Resilient Privacy Preservation Scheme to Detect Sybil Attacks in Vehicular Ad Hoc Networks

Allam Balaram* and S. Pushpa

Department of Computer Science and Engineering, St. Peter's University, Tonakela Camp Road, Sankar Nagar, Avadi, Chennai – 600054, Tamil Nadu, India; balaramallam@gmail.com, pushpasangar96@gmail.com

Abstract

Objective: Vehicular Ad hoc Networks (VANETs) have the potential to improve road safety dramatically, regulate traffic, management of parking lots and public areas. Security and Privacy are two significant concerns in VANETs, as a malicious vehicle may deliberately deceive other vehicles in the network. Analysis: Disastrously, several privacy-preserving methods are susceptible to Sybil attacks, whereby a malicious vehicle impersonates as multiple benign vehicles for gaining a disproportionately large influence. Conventional pseudonym generation schemes preserve driver’s privacy and also facilitate identifying the Sybil attacker. However, the pseudonym scheme induces a brand new issue where in a smart attacker may compromise semi-trusted RSUs and launch a Sybil attack in a particular area. Findings: This paper proposes a System for detecting misbehavior vehicles with location Privacy (SYBIL-CAP), consisting TcA - Preserving Location Privacy (TAP-LOOP), and Resilience to RSU compromise (RESUME) for identifying Sybil attacker. SYBIL-CAP provides a temporarily authorized certificate that includes the trusted certificate and secret key trajectories to vehicles to recognize compromised RSU without requiring the unique identity of vehicles. More precisely, in TAP-LOOP, a vehicle approaches a TCA to receive a location-hidden trusted certificate via RSU to conceal its sensitive information at all times. RESUME implements Diffie-Hellman Key Exchange (DHKE) algorithm between two adjacent RSUs to generate a shared secret key, appended in the temporarily authorized certificate. A vehicle identifies the compromised RSU and malicious vehicle by verifying the authorized message at a group of three consecutive RSUs. Improvement: The simulation results depict that the SYBIL-CAP largely restricts Sybil attack by detecting compromised RSU with lower overhead, compared to existing P2DAP.

Keywords: Location Privacy, Sybil Attack, Secret Key Trajectory, Temporary Authorized Certificate, Vehicular Ad hoc Networks (VANETs)

1. Introduction

VANET is necessary to increase driving comfort and safety level of the transportation system. The VANET contains network entities primarily, including vehicles, Road Side Units (RSUs), and Trusted Certification Authority (TCA). Also, the vehicles are equipped with sensors and Global Positioning System (GPS) to monitor potholes in the road and learn their positions respectively. Thus, it improves the road safety and provides a greater degree of driving experience. Fundamentally, security fabrication in wireless networks must assure authentication, non-repudiation, and confidentiality to defend networks against malicious vehicles. Proximal to the fundamental security requisites, it is vital to protect the sensitive information such as real identity and the current location of vehicles against unlawful tracing attackers during the journey.

In urban vehicular networks, the location privacy of vehicles is a great concern as an attacker can easily track or divert a target vehicle to perform crimes. To ensure the authenticity of messages propagated in vehicular networks, a straightforward technique exploits certified public keys termed as pseudonyms that are provided by a TCA to sign the messages. In contrast, with the aim of preserving the vehicles from an attacker by identifying the keys which are used, a vehicle can switch its pseudonym among numerous pseudonyms hence it is rigorous to correlate with one.
another. In pseudonym approach, it is a challenging task for an attacker to examine the pseudonyms and several efficient techniques are proposed in [10].

Although the pseudonym protects the user privacy, it leaves another security hole. A malicious vehicle may pretend as multiple vehicles named as Sybil attack and then inject a false event into the network. It is complex to determine whether the two messages are from the identical vehicle by examining their pseudonyms that lead to a biased or inconclusive decision. To rectify this, [11] proposes a lightweight solution where the vehicle retains only a valid pseudonym at a time and thus efficiently prevents the malicious vehicles from linking a vehicle's different pseudonym. Also, an ingenious attacker may compromise an RSU and obtain many certified pseudonyms from compromised RSU and thus easily can create false events in that area.

This paper proposes a System for detecting misbehavior vehicles with location Privacy (SYBIL-CAP) that employs the unlikable secret key trajectories of vehicles to detect a compromised RSU and a Sybil attacker without revealing the original information of vehicles.

1.1 Contributions
The primary objective of SYBIL-CAP is to preserve the location privacy of vehicles against compromised RSU and Sybil attack using secret key trajectories. SYBIL-CAP incorporates three classic techniques named as an optimal deployment method on RSU, TAP-LOOP, and RESUME.

To achieve maximum performance, SYBIL-CAP utilizes a precise optimal deployment method among RSUs. SYBIL-CAP allows only some degree of overlap between two RSUs to avoid overhearing of the secret key by compromised RSU.

To guarantee location privacy of vehicles, TAP-LOOP provides location hidden trusted certificate to each vehicle for hiding its unique identity. SYBIL-CAP reduces the overhead complexity on TCA, as the vehicle utilizes the same trusted certificate to a group of RSUs for authentication.

To prevent a smart attacker using multiple trusted certificates to launch a Sybil attack, the RESUME provides the secure secret key to the vehicle by implementing DHKE algorithms on RSUs. The vehicles identify the forged authorized certificate by verifying the secure key trajectory to a group of RSUs.

Effective simulation results demonstrate that the SYBIL-CAP achieves a greater degree of location privacy against compromised RSU when compared to the existing Privacy Preserving Detection of Abuses of Pseudonyms (P2DAP) scheme.

1.2 Problem Statement
Most of the existing work enables each vehicle to receive multiple pseudonyms from the RSU to preserve its location privacy. Although the multiple pseudonym schemes preserves the privacy of vehicles, an attacker can design forged pseudonyms itself by linking the spatial and temporal relationship between multiple pseudonyms. As a result, an attacker can masquerade as multiple vehicles and inject a false message into the network. To avoid the attack, some conventional techniques introduce a lightweight solution, where vehicles have only a valid pseudonym at a time, and a vehicle obtains new pseudonym from TCA when the current pseudonym becomes invalid. It assists the RSU to determine the attacker, even though the RSU is a semi-trusted entity where a smart attacker can still gain multiple pseudonyms of a benign vehicle stored in the RSU by compromising the RSU. Thus, the attacker can inject false event messages in that particular area. If the compromised RSU is not detected immediately, it impacts the critical functions of security system such as authenticating message provision and pseudonym generation. It is crucial to design a robust security scheme to detect compromised RSU and Sybil attacker, and it also assures the location privacy of users. The SYBIL-CAP determines the compromised RSU and Sybil attacker using TAP-LOOP and RESUME schemes.

1.3 Paper Organization
The remainder of the paper is organized as follows. Section 2 discusses the earlier works on location privacy and the Sybil attack detection. Section 3 describes the system and attacker models in vehicular networks. Section 4 elaborates the design of SYBIL-CAP. Section 5 demonstrates the effective simulation results of SYBIL-CAP. Section 6 provides concluding remarks of SYBIL-CAP.

Many security mechanisms have been proposed in distinct ways in dissimilar networking areas which preserve the privacy of vehicles that involve in vehicular communication. During communication, an attacker can track the location of a victim vehicle based on its event distribution messages. To overcome this drawback [12] proposes an approach called CARAVAN...
mitigates the number of broadcasts that the vehicle uses in V2R communication by dividing the vehicles into groups. Additionally, CARAVAN suggests an enhancement technique to separate RSUs and to control their transmission power. However, the attackers launch an attack by tracing a Location Based Service (LBS) messages, as the communication medium is unreliable. The work in provides anonymity to the vehicles in which a vehicle updates its keys on direction changes. However, anonymity cannot be achieved in global adversary model.

Mix-Zones create cryptographic mix-zones at road intersections based on a CMIX protocol, and it preserves the location privacy of users. It mixes the vehicle's identifier by combining the mix-zones into the mix-networks that provide unlinkable dynamic pseudonyms for a vehicle. AMOEBA employs a vehicle's group navigation scheme to achieve location privacy and it allows the vehicles to get LBS applications in an anonymous manner. However, an attacker can easily target a vehicle in the existing group by entering a new group earlier. To rectify this issue, the DLP derives a delay distribution model for vehicles in the density zone from identifying the attackers. The Pseudonym Changing at Social spots (PCS) mechanism develops anonymity set for achieving location privacy in vehicular networks using a Key-insulated Pseudonym Self-Delegation (KPSD) scheme to palliate the hazards due to vehicle theft.

Changing single pseudonym in vehicular communication is not sufficient to effectively preserve the privacy of users, as an attacker can eavesdrops many pseudonyms of benign vehicles in a particular area by overhearing or spoofing. To address this problem, some of the conventional methods allows a vehicle to use multiple pseudonyms in which a vehicle frequently changes pseudonyms to strong location privacy. However, the multiple pseudonym approaches are vulnerable to Sybil attack. A privacy-preserving Sybil attack detection scheme allows the TCA to distribute a set of pseudonyms to the vehicles via RSU, and the RSUs can only detect abused pseudonyms. Such method requires high cost due to full coverage of RSU deployment. Also, when an RSU detects suspicious pseudonym, it requires sending the suspicious pseudonym to TCA for taking further actions. Thus, it makes the TCA be a bottleneck.

The works introduce a group signature scheme to assure that a verifier vehicle can identify the forged messages received from neighboring vehicles by scrutinizing the content of the message. The schemes only handle different messages, but not similar. Multiple vehicles observe the same driving environment and it may generate different messages with very similar semantics. To solve this issue, the RSU provides authorized time stamps to its proximity vehicles as a proof of presence at this RSU at a given moment. During communication process, the vehicles employ the authorized time stamps for identity verification. In consequent time stamp series with corresponding RSU's public key is used for identifying the attacker. However, an attacker infers the location of a targeted vehicle by exploiting location information using RSU signature; the RSUs employ the same signature for a long time to provide time stamps to vehicles.

Footprint designs location hidden trajectories using two properties such as unlink ability and a signer ambiguous. The location hidden trajectories can preserve the location privacy of vehicles at the same time the footprint detects a Sybil attack using the social relationship among trajectories. Even though a smart attacker may compromise the semi-trusted RSUs, the attacker can obtain legal trajectories of another vehicle from the compromised RSU, converting it as a Sybil attack launch in that area. A P2DAP proposes a new technique to detect a Sybil attack in vehicular networks. The P2DAP distributes the computational complexity from the TCA to RSUs. Hence, it releases only a limited amount of information by using hash collisions. In P2DAP, RSU detects a Sybil attack through passive overhearing and also, it preserves the vehicle’s location privacy. However, it does not provide precise solutions to detect compromised RSU, and an attacker can obtain the coarse-grained hash key from the compromised RSU.

2. System Model

- Network: G (N, E)
- Vehicle: V
- Malicious and honest Vehicle: V_m and V_h
- Direct Connection: E
- Public Key: K_pub
- Private Key: K_pri
- Public Key List: PKL
- Three Consecutive RSUs: β RSU
- Secret Key Information: K_s
- Real Identity Information: R_ID
- Trusted Certificate: T_c
- Temporary Authorized Certificate: T_AC
The network is represented as a communication graph $G (N, E)$. The set $N$ includes TCA, RSUs, and vehicles and the set $E$ contains all directional links between vehicles. TCA is responsible for managing the RSUs in VANET. For establishing SYBIL-CAP in a secure manner, TCA which has sufficient resources provides $(K_{pub}^{RSU})$ and $(K_{pub}^{v})$ to the corresponding $\beta_{RSU}$ and vehicles $(V)$ respectively. Also, it provides $(K_{pri}^{RSU})$ and $(K_{pri}^{v})$ to each RSU and vehicle respectively via a secure channel. The RSU and $V$ employ the key pairs to encrypt and decrypt the control and data packets. In SYBIL-CAP, the interconnected RSUs offer a backbone structure to the vehicles, and it provides $K_s$ to each $V$ for determining malicious $V (V_m)$ and compromised RSU. $V$ is equipped with OBU for enabling V2V and V2R communication and GPS to know its location.

2.1.1 Vehicle Registration Process

At the time of registration, a vehicle registers its $R_{id}$ to the TCA for getting $K_{pub}^{v}$ and $K_{pri}^{v}$. If $V$ enters into VANET, it receives a $T_c$ from TCA through RSU, and it forms a $T_{AC}$ using $T_c$ and $K_s$ trajectory.

2.1.2 Vehicle Communication Process

If communication occurs between two vehicles, the sender $V$ submits its $T_{AC}$, including $K_s$ trajectory built using $\beta_{RSU}$ to the receiver $V$. The receiver $V$ verifies the $T_{AC}$ to the $\beta_{RSU}$ to determine the $V_m$ and compromised RSU.

3. Attacker Model

As per the attacker model $G (N, E)$ it contains three types of nodes such as fixed trusted TCA, fixed semi-trusted RSU, and high-speed movable un-trusted $V$. The $V_m$ launch attacks into the network by pretending as multiple identities. Assume that the $V_m$ has higher power than other honest vehicles $(V_h)$ of launching a Sybil attack. In Sybil attack, $V_m$ injects a false event into the network and reinforces that event by impersonating as multiple vehicles. The $V_h$ takes decisions based on a false event report submitted by multiple vehicles. Moreover, $V_h$ believes the false event, and it takes the wrong decision. $V_m$ easily diverts the targeted $V_h$ for eavesdropping money or performing crimes. $V_m$ may get sufficient information for launching attacks in two ways such as message persuasion and compromised RSU.

3.1.1 Message persuasion

The $V_m$ eavesdrops the communication of other vehicles due to the nature of the wireless medium. The $V_m$ employs the eavesdropped information to launch a Sybil attack.

3.1.2 Compromised RSU

An ingenious $V_m$ may compromise an RSU, the RSU provides the authentication of other $V_h$ to the $V_m$.

4. SYBIL-CAP Overview

The SYBIL-CAP integrates elegant techniques such as RSU deployment, TAP-LOOP, and RESUME to detect the Sybil attacker and compromised RSU. In optimal deployment method, the TCA distributes a limited number of RSUs evenly along the roadside which is able to cover a maximal service area for providing security services. A vehicle in VANET requires a temporarily authorized certificate from TCA to submit the certificate as a proof at the time of V2V communication. The SYBIL-CAP provides the temporarily authorized certificate that includes a trusted certificate and a secret key trajectory that are generated using TAP-LOOP and RESUME techniques respectively. This trajectory represents the sequence of the secret key issued by RSUs along a traveling path. The TAP-LOOP adopts a temporarily authorized certificate scheme for TCA to issue a trusted certificate to RSU. Even though it preserves the location privacy of a vehicle, it increases the overhead complexity in VANET. The TCA in SYBIL-CAP issues the same certificate to a group of three consecutive RSUs and improves the system performance regarding the amount of traffic as well as location privacy. However, a compromised RSU may release the trusted certificate of vehicles held by it to the attacker. To avoid this, RESUME implements the DHKE algorithm among RSUs to issue the secret key to each vehicle separately. Vehicle energy is not a problem in SYBIL-CAP, as the vehicle only acts as a router for exchanging shared secret key between RSUs. Before establishing communication with other vehicles, a vehicle must submit its authorized message, including the trusted certificate and shared secret key received from three consecutive RSUs for authentication. In the verification process, each RSU in a group evaluates the final secret key to a corresponding shared secret key with its signature. The RSU, which contains the corresponding vehicle, collects the final secret keys from other RSUs in its
group and provides the keys to the vehicle for reference. The vehicle identifies the compromised RSU by verifying the final secret keys generated by a pair of consecutive RSUs. The SYBIL-CAP distributes the workload from the TCA to RSUs while releasing only a limited amount of information, so it achieves location privacy in case of RSU compromise.

4.1 Deployment of RSU
As per SYBIL-CAP, it is crucial to provide a temporarily authorized certificate, including trusted certificate and trajectory for establishing communication among vehicles. In SYBIL-CAP, the TCA issues trusted certificate to each vehicle and also a group of RSUs. Identifying the attackers among vehicles is sufficient. However, in case the RSU is compromised, it is crucial to avoid the trajectory information overheard by RSUs so that the genuine RSU is required to establish the secure communication for providing trajectory to vehicles. The SYBIL-CAP allows some degree of overlap among RSUs to facilitate the communication among them with long transmission power, but it employs only short transmission power to communicate with vehicles. Thus, it avoids overhearing the secure key information released by other RSUs resulting in secure communication even when the RSU compromise.

To assure that each vehicle receives authorized messages from RSU, it requires that stationary installation of sufficient RSUs along roadside ensure to provide a backbone structure to VANET. Deploying huge number of RSUs is unavoidable owing to the high cost and easy launch of the overhearing attack. The SYBIL-CAP employs an optimal deployment method for locating a limited number of RSUs along roadside uniformly and it makes the SYBIL-CAP easier to provide security services to the vehicles of all time.

\[ D_{RSU} = 2r - I_r \] (1)

The SYBIL-CAP deploys RSUs with some degree of overlap as shown in equation (1), where \( D_{RSU} \), \( r \), and \( I_r \) represents Distance between two RSUs, Radius, and Interference range of two RSUs respectively. Interference range of RSUs is varied due to the corresponding area of a city and rural. According to the equation (1), SYBIL-CAP places the RSUs at least far away from each other to avoid the overhearing attack. The TCA overload is divided evenly among RSUs, and it results in a fine temporary authorized certificate which facilitates the secure communication between vehicles and diminishes the workload on TCA. Even though SYBIL-CAP shares trusted certificate of vehicles among three consecutive RSUs, it assures the location privacy because it can identify the compromised RSU by using the RESUME technique with the optimal deployment of RSUs.

4.2 TCA - Preserving Location Privacy (TAP-LOOP)
In SYBIL-CAP, whenever a vehicle enters into a network, it needs a trusted certificate from TCA via RSU to hide its real location and identity information. Instead of generating the trusted certificate to a vehicle under all RSUs, TCA provides single temporary trusted certificate to a vehicle until it leaves three consecutive RSUs along its traveling route. This scheme reduces the routing overhead complexity. Trusted certificate generation scheme includes two steps such as initialization and certificate renewal.

Initially, a vehicle sends a request message to the RSU for generating authorized certificate temporarily. The TCA verifies the information in the request message like vehicle’s ID and signature, and it generates a temporarily authorized certificate to the vehicle. For reducing overhead, the SYBIL-CAP divides the RSUs into several groups under the TCA. Each group consists of three consecutive RSUs in a road. The TCA forwards the trusted certificate of a vehicle for a group of RSUs and only first RSU in a group takes the responsibility to send the trusted certificate to the corresponding vehicle. The trusted certificate contains some fields such as vehicle’s temporary ID, RSU’s group ID, TCA’s signature, and Time To Live (TTL) value.

In TAP-LOOP, a vehicle needs to change its temporary certificate if it encounters a new RSU group. In certificate update step, a vehicle must submit its previous temporary certificate to the RSU of a new group for getting a new trusted certificate. If a vehicle receives a new certificate, the previous certificate becomes invalid. Likewise, the vehicle changes its temporary certificate frequently for strong location privacy. Moreover, the vehicles only hold one valid trusted certificate at a time in TAP-LOOP, and an attacker cannot launch an attack without multiple trusted certificates.

Although in some cases, a malicious vehicle may compromise an RSU and the RSU can issue many trusted certificates of other genuine vehicles to the malicious vehicles, thus launching attacks in that area. To avoid this, the SYBIL-CAP includes a RESUME technique in
Resilient Privacy Preservation Scheme to Detect Sybil Attacks in Vehicular Ad Hoc Networks

TAP-LOOP that can determine the compromised RSU in VANET.

4.3 Resilience to RSU compromise (RESUME)
RESUME implements a DHKE algorithm between RSUs to build a security tunnel among vehicles in VANET even in the case of RSU compromise. During the provision of trusted certificate to the vehicle, each RSU generates shared secret key information for a vehicle to form a secret key trajectory using DHKE algorithm. Any vehicle in VANET can determine the compromised RSU by verifying secret key trajectory at three consecutive RSUs.

4.4 Diffie-Hellman Key Exchange (DHKE) Algorithm
DHKE algorithm is a cryptographic method that allows two communicating parties without prior knowledge to derive common secret key information over the insecure channel. The DHKE algorithm employs prime number, base value and a secret integer for deriving a secure key. Before exchanging the shared secret key using DHKE algorithm, the two communicating parties must agree on a sufficient prime number (P) with congruence class. A congruence class is a set of integers that are congruent to the modulo P. Congruent refers multiplicative series of integers modulo P, which is also co-prime to P. A non-zero base (B) is a primitive root modulo P selected from the congruence class.

4.4.1 DHKE Algorithm Steps
The DHKE algorithm includes the following steps.

4.4.1.1 Generating Shared Secret Number
Sender and receiver select a common prime number and selects a base value from the congruence class of modulo P. After selecting common prime and base value, the sender and receiver generate an independent shared secret random integer.

4.4.1.2 Shared Secret Key Provision
Sender and receiver substitute the common prime number, base value, and secret random integer in $K = B^r \mod P$ for computing shared secret key $K_s$ and $K_r$. The RSUs share the shared secret via the corresponding vehicle.

4.4.1.3 Secure Final Secret Key Generation
The sender and receiver exchange the shared secret key value and estimate a same final secret key value as $K_s = (K_r)^s \mod p$ and $K_r = (K_s)^r \mod p$.

4.5 SYBIL-CAP Implements DHKE
SYBIL-CAP implements the DHKE algorithm among RSUs for determining the compromised RSU in VANET. Implementing the DHKE algorithm in SYBIL-CAP does not affect the energy level of a vehicle as the DHKE algorithm execution takes place at RSUs which have adequate energy. SYBIL-CAP implements the DHKE algorithm among RSUs in three steps. Note that TCA issues the prime number to all the RSUs for all the vehicles registered in it. SYBIL-CAP implements a first step of generating shared secret integer to a vehicle among neighboring RSUs, only when a corresponding vehicle travel within the communication range of any one of the RSU. In the second step, instead of sharing the secret number among RSUs directly, it uses the corresponding vehicle as a router. The RSUs provide the shared secret information to the vehicle with its signature. With the aim of identifying the compromised RSU using secret trajectory, SYBIL-CAP implements the third step only when a vehicle demands communication with another vehicle. The secret trajectory of three diverse secret information is about a group of RSUs and it plays a major role in the identification of compromised RSU in the network.

4.6 Secret Key Trajectory Generation
Initially, the TCA knows the total number of vehicles and evenly divides the vehicles into multiple groups in SYBIL-CAP. TCA generates a prime number with congruence class for a group of vehicles, and it distributes the prime number list to all RSUs in the network. If a vehicle enters into the communication range of any RSU, it requests the RSU to generate temporarily authorized certificate including trusted certificate and shared a secret key. The corresponding RSU combines with its preceding and succeeding RSUs and executes the DHKE algorithm to produce two different shared secret keys to the vehicle. The RSU attaches the two shared secret keys of preceding and succeeding RSUs in a packet. A vehicle receives the shared secret key packet from the corresponding RSU. A vehicle forms trajectory using the various shared secret
key of RSU group, as the vehicle needs to verify the secret key trajectory to a group of three consecutive RSUs during the communication process.

Consider if a vehicle2 reaches the communication range of RSU3. According to the first step of DHKE algorithm, a pair of RSU (RSU34) has knowledge about the prime number value of a corresponding vehicle2, and they select a common non-zero base value \( b3 \) from the congruence class of that vehicle. After choosing a common prime and base value, the RSU34 picks secret random integers \( s3 \) and \( s4 \) independently. An RSU3 does not reveal the secret random integer \( s3 \) to anyone in VANET.

\[
K_s = b3 \mod P
\]  

\[\text{(2)}\]

In accordance with DHKE algorithm, RSU34 evaluates the shared secret key using equation (2). The RSU3 attaches the shared secret key of RSU4 and RSU2 in a packet with its signature. A vehicle receives shared secret key packet from the corresponding RSU3 during the provision of the authorized certificate. Likewise, a vehicle2 receives multiple shared secret key along its traveling route, and it forms a secret key trajectory \((K_2v^2, (K_1+K_3)v^2, (K_2+K_4)v^2)\) using the multiple shared secret keys that are received from RSU1, RSU2, and RSU3. Moreover, a vehicle receives \( n \) number of shared secret keys along its voyaging path to form a secret key trajectory.

It is essential to consider the trajectory length in SYBIL-CAP, as a vehicle meets a large number of RSUs along its path. If the trajectory length is too long, an attacker can partially know the trajectory of a vehicle for that long travel. SYBIL-CAP limits the trajectory length based on the system model and RSU deployment. The trajectory length is limited as three in SYBIL-CAP as a vehicle only needs to verify its trajectory at a group of three consecutive RSUs. So a vehicle maintains the trajectory for previous three RSUs in its traveling path.

4.7 Sybil Attack Detection Mechanism

It is possible that an attacker can collect multiple forged trajectories through message persuasion or compromised RSU and launch Sybil attack into the network. There is a verification need for determining the forged trajectory injected by a Sybil attacker and the compromised RSU. SYBIL-CAP employs the third step of DHKE for determining the Sybil attacker and compromised RSU, and it implements the third step on all participating vehicles in event sharing.

During communication, the sender vehicle must submit its temporary authorized message, including the shared secret key received from previous three RSUs along its path to the receiver vehicle. The receiver vehicle has to verify the authenticated message to the group of RSUs before making communication with the sender. Each RSU verifies its corresponding secret key and sends a reply packet to the vehicle via current RSU. Even if the current RSU is compromised, it cannot open the authentication packet received from other RSUs. The vehicle identifies the current compromised RSU when the final secret key of a pair of two consecutive RSUs is not same.

Consider vehicle3 wants to communicate with vehicle2 in Figure 1. Vehicle3 submits its authorized certificate, including the secret key trajectory of three consecutive RSUs, \( K_s(\beta_{RSU2}, \beta_{RSU2}, \beta_{RSU4}) \). Vehicle2 submits the received shared secret key to RSU3 and the RSU3 provides individual shared secret key copy such as \( K_s(\beta_{RSU3}) \) and \( K_s(\beta_{RSU4}) \) to the RSU2 and RSU1 respectively. The RSU2 and RSU1 estimate the final secret key using DHKE algorithm for the received secret key and send the final secret key values to the vehicle via RSU3 for vehicle reference. If the final secret key values of succeeding pair of two RSUs (RSU1&2 and RSU2&3) are equal, the vehicle establishes communication with the vehicle that submits trajectory. Otherwise, the vehicle forwards the false alarm message to the next RSU, when it moves into the communication range of next RSU.

In SYBIL-CAP, next RSU reports to the TCA against compromised RSU when it receives a false alarm of mismatched final secret key from the vehicle. In SYBIL-
5. Performance Evaluation

The performance of SYBIL-CAP is demonstrated through Network Simulator (NS-2) version 2.35, using the MAC IEEE802.11p module. The SYBIL-CAP is compared with existing P2DAT for analyzing performance. The SYBIL-CAP performs simulation on a map representing an area of 1.5 x 1.5 km². The SYBIL-CAP randomly deploys 100 number of vehicles with optimally deployed 12 RSUs over the network area. The simulation Time is 500 seconds. The communication range of a vehicle and RSU is 250m and 500m respectively. The high average speed of a vehicle is 60Km/hr. Each vehicle utilizes Greedy Perimeter Stateless Routing (GPSR) protocol, as it is a position based routing protocol especially optimal for vehicular networks. The initial energy of a vehicle is 100 Joules. The SYBIL-CAP implements Constant Bit Rate (CBR) in the application layer and User Datagram Protocol (UDP) in the transport layer with a packet size of 1024 bytes in the interval of 4 milliseconds. The link bandwidth is 2Mbps. The SYBIL-CAP designs the VANET scenario by employing Simulator of Urban MObility (SUMO) and MObilit model generator for VEHicular networks (MOVE). Each vehicle exploits Omni directional antenna for enabling V2V and V2R communication.

5.1 Simulation Results

The qualitative performance of SYBIL-CAP is examined using some metrics such as Detection Accuracy, False Positive (FP), RSU Isolation Delay, Tracking Time, and Overhead.

5.1.1 Detection Accuracy

The detection accuracy is defined as the percentage of Sybil attack attempts that are determined successfully by SYBIL-CAP. The SYBIL-CAP analyzes the detection accuracy regarding True Negative (TN). The true negative is defined as the percentage of forged vehicles that are accurately identified as Sybil vehicles by SYBIL-CAP.

5.1.2 False Positive (FP)

It is the percentage of normal vehicles which are inaccurately regarded as Sybil vehicles by SYBIL-CAP.

5.1.3 RSU Isolation Delay

RSU isolation delay is the total time taken by the genuine RSU and TCA to isolate a compromised RSU from the network after receiving a false alarm report from the corresponding vehicle.

5.1.4 Tracking Time

It is the maximum time taken by a vehicle to determine the attacker and compromised RSU through authorized certificate verification.

5.1.5 Overhead

It is defined as the number of additional packets appended to preserve and detect vehicle’s location privacy and attack.

5.2 Detection Accuracy Results

Figure 2 demonstrates the TN results of SYBIL-CAP by varying the vehicle density from 50 to 100 in the fixed network area of 1.5 x 1.5km². Also, for each density, the SYBIL-CAP repeats the simulation for different trajectory length. The TN decreases with increasing the number of vehicles in the network. The reason behind this that the vehicles may losses some authorized packets due to congestion. For instance, the SYBIL-CAP attains 94% and 89.4% of true negative for 50 and 100 vehicle density respectively, when the trajectory length is 3. On the other hand, the trajectory length affects the TN as the vehicles; verify the trajectories to a group of RSUs for detecting compromised RSU in the network. The SYBIL-CAP employs DHKE that is applied between a pair of RSUs in a group. If a vehicle’s Trajectory Length (TL) is two, it verifies the trajectory at only two consecutive RSUs during communication that may lead to suspect a genuine RSU and thus impacts on the TN. So the vehicle trajectory length limit is three in SYBIL-CAP and thus improves the true positive rate up to a maximum 94.1%.

![Figure 2. Vehicle density vs. true negative.](image-url)
Figure 3 shows the TN results of SYBIL-CAP by increasing the number of RSUs from low to high for different Vehicle Density (VD). In Figure 3, SYBIL-CAP varies the number of RSUs within the same area (1.5 x 1.5 km²), resulting the interference range between two RSUs are also varied. In P2DAP, the RSU determines the attack through passive overhearing. The P2DAP requires a substantial interference range of overhearing process to detect attackers and the TN of P2DAP raise to around 1.5% when at least 15-16 RSUs are deployed in 1.5 x 1.5 km². Owing to the high cost, SYBIL-CAP employs optimal deployment method to deploy a fewer number RSUs with minimum interference range, and it allows the vehicles to verify the trusted certificate to a group of RSUs. Moreover, it requires less number of RSUs (12-13) to verify trajectories for attack detection. TN decreases with increasing vehicle density as the packets are waiting in the queue when vehicle density is maximum to around 100. Thus, it unexpectedly reduces the detection accuracy from 94.1% to 90.1% for 60 and 100 vehicle densities due to the collision.

Figure 4 illustrates the True-negative results that are obtained by varying the number of attackers from 2 to 14 for various trajectory lengths. The TN is slightly decreased, when varying the number of attackers from low to high. The number of attackers cannot affect the TN rate severely, as the SYBIL-CAP employs sufficient trajectory length for accurate attack detection. For instance, the SYBIL-CAP reduces the TN by 0.27%, when increasing the number of attackers from 2 to 16 for trajectory length of 3. The trajectory length 2 is not sufficient to effectively detect the compromised RSU in SYBIL-CAP. The trajectory length 3 is sufficient to detect the compromised RSU. Increasing the trajectory length more than 3 cannot improve the TN results significantly as depicted in Figure 4.

5.3 False positive (FP) Results

FP rate is analyzed for different vehicle density with various trajectory length limits. The RSUs receive a huge number of verification certificates in a highly congested road, and there is a chance of missing the verification packets due to congestion. As results, a genuine RSU may suspect other genuine RSU to be compromised by an attacker and thus increases the FP rate of SYBIL-CAP. In Figure 5, a maximum number of vehicles 100 within 1.5 x 1.5 km² area, makes the network highly congested, and the FP rate is increased from 8.2% to 10.3% unexpectedly for trajectory length limit 3.

Figure 6 shows the FP rate of SYBIL-CAP for a different number of attackers. Additionally, the plot is varied for various trajectory lengths to the corresponding attack-varying scenario. In SYBIL-CAP, a vehicle confirms the compromised RSU using two pairs of DHKE secret key values. If the trajectory length is two, the vehicle gets only one DHKE secret key pair value and it is not sufficient to confirm the attacker accurately. In Figure 6, FP rate rapidly increases up to 7.8%, when the trajectory length is two. So, SYBIL-CAP improves the detection accuracy by limiting the trajectory length.
Resilient Privacy Preservation Scheme to Detect Sybil Attacks in Vehicular Ad Hoc Networks

5.4 RSU Isolation Delay Results
Figure 7 shows the simulation results of isolation delay of SYBIL-CAP and P2DAP, by varying the vehicle speed from 30m/s to 60m/s. The vehicle speed and RSU communication range adversely affect the RSU isolation delay. In SYBIL-CAP, if a vehicle detects an attacker or a compromised RSU, it needs to send a report message to the other adjacent genuine RSU. The low-speed vehicle reaches the adjacent RSUs eventually, and it increases the compromised RSU isolation delay. In Figure 7, the SYBIL-CAP achieves isolation delay of 10s and 8.75s to vehicle's speed 35m/s and 40m/s respectively for 500 communication range of the RSU.

5.5 Tracking Time Results
It illustrates the comparative results of tracking time of both the SYBIL-CAP and P2DAP systems. The number of RSUs and its communication range markedly affects the tracking time, and 80 vehicles are extreme for 1.5 x1.5 km² area. If the number of vehicles exceeds more than 80 in the same area, the RSUs are a bottleneck due to receiving a high amount of authorized certificate generation and verification request from vehicles. Due to congestion, when a vehicle does not receive a response from the corresponding RSU for its Verification request within a particular period, it has to retransmit the request, in turn, it introduces an additional tracking delay. Also, the distance between two RSUs increases with decreasing communication range of RSUs. According to SYBIL-CAP, the group verification requires extra time due to small interference range among RSUs. Unlike SYBIL-CAP in P2DAP, every message is verified at TCA, which creates an inordinate delay in the network. As a result, the tracking time increases. Moreover, the SYBIL-CAP attains lower delay than P2DAP. The SYBIL-CAP and P2DAP achieve 23.5s and 24.2s of isolation delay respectively to verify authorized certificate of 100 vehicles in the presence of 12 RSUs with 500 communication range (Figure 9).
5.6 Overhead Results
Figure 10 shows the results of the overhead ratio of SYBIL-CAP and P2DAP by varying the RCR for different VD. As per the SYBIL-CAP, the vehicles detected as attacker and compromised RSU by verifying authorized certificate at a group of the three RSUs. If a vehicle detects compromised RSU, the vehicle must report the other adjacent RSU for revoking compromised RSU. The RSU forwards the report to the TCA. A vehicle employs a high number of report packets when the RCR is high. Thus, it increases the additional packet overhead in the network. However, the overhead is not as significant as the vehicles employ a small number of packets to isolate the compromised RSU and attacker, compared to existing P2DAP. In SYBIL-CAP, increasing RCR impacts on overhead to around 0.003.

Figure 11 demonstrates the overhead ratio of SYBIL-CAP and P2DAP systems by varying the RCR from low to high for different vehicle speed (S). Instead of receiving trusted certificate from all RSUs in SYBIL-CAP, the vehicle utilizes the same certificate to a group of three consecutive RSUs. However, if the vehicle’s speed is high, the authorized certificate of a vehicle expires quickly, and it requires a new certificate from RSU immediately. At the same time, the vehicle which detects attacker needs to send a report to TCA via RSU when it detects attacker or compromised RSU in the network. Moreover, it increases the overhead maximum up to 0.0048 for very high-speed vehicles (100m/s) scenario.

6. Conclusion
This paper addresses the location privacy of vehicles and proposes an SYBIL-CAP that incorporates TAP-LOOP and RESUME to detect the Sybil attack. The SYBIL-CAP prevents vehicle’s location privacy at all times using TAP-LOOP. In TAP-LOOP, the vehicle’s unique identity is concealed by providing a temporarily trusted certificate. The RESUME implements a DHKE algorithm among RSUs for detecting attacker and compromised RSU. In SYBIL-CAP, RSU is responsible for verifying authorized certificates, thus reducing the overhead complexity on TCA. Also, the SYBIL-CAP employs an optimal deployment method to deploy RSUs where the only less number of RSUs cover the maximum service area. The effective simulation results demonstrate that the SYBIL-CAP can largely restrict Sybil attack and also improve the privacy of vehicles, compared to existing P2DAP. Moreover, the SYBIL-CAP improves the detection accuracy up to 94% more than that of P2DAP.

7. References
1. Lin X, Lu R, Zhang C, Zhu H, Ho PH, Shen X. Security in vehicular ad hoc networks. Institute of Electrical and Electronics Engineers (IEEE) Communications Magazine. 2008; 46(4):88–95.
2. Eriksson J, Girod L, Hull B, Newton R, Madden S, Balkrishnan H. The pothole patrol: using a mobile sensor net-
work for road surface monitoring. In Proceeding of the 6th International Conference on Mobile Systems Association for Computing Machinery (ACM), USA; 2008. p. 29–39.

3. Elsadig MA, Fadlalla YA. VANETs security issues and challenges: a survey. Indian Journal of Science and Technology. 2016 Jul; 9(28):1–8.

4. Yadav KA, Vijayakumar P. VANET and its security aspects: a review. Indian Journal of Science and Technology. 2016 Nov; 9(44):1–16.

5. Zarki ME, Mehrotra S, Tsudik G, Venkatasubramanian N. Security issues in a future vehicular network. In European Wireless (EuroWireless). 2002; 2:5–7.

6. Sampigethaya K, Huang L, Li M, Poovendran R, Matsuuraka K, Sezaki K. CARAVAN: Providing location privacy for VANET. In Embedded Security in Cars (ESCAR) Workshop; 2005.

7. Choi JY, Jakobsson M, Wetzel S. Balancing auditability and privacy in vehicular networks. In Proceedings of the 1st Association for Computing Machinery (ACM) International Workshop on Quality of Service and Security in Wireless and Mobile Networks, Montreal, Quebec, Canada; 2005 Oct 13. p. 79–87.

8. Calandriello G, Papadimitratos P, Lioy A, Hubaux JP. Efficient and robust pseudonymous authentication in VANET. In the Proceedings of Association for Computing Machinery (ACM) International Workshop on Vehicular Inter-NETworking (VANET), Montreal, Quebec, Canada; 2007 Sep 10. p. 19–28.

9. Rass S, Fuchs S, Schaffer M, Kyamakya K. How to protect privacy in floating car data systems. In the Proceedings of Association for Computing Machinery (ACM) International Workshop on Vehicular Inter-NETworking (VANET), San Francisco, California, USA; 2008 Sep 15. p. 17–22.

10. Parno B, Perrig A. Challenges in securing vehicular networks. In the Fourth Workshop on Hot Topics in Networks (HotNets-IV); 2005. p. 1–6.

11. Studer A, Shi E, Bai F, Perrig A. Tackling together efficient authentication, revocation, and privacy in VANEts. In the 6th Annual Institute of Electrical and Electronics Engineers (IEEE) Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks; 2009 Jun. p. 1–9.

12. Raya M, Hubaux JP. The security of vehicular ad hoc networks. In Proceedings of the 3rd Conference for Computing Machinery (ACM) workshop on Security of ad hoc and sensor networks, Alexandria, VA, USA; 2005 Nov 7. p. 11–21.

13. Julien F, Raya M, Felegyhazi M, Papadimitratos P. Mixzones for location privacy in vehicular networks. In Association for Computing Machinery (ACM) Workshop on Wireless Networking for Intelligent Transportation Systems (Win-ITS); 2007.

14. Sampigethaya K, Li M, Huang L, Poovendran R. AMOeba: Robust location privacy scheme for VANET. Institute of Electrical and Electronics Engineers (IEEE) Journal on Selected Areas in Communications. 2007 Oct; 25(8):1569–89.

15. Song JH, Wong VWS, Leung VCM. Wireless location privacy protection in vehicular ad-hoc networks. Mobile Networks and Applications. 2010 Feb; 15(1):160–71.

16. Lu R, Lin X, Luan TH, Liang X, Shen X. Pseudonym changing at social spots: an effective strategy for location privacy in VANETs. Institute of Electrical and Electronics Engineers (IEEE) Transactions on Vehicular Technology. 2012; 61(1):86–96.

17. Bjørn W, Zhendong M, Frank K, Papadimitratos P. Privacy in inter-vehicular networks: Why simple pseudonym change is not enough. In Wireless On-demand Network Systems and Services (WONS) Seventh International Conference Institute of Electrical and Electronics Engineers (IEEE); 2010 Feb. p. 176–83.

18. Matthias G, Guttler F. Privacy in VANETs using changing pseudonyms-ideal and real. In 65th Vehicular Technology Conference (VTC) Spring, Institute of Electrical and Electronics Engineers (IEEE); 2007. p. 2521–5.

19. Liao J, Li J. Effectively changing pseudonyms for privacy protection in VANETs. In the 10th International Symposium Pervasive Systems, Algorithms, and Networks (ISPAN) Institute of Electrical and Electronics Engineers (IEEE); 2009 Dec. p. 648–52.

20. Shi X, Xu H. An effective scheme for location privacy in VANETs. Journal of Networks. 2014; 9(8):2239–44.

21. Zhou T, Choudhury RR, Ning P, Chakrabarty K. P2DAP-sybil attacks detection in vehicular ad hoc networks. Institute of Electrical and Electronics Engineers (IEEE) Journal on Selected Areas in Communications. 2011; 29(3):582–94.

22. Wu Q, Ferrer JD, Nicolas UG. Balanced trustworthiness, safety and privacy in vehicle-to-vehicle communications. Institute of Electrical and Electronics Engineers (IEEE) Transaction on Vehicular Technology. 2010; 59(2):559–73.

23. Chen C, Wang X, Han W, Zang B. A robust detection of the Sybil attack in urban VANETs. In the Proceedings of Institute of Electrical and Electronics Engineers (IEEE) International Conference Distributed Computing Systems Workshops (ICDCSW); 2009. p. 270–6.

24. Chen L, Ng SL, Wang G. Threshold anonymous announcement in VANETs. Institute of Electrical and Electronics Engineers (IEEE) Journal on Selected Areas in Communication. 2011; 29(3):1–11.

25. Park S, Aslam B, Turgut D, Zou CC. Defense against Sybil attack in vehicular ad hoc network based on roadside unit support. In the Proceedings of 28th Institute of Electrical and Electronics Engineers (IEEE) Conference on Military Communication (MILCOM); 2009. p. 1–7.

26. Chang S, Qi Y, Zhu H, Zhao J, Shen X. Footprint: detecting Sybil attacks in urban vehicular networks. Institute of Electrical and Electronics Engineers (IEEE) Transactions on Parallel and Distributed Systems. 2012; 23(6):1101–14.

27. Zhou T, Choudhury RR, Ning P, Chakrabarty K. P2DAP-Sybil attacks detection in vehicular ad hoc networks. Institute of Electrical and Electronics Engineers (IEEE) Journal on Selected Areas in Communications. 2011; 29(3):582–94.