم تصميم شبكة المركبات المخصصة الشبكات اللاسلكية للمركبات للمساعدة في تجنب العديد من مشاكل المرور ، مثل الحوادث والاختناقات المرورية ومتابعة حالة حركة المرور وما إلى ذلك. تقترح هذه المقالة تكوينين محتملين كتطبيقات الشبكات اللاسلكية للمركبات للمساعدة في حل مشكلتان مروريتان وهما: ، وقوف السيارات ، وإدارة ما بعد الحوادث. حيث تم تصميم هذين النموذجين من VANET بهدف تحسين سيولة حركة المرور.

ومع ذلك ، فإن الشبكات اللاسلكية للمركبات هي أنواع خاصة من شبكات Mobile Ad Hoc (MANETs) مع عقد متحركة (مركبات) وعقد ثابتة على جانب الطريق (RSUs) . وبالمثل ، كل .MANETs يمكن لعقد الشبكة التحرك بحرية داخل تغطية الشبكة مع البقاء على اتصال. لذلك ، تتعرض الشبكات اللاسلكية للمركبات لهجمات ضعيفة. هجمات Sybil هي أكثر هجمات الشبكات اللاسلكية للمركبات تهديدًا والتي قد تؤدي إلى حدوث كوارث.

لذلك ، تقترح هذه المقالة تقنية من ثلاث مراحل لاكتشاف ومنع وتجنب هجمات .Sybil كما يقدم منهجية لتحليل خوارزميات تطبيقات الشبكات اللاسلكية للمركبات لتحديد الثغرات الأمنية التنبؤية ومن ثم يقترح طريقة لسد هذه الفجوات المهددة ، والتي تم تمثيلها في نموذجي التطبيقات للتفسير.

**الكلمات المفتاحية:** الشبكات اللاسلكية للمركبات، تطبيقات الشبكات اللاسلكية للمركبات، تأمين الشبكات اللاسلكية للمركبات، تجنب هجمات Sybil، هجمات Sybil علي الشبكات اللاسلكية للمركبات.

## 1. INTRODUCTION

VANET is the most popular real-life paradigm of ad hoc networks in which the nodes are mostly moving vehicles. VANET networks' main goals are of ensuring road safety and enhancing drivers' comfort, among other goals. Therefore, there are wide ranges of applications that can be designed for VANETs (Sheikh & Liang, 2019). This research is concerned only with two application categories, namely:

- **Convenience applications**: Examples are: navigation, personal routing, congestion advice, toll collection, parking availability information, etc., and
- **Safety applications**: Examples are: road control in case of accidents, crash notification, traffic violation warnings, curve speed warnings, emergency electronics brake light, pre-crash sensing, etc.

This article presents two sample applications, one from each of these two categories, namely, finding an empty Parking slot and After-Accident rescue management applications. The algorithms of the two applications are presented as demonstrations of how VANETs can play a role in resolving real life traffic problems to encourage the authorities to follow. The former application tries to solve a problem that almost all capitals worldwide are suffering from, while the latter application is intended to give a scenario demonstrating how VANETs can minimize the damages due to road accidents via the cooperation between all stakeholders involved in after-accident rescue operations, such as firetrucks, ambulance, police patrols, etc. Moreover, the former application is triggered by a vehicle's request, while the latter is initiated by an informative message; two different messaging perspectives to serve the remainder scope of the article. Those applications are discussed, and their algorithms are proposed.

Noteworthy, VANETs deal with real time information through the communication between moving nodes (Vehicles) and stand still nodes (Roadside Units—RSUs) that exchange significant messages, such as road accident warnings, traffic jam alerts, or even asking for traffic information. Therefore, they are at risk of various types of attacks to misbehave the network and cause road disasters. Sybil attacks (Newsome et al., 2004) are the most harmful types of VANET attacks.

Sybil attacks are special types of attacks that emerged only for VANETs the ad hoc networks of moving vehicles. Sybil attackers not only pretend the identity of other nodes of the network but also replicate them and create multiple faked identities to falsify the traffic scenarios. Consequently, every generated attack is played after spoofing either the position or the identity of other nodes in the network (GROVER et al., 2010) They usually send false messages with multiple identities, which exposes the traffic to misbehaviors that often lead to traffic jams and/or accidents. Therefore, securing VANETs communication is mandatory.

The main objective of this research is to investigate how to prevent and avoid Sybil attacks on VANETs. However, this article has a limited scope as it assumes only Vehicle-to-RSU (V2R) message spoofing.

For the purpose of this article only, messages from RSUs are assumed trustful, while also ignoring Vehicle-to-Vehicle (V2V) message spoofing; two important types of possible attacks that will be considered in future articles.

In this article, the two sample VANET applications are analyzed for detecting security holes in their algorithms and some possible algorithm improvements are suggested to reduce the probability of vulnerability. On another dimension, the article proposes a three-Staged mechanism to enhance the vehicle authentication to avoid identity spoofing the key technique of Sybil attackers. Therefore, the article proposes a Sybil avoidance, prevention, and detection technique that is explained by using the two sample applications. The algorithms of all components of the technique are presented.

Section 2 of this article reviews some related work, while Section 3 presents the two sample VANET applications and their algorithms that are susceptible to Sybil attacks. Section 4 presents the proposed 3-Stage mechanism that is used for attacks detection and avoidance. This mechanism integrates three techniques together to strengthen the solution. The first technique uses the PKI with hashing for sender vehicle authenticity. The other two techniques are the location identification and timestamping, which are integrated together in the form of what is called a sequencing pair of (p, t), which is heavily used for message authenticity and message verification. Section 5 presents the proposed methodology of vulnerability analysis of algorithms for attacks prediction, and then it presents a preventive approach for vaccinating the algorithms through the introduction of the concept of daemon functions in order to protect against possible predicted attacks. Section 6 concludes.

## 2. LITERATURE REVIEW

VANET security requirements may be characterized into groups according to the network topology and communication mode, and VANET Characteristics in terms of Vehicles and Drivers (Hasrouny et al., 2017). Network topology and communication modes are divided into three different types:

- **Unbounded and scalable networks:** because of the wide distances of implementation between one or several cities, thus security for cooperation and management is the one required.
- **Wireless communication:** communication between nodes is via wireless channels, thus requires communication security.
- **High mobility and rapidly changing network topology:** it is hard to specify the nodes position because of the nodes high and random movement, thus enhancing the privacy of nodes is required.

In addition, VANET Characteristics related to Vehicles and Drivers are divided into three types:

- **High processing power and sufficient energy:** VANET have their own power in the form of batteries and high computing powers to run complex cryptographic calculations,
- **Better physical protection:** VANET nodes are physically better protected, it is more difficult to be compromised physically, thus reducing the effect of infrastructure attacks, and
- **Known time and position:** most vehicles are equipped with Global Positioning System (GPS) because many applications rely on position and geographical addressing or area. A tamper proof GPS is used for secure localization to protect nodes location against attackers.

Different attacks may affect VANET systems causing data loss, delay, or even losing the trust of legal nodes; Sybil attacks are the most serious and harmful threats. Sybil attacks can be classified into three different categories, namely, communication, identity, and participation categories. In the communication category, an authentic node sends messages that are caught by a Sybil node in a direct or indirect way, while in the identity category, the attackers create a new identity (fabricated identity) or spoof legitimate identity (stolen identity), yet in the participation category, multiple Sybil identities are created by a malicious node. Some resolutions have been proposed by different researchers to solve VANETs' security

problems; among them are the following ones that inspire the three-Staged avoidance and authentication mechanism proposed by this research.

Kabbur and Kumar (Kabbur & Arul Kumar, 2020) proposed an RSU cooperative-based Sybil attack prediction mechanism that uses the RSU triangulation pattern based on the Radio Signal Strength (RSS) to verify the vehicle's positions communicated across different neighboring RSUs to detect conflicts in timestamps. Syed and Prasad (Syed & Prasad, 2019) proposed a two-phased security mechanism to identify and block the Sybil nodes. The first phase applies the Public Key Infrastructure (PKI), while the second phase uses a hash function; the two mechanisms are merged to both prevent the real data and protect against faked information. Hamdan, Hudaib, and Awajan (Hamdan et al., 2019) proposed a hybrid algorithm to defend the VANET network against Sybil attacks. This hybrid approach combines both the footprint and the Privacy-Preserving Detection of Abuses of Pseudonyms (P2DAP) methods together to gain the benefits of both. P2DAP acts better when the number of vehicles increases, while the footprint algorithm acts better when the speed of vehicles increases. The hybrid algorithm depends on encryption, authentication, and vehicle trajectory. Bo Yu, Cheng-Zhong Yu, and Bin Xiao (Yu et al., 2013) proposed a cooperative method to verify the passion of Sybil nodes by using Random Sample Consensus (RANSAC) algorithm and introduced a statistical method named Presence Evidence System (PES) to verify where the vehicle come from, these approaches can effectively suppress the attacks launched by greedy drivers.

## 3. VANET APPLICATION SCENARIOS

VANETs are used to provide communications to nearby vehicles in terms of V2V and vehicles to other communication devices such as a V2R. Applications are divided into two main categories, convenience-related and safety-related applications. The former type of applications target enhancing the drivers' comfort. It can provide the driver with the updated climate information, parking areas, nearby restaurants or hotels and guides him to the place. The latter type of applications work on the safety of both roads and drivers (Sheikh & Liang, 2019), (Qian & Moayeri, 2008). They try to improve the traffic safety, such as, emergency problems, avoiding collisions and accidents, issuing changing-lane warnings and after-accident road control.

This section discusses and explains some of such applications sample applications from both categories. The purpose is to propose models of applying VANETs in some applications of both types, as sample models. These application models are aimed to propose efficient solutions to some of the common traffic problems that the Egyptian and regional roads are suffering from. Another purpose of presenting those samples is to give traffic authorities a clue on how to use VANETs in solving many other traffic problems. In addition, these sample applications play another role in this article as they are used as a vehicle of demonstrating the vulnerability prediction and avoidance techniques as suggested by this article.

### 3.1 Comfort Applications

Applications of the Comfort category target improving the traffic efficiency and smoothing. Examples of such applications are traffic information system, available parking areas, weather information, restaurant location, gas station, and price information. This section proposes models for two application examples, namely, guiding the vehicle to a parking slot, and road control after emergencies taken place.

**Application 1: Finding Empty Parking Areas.**

Finding a parking slot is a real problem in most of the capitals' roads and it might consume valuable time searching for a slot to park in whether in a garage or at streets nearby the destination; a typical application that VANET can offer a proper and efficient solution for it.

In the proposed model, the vehicle sends a request to the nearest RSU requesting an empty parking slot. Other vehicles in the target zone can also help. When an RSU nearby a garage receives a request for a parking slot, it searches its database and responds back. It then reserves the slot when receiving the requesting vehicle's acknowledgment. On the other hand, street vehicles receiving the request can voluntarily respond when finding an empty street-parking slot; however, they surely cannot reserve the slot that might be consumed before the requesting vehicle reaches it, which might lead to getting into a loop of resending the request. Figure 1 depicts the Parking problem, while Algorithm 1 explains the interactions between vehicles and the involved units.

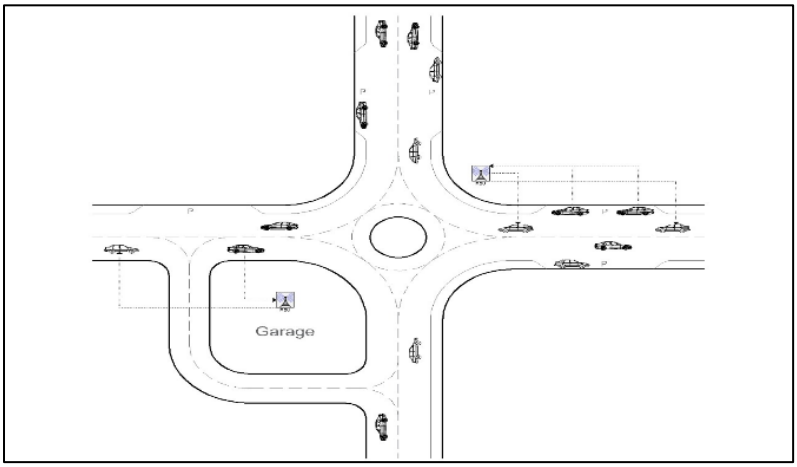


**Fig 1: Parking as an Example of a Comfort Application.**

**Algorithm 1:** Finding an empty parking slot.

**Request Parameters (input parameters):**

- Location or destination.
- If possible, to be within a certain perimeter, or should it be at the exact destination.
- The type of accepted parking area (e.g., public garage, parking lot, street, etc.).
- Current location coordinates (to determine the expected time of arrival).

**Response Parameters (output parameters):**

- Available empty slots in the garage.
- Available empty slots in the nearby streets.

**The Algorithm:**

1. Request for an empty parking area (request is sent to the RSU).
2. If there is an empty slot in the "garage",
   2.1 Then RSU marks the slot as reserved for the requesting ID;
   2.2 Reply with the available slot.
3. If the requesting vehicle acknowledges,
   3.1 Then RSU reserves the slot.
4. When the requester arrives, it sends an arrived message.
5. Cancelation: If the Requester sends a cancelation message
   5.1 Then the RSU marks the slot as empty.

## 3.2 Safety Applications

Safety is the major objective of VANETs, this type of applications increases the safety of passengers and drivers by exchanging safety relevant information via V2V communications. In VANET, each vehicle is equipped with a digital map and electronic sensors, through which sudden changes in path or speed can be detected and appropriate information, such as emergency warnings, road condition warnings, lane changing warnings, etc., be sent to the neighboring vehicles.

**Application 2: Emergency Event Road Management.**
Generally, roads can be blocked due to congestions and accidents. If vehicles coming into this area are not warn, they will continue to flow into the core of the crowd and get stuck there; a catastrophic situation that could last for hours. Warning the vehicles might avoid falling them into a hectic situation, and better off, offering drivers with alternative routes. Figure 2 depicts this situation. This is another application where VANET configuration can help. If the vehicles in an accident zone, immediately send an alert message to the neighboring vehicles and to the nearby RSUs, disastrous situations and traffic jams might be avoided. These accident alert messages will be processed by the nearest RSU. More importantly, the RSU can request the necessary rescue services, such as ambulance, firetrucks, and police patrol. The RSU can provide those rescue control centers and dispatchers with accurate inforamtion so that they send the exact required support, which will save unwanted costs of sending either excessive (excessive cost on the side of service provider) or slight (excessive cost on the crash-involved vehicles and souls) supports. Algorithm 2 summarizes the interaction scenarios between all involved parties.

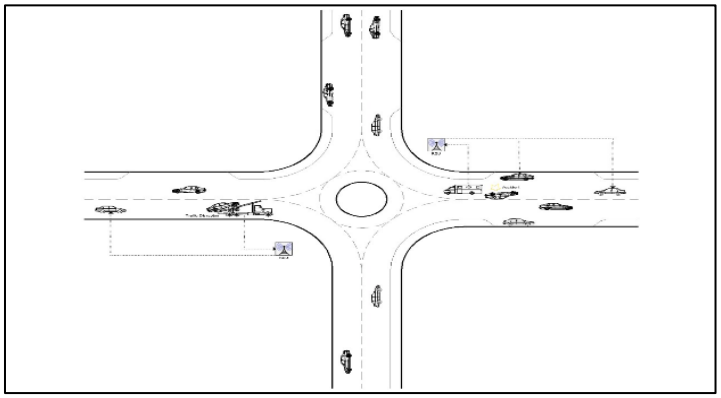

**Fig 2: Example of an Emergency Event Verification.**

**Algorithm 2:** Accident manipulation.

**Input Parameters:**

- Place or location of the accident.
- Number of vehicles involved in the accident.
- Required rescue services (ambulance, police, fire truck, etc.).

**Response Parameters:**

- Call for rescue (accident parameters).
- Streets required to be cleared.

**The Algorithm:**

1. A vehicle involved in the accident or any nearby vehicle sends to the RSU that there is an accident giving the proper parameters.
2. RSU sends a help-request message to the nearest requested service centers (e.g., ambulance, police, fire truck, etc.) with the accident parameters.
3. RSU sends a broadcast for other vehicles to avoid rushing into this place or street.
4. Requested services will broadcast to those streets on their routes to the accident location to reduce the

crowd and avail paths for the rescue vehicles so that they can reach the accident location easily.
5. The RSU broadcasts to all street vehicles those streets requested by the service vehicles to be cleared.

## 4. ATTACKS AVOIDANCE AND DETECTION

Many protocols have been proposed for the detection and protection against attacks. The following three methods are the ones inspiring our proposed technique.

1. **The trusted certification methods**. They are the most common prevention methods generally used for securing messages in traditional networks. They use the public key cryptography and trusted certification. This technique builds on the concepts of Public Key Infrastructure (PKI) (Syed & Prasad, 2019) and the unique trusted certificate (Hamdan et al., 2019). Therefore, a centralized third party (Certificate Authority—CA) issues such identification certificates, a unique certificate for each node. However, trying to copy this technique and apply it for VANEs wouldn't be as effective; refer to Syed Mohd Faisal and Taskeen Zaidi (Faisal & Zaidi, 2020) who stated. "There is no mechanism for issuing unique identities to every vehicle; it is to be done manually, there is no proper mechanism to identify lost and stolen certificates".
2. **The Position verification methods**. In this approach, the physical location of each vehicle is verified before data transmission and is assured to be referring to the proper identity (Faisal & Zaidi, 2020), . Unfortunately, this method, as presented, assumes vehicles authenticity when sending the GPS coordinates (Yu et al., 2013). In fact, a Sybil attacker may manipulate these coordinates before sending the message.
3. **The Time stamp methods**. They depend on the RSU to provide the time stamp for each vehicle at the time of entering the RSU's zone. However, (Sharma et al., 2017) and (Hamdan et al., 2019) improved the algorithm by using a timestamp sequence that is propagated to the neighboring RSUs to keep track of the vehicle trajectory between RSUs' zones. Unfortunately, this approach does not track the vehicle's trajectory inside the zone.

### 4.1 The Proposed new attack avoidance technique

One of the prominent attacks in VANETs is the Sybil attack, in which the attackers create multiple false identities to disturb the functionality of the VANET. This article proposes an avoidance and prevention technique against Sybil attacks. The proposed technique combines the three common security techniques, namely, trusted certification, position verification, and time stamping to give more accuracy while VANETs communication is taking place. Vehicles participating in the VANETs network must have an authorization ID that is given by a certificate authority that issues a temporary certificate with using a key pair for each vehicle touring inside its zone. This certificate is used for the vehicle's authentication in all messaging and communication within this zone. This certificate is for temporary use only inside the zone, which avoids the possibility of being hacked during the short period of time the vehicle spends inside a zone. Therefore, when the vehicle leaves the zone, the certificate expires and the vehicle must request another temporary certificate from the next RSU guarding the new zone it has just entered, at which time the RSU requests to verify the vehicle's certificate by its neighboring RSU before issuing the new one.

In another dimension, each message the RSU receives from an authenticated vehicle (via the certification system) it is yet susceptible to tampering. The RSU must then verify the contents of the message before accepting it. Message verification is done via verifying the location indicated in the message and verify it with the expected actual current location of the vehicle. To do so, the RSU keeps track of all movements of the vehicle within its zone via collecting pairs of position and timestamp of when the vehicle reaches the position (p, t). Each time a vehicle reaches a roads intersection this pair is collected. Two methods can

be used to collect this pair of (p, t), either the vehicle itself can send it via a message or the VANETs infrastructure itself collects it via placing detectors at the road intersections. In the former method, the message can still be tampered by the Sybil attacker; therefore, a verification algorithm (a daemon) is applied by the RSU before accepting the new pair, see Algorithm 5. This algorithm does the proper calculations to assure that it is possible that the vehicle can traverse the distance from the last point reported by position-time pair ($p_1$, $t_1$) to the new reported pair ($p_2$, $t_2$) within an acceptable time period. In the latter method, special type detectors are placed at the critical road intersections to read vehicle plates and report the p-t pair to the RSU. This method is more secured since the p-t pair is communicated via a more secured channel between the detectors and the RSU.

In summary, the proposed technique uses the three elements of certification, location, and timestamp as described above to avoid and detect Sybil attacks through three stages as follows:
**Stage 1**, vehicle certification via issuing a temporary certificate to each vehicle requesting to wander around within the bespoke territory,
**Stage 2**, vehicle authentication when sending a message, and
**Stage 3**, message verification against tampering.

The algorithms describing the suggested mechanisms for the first two stages are described in the following subsections, while that of the third stage is described in Section 5.

### 4.1.1 Vehicle's Identity Registration

Each RSU is considered the sole authority responsible for authenticating vehicles participating in the VANETs network of its territory. The key to authentication is the unique temporary PKI-based certificate that is specially issued for each vehicle at the entry point to the territory, and which acts as the vehicle's passport to use during its wandering within the RSU's territory. This temporary certificate is issued by a Certificate Authority (CA). Two scenarios for this CA: a central CA can be located at the traffic authority headquarters to issue those temporary certificates when requested by the RSU, where the CA has to maintain a log of such requests together with their associated (p,t) pairs. Alternatively, the RSU can be considered a CA only for its territory. When a vehicle leaves the zone, then the certificate and its keys expire, and a new temporary certificate should be requested for the new territory. To increase the security level, the certificates are communicated after being hashed by the (p, t) pair to act as a digital envelope. Algorithm 3 explains the first stage of the avoidance algorithm—the issue of a certificate, while Algorithm 5 explains how this certificate is used to authenticate the message sender to detect faked Sybil nodes.

**Algorithm 3:** Certificate issuance

**Assumptions:**

1. To guarantee unique vehicle ID, the vehicle plate is used as its unique ID.
2. RSU is the only authority to issue unique temporary certificates for the vehicle to use within the RSU's territory.
3. The RSU cannot issue two certificates at the same timestamps.
4. The RSU maintains a database of vehicle IDs, certificate info, entry point, and timestamp of issuance.

**The Algorithm:**

1. At entry point of a new territory, the Vehicle asks for registering in the VANETs network.
2. The guarding RSU verifies the identity of the vehicle by interrogating the previous RSU issuing the vehicle's current temporary certificate.
3. If valid,
   - 3.1 Then it issues a new temporary certificate with a pair of KPI keys.
   - 3.2 The RSU registers the vehicle and its certificate's info in its database together with its entry position and the associated timestamp.
   - 3.3 The RSU digitally signs the certificate and then hash it with the (p, t) pair (to act as a digital envelop), then send it to the requester.

4. RSU maintains a sequence table for (p, t) pairs broadcast the timestamp table to the vehicle timestamp sequence is saved at the vehicles side.

### 4.1.2 Vehicle's Identity Authentication

Noteworthy, each RSU maintains a (p, t) sequence table for each vehicle to keep track of its trajectory inside its territory. This sequence table is stored at both the RSU and the vehicle so that its hash be used as a digital envelop for all message communications between the RSU and the vehicle, of course under the assumption that an RSU cannot issue two certificates at the same timestamp.

Each time a vehicle sends a message to the corresponding RSU, it must encrypt it using the public key of the RSU and then hash the message with its (p, t) sequence table. Both the encrypted message and the hashed message are signed with the private key of the vehicle and sent to the RSU. The mirror image of this algorithm is done at the RSU before sending a message to a vehicle except that the keys are interchanged.

When the RSU receives the vehicle's message, it reverses the algorithm. It uses the public key of the sender vehicle to decrypt the received package. It then decrypts the message using its own private key, then hash it with the (p, t) sequence table stored at its end to compare the two hashes together, if matches occur, it accepts the message and sends it to the verification algorithm; otherwise, the message is rejected.

Noteworthy, the (p, t) sequence table is updated each time the vehicle changed position to a critical intersection point where a trusted detector is placed. This sequence table is stored at both the RSU and the vehicle. Therefore, a Sybil vehicle can be identified and is considered a faked Sybil node if its timestamp sequence matches that of another vehicle, assuming that the RSU cannot give two vehicles the same timestamp, hence, the pair of (p, t) cannot replicate for two vehicles, besides and more evidential the full sequence table. Algorithm 4 explains this scenario.

**Algorithm 4:** Authenticating vehicles when the RSU receives a message

**Assumptions:**

1. Hash of (p, t) sequence table is used as a digital envelop for communication between vehicle and RSU.
2. The (p, t) sequence table is updated each time the vehicle reaches a critical intersection point.
3. The updated (p, t) sequence table is stored at both the vehicle and the RSU.

**The Algorithm:**

Before a message is sent by a vehicle to the RSU:

1. Vehicle encrypts the message using the RSU's public key, and hashes the message with the (p, t) sequence table.
   $X= [E_{RSU\ PU}(M) \parallel H_{(p,\ t)}(M)]$
2. Vehicle signs X with its private key of the vehicle $Y= E_{V\ PR}[X]$
3. The vehicle sends Y to the RSU.

When the RSU receives the message,

4. RSU decrypts Y using the public key of the vehicle to get both the encrypted message and the hashed message.
   $X'= D_{V\ PU}[Y]$
5. RSU decrypts the message using the RSU private key, then hashes the message using the (p, t) sequence table.
   $M'= D_{RSU\ PR}(M) \rightarrow H_{(p,\ t)}(M')$
6. RSU compares the two hashed messages, if matching then accept the message else reject it.
   If $H_{(p,\ t)}(M) = = H_{(p,\ t)}(M')$ then accept else reject

### 4.1.3 Message Authenticity

After authenticating the message sender using Algorithm 3, Algorithm 4 verifies against message tampering. Two verifications take place, namely, location verification and information content verification. The location verification is done via using the (p, t) sequence table to verify that the location mentioned in the message is a reachable location at the bespoke timestamp. A simple algorithm calculates the lengths of all possible paths the vehicle can follow to verify that the reported location is reachable within the timeframe from the last recorded (p, t) pair according to the average speed the vehicle as calculated with the aid of the (p, t) sequence table.

The info content of the message is verified depending on the nature of the message as described in Section 5.

## 5. VULNRABILITY ANALYSIS, PREDICTION, AND PREVENTION

In Sybil attacks, a malicious node or an intruder creates multiple bogus and masqueraded identities to deceive the network to treat them like other authentic nodes (Kumar Karn & Prakash Gupta, 2016). These fake nodes send turbulent messages that may disturb the traffic for its own favor. Therefore, this article presents a methodology for analyzing a VANET's application algorithm to identify possible security holes, and hence, suggesting fixes to prevent against those possible attacks. The remaining of this section discusses the proposed methodology of both analysis and prevention against Sybil attacks.

### 5.1 Vulnerability Prediction

The scenario of interaction should be carefully analyzed to locate those possible intervention points. Those points are the weakest points from which the attacker can penetrate the network.

This article proposes a simple methodology for security holes analysis in a VANET application, where the interaction scenario of the application algorithm should be represented as an Interaction diagram with clear representation of all actors, as shown in Figure 3. Due to the limited space of the article, the analysis, as presented here, has a limited scope expressed in terms of few assumptions. 1) All authority units (e.g., RSU, fire stations, etc.) are assumed authoritative and credible; hence, R2V messages are assumed correct messages. 2) All intervening entities (e.g., street vehicles) are assumed untrustworthy and hence, may be a source of attack. 3) V2V messages are outside the scope of this article. Accordingly, in the interaction diagram, all V2R messages issued by a street vehicle are assumed suspicious, and hence, are carefully studied to determine the best prevention approach.

The proposed attack prevention approach depends on designing daemons functions that use the (p, t) sequence table to do simple calculations verifying the location of the suspicious vehicle as compared to a certain reported location. The algorithm then decides whether these distances and locations are possible, hence accepts, rejects, or asks for resending the message. Examples of those daemons used for the two sample applications of Section 3 are:

- *Verify-Vehicle-location (ID, reported-location),* this daemon function verifies whether the vehicle can possibly be in a nearby location to the reported-location.
- *Avg-trajectory length (ID, Reported-location),* this daemon function calculates the average current expected distance of the vehicle from the Reported-location considering all possible trajectories from the last reported (p, t) entry.
- *Calculate-All-Possible Locations (Vehicle ID),* this daemon function calculates all possible locations the vehicle can be at now. It uses the (p, t) sequence table in its calculations knowing the map of the territory and all possible trajectories.

- *Are-in-the-Route (ID, Requested streets, Target-location)*, this daemon function determines all possible trajectories for a specific vehicle to take from its last reported (p, t) to reach the Target-location and returns Yes if any of them contains the Requested-streets.

## 5.2 Attack Analysis and Vulnerability Prevention for the Sample Applications

The following subsections demonstrate how to analyze the algorithms of the sample applications of Section 3 for identifying security holes that can be a source of possible Sybil attacks disturbing the VANET network.

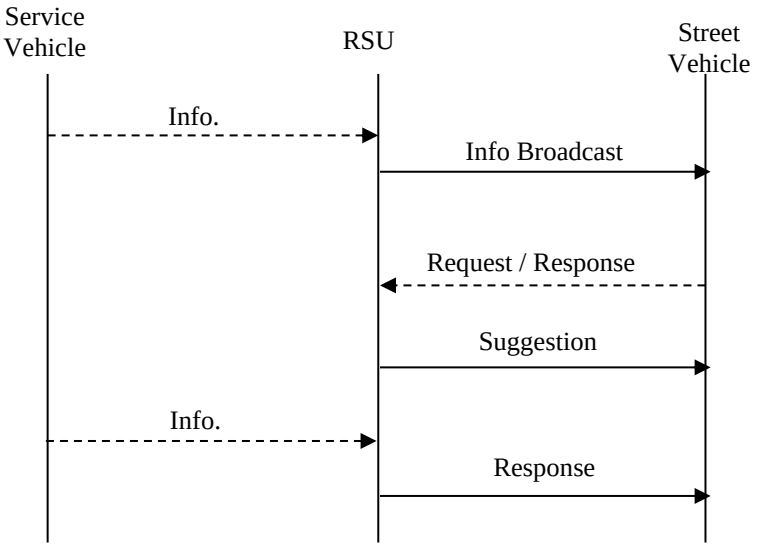


**Fig 3: An Interaction Diagram for an Abstract VANET Application Scenario (Dashed lines are possible malicious messages).**

**Analysis of Application 1: (Attack Analysis for the Parking Application)**
The scenario of interaction of Application 1 (the Parking Application) is depicted as an interaction diagram as shown in Figure 4. By analyzing the Interaction diagram (see Figure 5), attackers may take place causing the requesting vehicle to miss the opportunity of finding an empty parking slot.

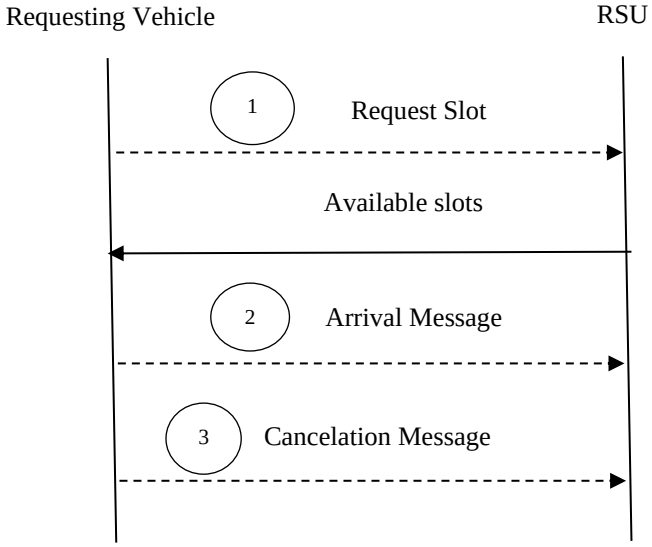


**Fig 4: The Scenario of Requesting an Empty Parking Slot as per Algorithm 1.**

Figure 5 depicts the analysis of the scenario of Figure 4 identifying possible malicious interactions. For instance:

1. A Sybil intruder can create several fake nodes and keep sending flooding messages to overload the station causing a DoS situation.
2. A Sybil node pretending the identity of the authentic requester vehicle may send fake arrival messages, leading the RSU to change the reserved slot to occupied, causing the requester vehicle to lose the parking opportunity as well as keeping the reserved slot hanging up.
3. Similarly, a Sybil attacker may send a faked cancellation message, which would lead authentic requester to lose its opportunity for a parking slot.
4. This type of error, in which the requester itself forgets to cancel its request for a parking slot after changing its mind for a reason or another. This would leave the parking resource unutilized.

Algorithm 5 is a modified preventive algorithm for Algorithm 1. Please note that all assumptions, request parameters, and response parameters are kept the same. The focus is only on the algorithm itself and the insertion of the proper preventing daemon function.

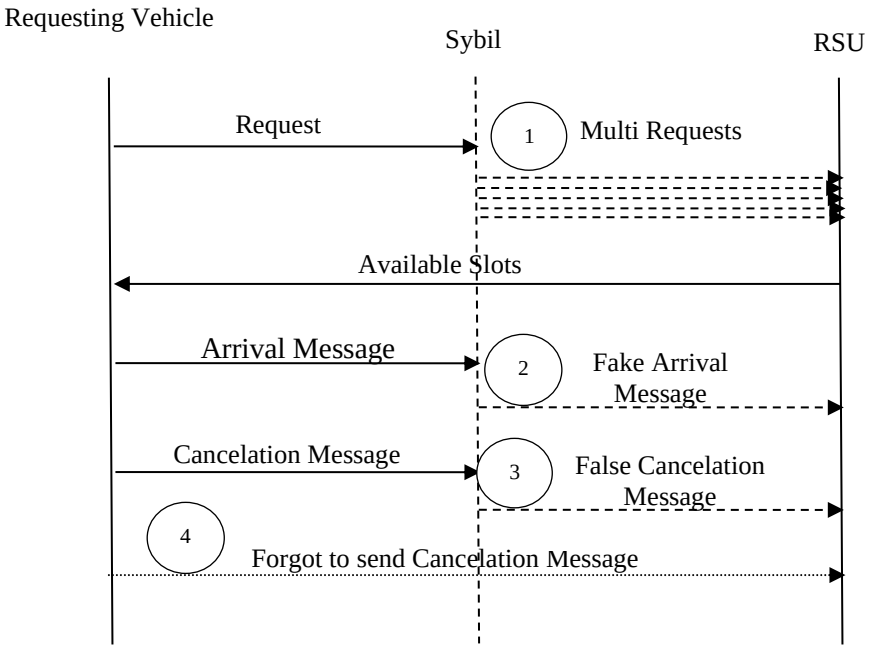


Fig 5: Predicting Possible Attacks for the Application of Requesting a Parking Area.

**Algorithm 5:** (*Preventative*) Finding an empty parking slot.

**The Algorithm:**
**After Authenticating the sender vehicle (Stage 1), and**
**After authenticating the message itself (Stage 2),**

**then most** Sybil requests should have been caught by Stage1 and Stage2 of the 3-Staged technique, however, for more prevention do:

1. Request for an empty parking area (request is sent to the RSU).
   - *Call* ***Verify-location (message. requested parking location)****, if ok, then proceed, else, reject the message.*
2. If there is an empty slot in the "garage,"
   2.1 Then RSU marks the slot as reserved for the requesting ID

2.2 Reply with availability.

3. If the requesting vehicle acknowledges,
   3.1 Then RSU reserves the slot.
4. When the requester arrives, it sends an arrival message.
   - *Call **Verify-location (parking slot- location)**, if ok, then proceed, else, reject the message.*
5. Cancelation: If Requester sends a cancelation message
   5.1 Then the RSU marks the slot as empty.
   - *Send asking for Acknowledgement, if no acknowledgement received, then ignore the message since it is most likely a Sybil message.*

*6. If expected arrival time is reached (calculated by: Call **Avg-trajectory length (Parking slot location)**,*
   *6.1 Then send Acknowledgement to the requesting vehicle (whether Sybil or authentic nodes). This avoids dangling slots.*

**Analysis of Application 2: (Attack Analysis for the Accident Notification Application)**

The scenario of interaction of Application 2 (the Accident Notification Application) is depicted as an interaction diagram in Figure 6. Figure 7 depicts the analysis of the interaction scenarios identifying possible malicious attacks. For instance, a Sybil node may appear in two different places either acting as an authentic street vehicle sending the accident notification or acting as a rescue vehicle. For Instance:

1. A Sybil node exhibiting the role of a street vehicle can send either false accident location and/or wrong accident info to baffle the RSU, hence disturbing the rescue and management of the situation. The message verification algorithm should detect this Sybil attack by comparing the expected current real location of the sender vehicle to the reported accident location.
2. A Sybil node exhibiting the role of a rescue service node can then set false requests for its own favor, e.g., to clear some roads to facilitate the reachability of rescue vehicles to the accident location.

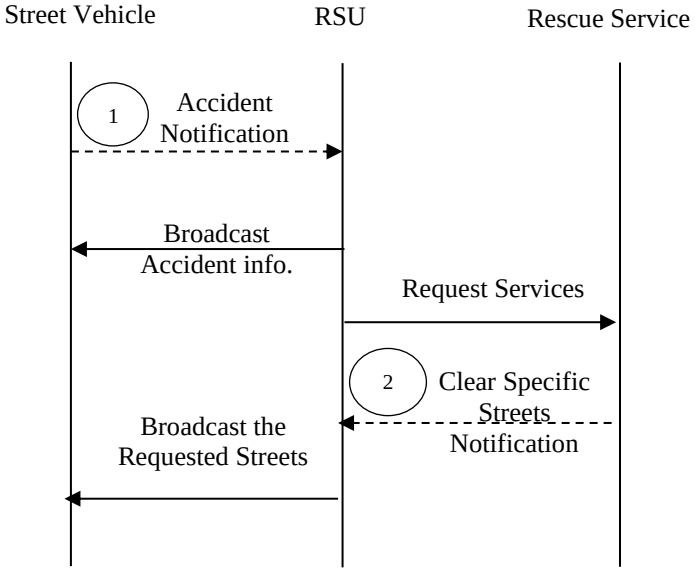


**Fig 6: The Alert Scenario for Handling an Accident.**

Algorithm 6 is a modified preventative algorithm for Algorithm 2. Please note that all assumptions, request parameters, and response parameters are kept the same. The focus is only on the algorithm itself and the insertion of the proper preventing daemon function.

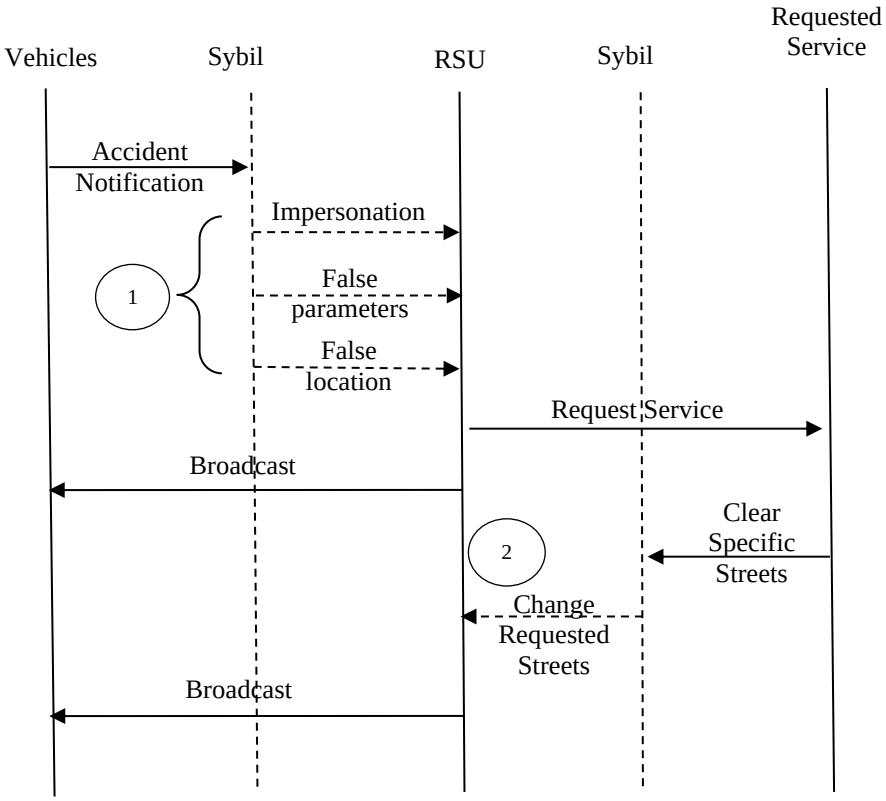


**Fig 7: Predicting Possible Attacks during Handling an Accident.**

**Algorithm 6:** (*Preventative*) Accident manipulation.

**The Algorithm:**
**After Authenticating the sender vehicle (Stage 1), and**
**After authenticating the message itself (Stage 2),**

**then most** Sybil requests should have been caught by Stage1 and Stage2 of the 3-Staged technique, however, for more prevention do:

1. A vehicle involved in the accident or any nearby vehicle sends to the RSU that there is an accident giving the proper parameters.
   - ***For Impersonation****: this should have been caught by Stage2 of the 3-Stage technique.*
   - ***For false location prevention****: call* ***Calculate-All-Possible Locations (Vehicle ID)****, if the sender vehicle cannot be in a nearby location to the reported accident location, then reject the message.*
   - ***For False parameters****: collect the info of the messages received from all vehicles (Sybil or authentic) and take averages before finalizing the rescue plan.*
2. RSU sends a help-request message to the nearest requested service centers (e.g., ambulance, police, fire truck, etc.) with the calculated accident parameters.
3. RSU sends a broadcast for other vehicles to avoid rushing into this place or street.
4. Service vehicles asks the RSU for clearing specific streets to ease the reachability to the accident location.
   - *The vehicle authentication should be cleared via Stage2 of the 3-Stage technique.*
   - *More validation can be done by calling the daemon function* ***Are-in-the-Route (Rescue-ID, Requested streets, Accident location)****, if the answer is false, the message is rejected.*
5. The RSU broadcasts to all street vehicles those streets requested by the service vehicles to be cleared.

## CONCLUSION

Security vulnerability in VANETs threatens people lives. Therefore, this research has focused on finding mechanisms that prevent and avoid against VANET attacks, especially Sybil attacks, the most harmful of them all.

This article introduced a methodology for analyzing VANET's application algorithms for identifying security holes. The article, then, offered few daemon functions that can fix the vulnerability holes and prevent against Sybil attacks. Moreover, a 3-Staged avoidance and authentication mechanism is proposed to strengthen the VANET's authentication system, the system that suffers from Sybil attackers' circumvention. Preventing against Sybil attacks at the application level and avoiding Sybil identity spoofing at operation run time would work together for strengthening the security of the VANET system.

Due to the space limitation of this article, only V2R vulnerable messages are considered. Future articles will address the other two types of messages, namely, R2V and V2V.

## REFERENCES

[1] Faisal, S. M., & Zaidi, T. (2020). Timestamp Based Detection of Sybil Attack in VANET. 22(3), 397–408. https://doi.org/10.6633/IJNS.202005

[2] GROVER, J., GAUR, M., & LAXMI, V. (2010). Sybil Attack in VANETs Detection and Prevention. Security of Self-Organizing Networks, July, 269–294. https://doi.org/10.1201/ebk1439819197-15

[3] Hamdan, S., Hudaib, A., & Awajan, A. (2019). Detecting Sybil Attacks in Vehicular Ad Hoc Networks. ArXiv. https://doi.org/10.1201/b12988-18

[4] Hasrouny, H., Samhat, A. E., Bassil, C., & Laouiti, A. (2017). VANet security challenges and solutions: A survey. In Veh. Commun. (Vol. 7, Issue January, pp. 7–20). Elsevier Inc. https://doi.org/10.1016/j.vehcom.2017.01.002

[5] Kabbur, M., & Arul Kumar, V. (2020). MAR-Sybil: Cooperative RSU Based Detection and Prevention of Sybil Attacks in Routing Process of VANET. Journal of Physics: Conference Series, 1427(1). https://doi.org/10.1088/1742-6596/1427/1/012009

[6] Kumar Karn, C., & Prakash Gupta, C. (2016). A Survey on VANETs Security Attacks and Sybil Attack Detection. International Journal of Sensors Wireless Communications and Control, 6(1), 45–62. https://doi.org/10.2174/2210327905999151103170103

[7] Newsome, J., Shi, E., Song, D., & Perrig, A. (2004). The Sybil attack in sensor networks: Analysis & defenses. Third International Symposium on Information Processing in Sensor Networks, IPSN 2004, 259–268.

[8] Qian, Y., & Moayeri, N. (2008). Design Secure and Application-Oriented VANET. Event (London).

[9] Sharma, S., Scholar, M. T., & Vanets, V. A. N. (2017). A Novel Mechanism of Detection of Sybil Attack in Vanet using Timestamp Approach. 8(1), 200–204.

[10] Sheikh, M. S., & Liang, J. (2019). A comprehensive survey on VANET security services in traffic management system. Wireless Communications and Mobile Computing (Hindawi), 2019. https://doi.org/10.1155/2019/2423915

[11] Syed, S. A., & Prasad, B. V. V. S. (2019). Merged technique to prevent SYBIL Attacks in VANETs. 2019 International Conference on Computer and Information Sciences, ICCIS 2019, 1–6. https://doi.org/10.1109/ICCISci.2019.8716435

[12] Yu, B., Xu, C. Z., & Xiao, B. (2013). Detecting Sybil attacks in VANETs. Journal of Parallel and Distributed Computing, 73(6), 746–756. https://doi.org/10.1016/j.jpdc.2013.02.001

1.