The Journal of Supercomputing (2023) 79:2153–2179
https://doi.org/10.1007/s11227-022-04736-5

VANET authentication protocols: security analysis and a proposal

Otto B. Piramuthu[1] · **Matthew Caesar**[1]

Accepted: 16 July 2022 / Published online: 7 August 2022

Abstract
Wireless communication among vehicular ad hoc network (VANET) entities is secured through cryptography, which is used for authentication as well as to ensure the overall security of messages in this environment. Authentication protocols play a significant role and are therefore required to be free of vulnerabilities that allow entity impersonation, unauthorized entry, and general misuse of the system. A resourceful adversary can inflict serious damage to VANET systems through such vulnerabilities. We consider several VANET authentication protocols in the literature and identify vulnerabilities. In addition to the commonly considered vulnerabilities in VANETs, we observe that the often-overlooked relay attack is possible in almost all VANET authentication protocols. Relay attacks have the potential to cause damage in VANETs through misrepresentation of vehicle identity, telematic data, traffic-related warnings, and information related to overall safety in such networks. We discuss possible countermeasures to address identified vulnerabilities. We then develop an authentication protocol that uses ambient conditions to secure against relay attacks and other considered vulnerabilities. We include security proof for the proposed protocol.

Keywords VANET · Authentication · Vulnerabilities

1 Introduction

Vehicular ad hoc networks (VANETs) help vehicles safely navigate through accident avoidance, blindspot awareness, other road hazards, and timely dissemination of emergency information. Typical VANETs include vehicles, roadside units (RSU), and trusted (TA) or certification (CA) authorities. Communication between any two vehicles or vehicle and RSU occurs through wireless network technology [1] such

✉ Otto B. Piramuthu
obp2@illinois.edu

[1] Computer Science, University of Illinois at Urbana-Champaign, Urbana, IL 61801, USA

as short-range radio like wireless local area network (WLAN) that includes Wi-Fi and ZigBee, cellular technologies such as long-term evolution (LTE) or visible light communication (VLC). Each vehicle is equipped with an on-board unit (OBU) for secure communication with other entities. In general, communication between RSU and TA/CA occurs through wired means as these entities are often stationary.

Given the dynamic network topology, the large number of nodes (vehicles), and frequent switching among RSUs, it is possible for malicious adversaries to disseminate false information, modify or drop messages, as well as impersonate vehicles or RSUs. Such attacks have the potential to harm or compromise the system [2–6]. For example, a malicious vehicle can impersonate an emergency vehicle such as an ambulance to gain fast access to roadways or send fake accident messages to redirect traffic. Another example is that of a scenario [7] in which an adversary creates several counterfeit identities that are then used to disseminate false status messages claiming that these identities represent slow-moving or stationary vehicles. With the perception of an impending traffic jam, other vehicles are bound to avoid this fake congested route, thereby creating a congestion-free route for the attacker. Attackers can also flood an RSU with a large number of messages. This renders the RSU temporarily unavailable for other purposes, such as attend to a request from another RSU to disseminate information about an accident to vehicles in its monitored control area [8]. These illustrate the deleterious effects of attacks on VANETs.

Wireless communication interfaces such as those in vehicular OBUs can be used as attack vectors to gain wireless access to intra-vehicular communication networks such as CAN (controller area network). Attacks on CAN through Bluetooth, infotainment, telematics, tire sensor, among others have been used to take control of various functions (e.g., display, brakes, acceleration, steering, climate control) of the attacked vehicle [9] [10] [11] [12] [13]. An adversary with only modest resources has the potential to launch a massive attack on VANETs to cause property damage and thousands of fatalities as well as disrupt transportation [14]. This problem is bound to get worse as more and more connected vehicles are introduced in our roadways, disregarding associated vulnerabilities.

With the highly dynamic nature of vehicles and the sheer number of vehicles in VANETs, it is a challenge to ensure the truthfulness of passed messages and to maintain the security and privacy of each vehicle [15]. Messages in VANETs need to be secured and vulnerabilities must be identified and rectified before damage is done. A step in this direction is to ensure that all vehicles and RSUs are authenticated [16]. It is therefore imperative to ensure the absence of vulnerabilities in VANET authentication protocols to secure VANET systems against malicious adversaries and to facilitate the design and implementation of secure protocols. To this end, our contribution is threefold: we (a) critically evaluate several recently published VANET authentication protocols and identify vulnerabilities, (b) suggest possible countermeasures when appropriate, and (c) develop a secure authentication protocol against relay attacks.

As background for the remainder of the paper, we list and discuss common attacks in VANETs along with related implications in Sect. 2. We also consider these from the perspective of security and privacy in VANETs, with specific focus on vulnerabilities and related attacks. In Sect. 3, we discuss security analysis on

several VANET protocols. We then present and critically evaluate our protocol in Sect. 4. We conclude the paper with a brief discussion on the identified vulnerabilities, their characteristics, and what could be done to protect against such vulnerabilities in Sects. 5 and 6.

2 VANET attacks and related implications

Message-based attacks on VANET nodes that comprise vehicles, RSUs, and trusted authority can be classified based on the attacker's model [17]. This includes attacks from inside (e.g., authenticated member) vs. outside (e.g., intruder) the VANET, malicious (e.g., with personal profit not as a motive) vs. rational (e.g., personal profit as motive), active (e.g., message modification) vs. passive (e.g., eavesdropping), and local (limited scope) vs. extended (larger scope across the network). Raya and Hubaux [17] also identify several potential attacks in VANETs such as the dissemination of bogus information that affect the behavior of other drivers, cheating with sensor (e.g., speed, location, direction) information, track and trace vehicles, denial of service (DoS), and impersonation (masquerading) attacks. VANETs also face the possibility of replay and relay attacks.

An inside attack is mounted by a trusted [18] VANET node (e.g., vehicle, RSU) that goes rogue or colludes with other nodes whereas an outside attack is by an entity that is not a trusted VANET node. Active attacks generally require resourceful adversaries as messages are often captured, modified, and then transmitted by the adversary to the intended recipient. Passive attacks do not require much effort for the adversary as these primarily involve eavesdropping on passed messages.

An adversary can disseminate bogus information with knowledge of information necessary to transmit messages to other nodes. Such knowledge can be gained, for example, through passive or active attacks. Similarly, transmission of incorrect or fake sensor values is also possible. Tracking and tracing of vehicles generally occur through knowledge of information that identifies a specific vehicle. Such identification information should therefore not be transmitted in the open for fear of unintended recipients. DoS attacks can occur during key updates, for example, on one side and not the other between two communicating parties, resulting in desynchronization when a party fails to recognize message from the other. Impersonation attacks are serious since they allow an adversary to successfully represent a node to others. Replay attacks allow an adversary to observe communication between nodes, capture messages, and replay the messages at a later point in time, to be accepted as valid by the recipient. Relay attacks [19] are difficult to identify or control since the adversary simply relays (unmodified) messages between parties. Relay attack allows an adversary to falsify distance information between communicating parties. For example, an adversary can relay messages between a vehicle and another vehicle or RSU that are farther apart to prove that the first vehicle is indeed near the other vehicle or RSU. Distance falsification has the potential to virtually insert a vehicle in an area where it is not actually present to generate the illusion of heavy traffic, report an incident from elsewhere by virtually shifting its location, mount attacks from far away, and avoid being observed or caught, among others. Any of these can result in

deleterious consequences. Clearly, any of these vulnerabilities has the potential to violate the security or privacy implications of the *victim* node. In Sect. 3, we critically evaluate VANET authentication protocols for the vulnerabilities mentioned above.

3 VANET authentication protocols & vulnerabilities

The notation used in the rest of this paper follows.

AID_i, PID_i	Anonymous or pseudo identity of vehicle or RSU i
$AID_{i,j}$, $PID_{i,j}$	The two parts of AID_i, PID_i ($j = 1, 2$)
C, R	Challenge and response pair
e	Bilinear map
E_k, D_k	Encrypt, decrypt with k
f_i	Polynomial index
$f(x, y)$	Bivariate polynomial with x, y as input
GK_p, GK_s	Group key of primary, secondary user
$H(.), H_2(.), H_3(.), h_i(.)$	Hash functions (ith hash function)
HC	Hash code
ID_v, ID_{RSU}, ID_{TA}	Identity of vehicle, RSU, TA
K_v, K_{RSU}, K_j, K_k	Session keys for vehicle, RSU, RSUs j and k
KV_i	Key value corresponding to f_i
loc_i	Location of vehicle i
M_i, M_j, M_k, M_{req}, M_{res}	Message from i, j, and k; request and response
P, Q, g	Generators of cyclic group $\mathbb{G}$
PEn_k	Public key encryption algorithm with key k
PK_v, PK_{RSU}, PK_i	Public key of vehicle, RSU, and entity i
PSK_i	Partial secret key of vehicle i
P_{pub}	Public key of trusted authority (TA)
PWD	Tamper-proof device password
q	A large prime number and order of elliptic curve
r, r_1, r_2, r_i	Random number
RID, RID_j	Real identity of vehicle (j)
Sig_k	Signature with key k
SK_v, SK_{RSU}, SK_{TA}	Secret (private) key of vehicle, RSU, and TA
T_i	Timestamp sequence i or from entity i
x	Private master key of trusted authority
A_i	Ambient condition at entity i
$\oplus$, $\|$	Exclusive-OR, concatenation operator

In the remainder of this section, we present a sketch of the authentication protocols and then identify vulnerabilities in the considered protocols. We do not attempt to patch the vulnerabilities that we identify since a patch in one part might create other vulnerabilities. Such an endeavor generally requires redesigning the protocol

from the ground-up which is out of scope for this paper. We discuss possible countermeasures in Sects. 5 and 6. Due to space considerations, we provide just enough detail on the authentication protocols for the reader to understand the same and the identified vulnerabilities. The interested reader is referred to the source publications for detailed information. The time-to-live (TTL) for each message in the protocols is just that authentication round. We list the protocols in increasing order of the first author names.

3.1 Hybrid signcryption scheme

Ali et al. [20] develop a conditional privacy-preserving hybrid signcryption (CPP-HSC) scheme that involves a sender vehicle and a receiver vehicle or RSU (Fig. 1). Note that the terms presented here correspond to the sender vehicle (V_i) and receiver vehicle (V_j). For RSU as the receiver of the message, V_j's values can be switched with the ones corresponding to RSU and the vulnerabilities remain the same.

An adversary can passively observe the message from the sender vehicle to the receiver vehicle and copy all the messages that are passed. The adversary can then use this copied information to decipher the entire set of terms (i.e., full-disclosure attack) used by V_i (the sender vehicle) as follows. The public key of the receiver vehicle (PK_{v_2}) and S_i are known to the adversary, and the nonce r_i can therefore be readily determined. Since χ_i is g^{r_i}, M_i can be determined from $\kappa_i \leftarrow M_i \oplus h_3(\chi_i)$. Now, the entire π_i ($= h_2(M_i||PID_i||PK_{v_i}||\chi_i||P_{pub})$) is known to the adversary since M_i and χ_i were just determined, h_2 is public information, PID_i is sent from sender vehicle in the open, PK_{v_i} and P_{pub} are both public keys and are therefore public information. Next, in U_i ($= \frac{r_i}{\pi_i SK_{v_i}} P$), all but SK_{v_i} (the private key of the sender vehicle) are known and SK_{v_i} can therefore be determined by the adversary. Now, the adversary has all the information necessary to generate a message (M'), include the appropriate time stamp (T_i), and send ($\kappa_i, U_i, S_i, T_i, PID_i$) to the receiving vehicle or

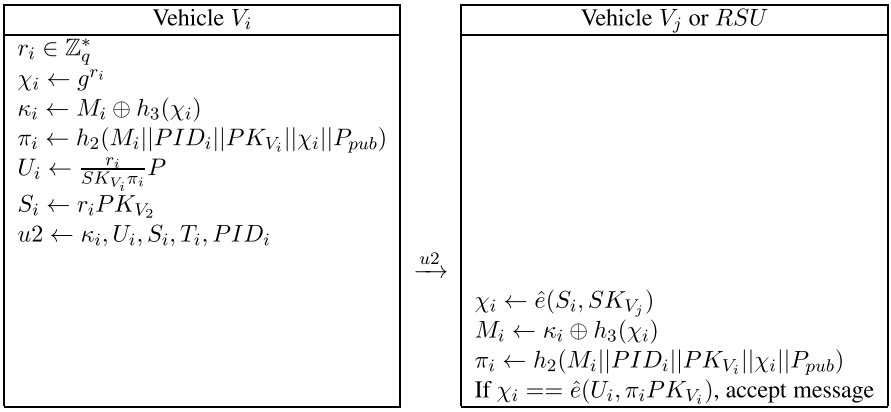

Fig. 1 CPP-HSC scheme [Ali et al. 20]

RSU for acceptance. Moreover, since the message from vehicle V_i does not include anything on other vehicles or RSU, an adversary can successfully relay the message from V_i to some other RSU and its associated vehicles for a relay attack.

3.2 Privacy-preserving authentication

Ali et al. [21] include several phases as parts of their privacy-preserving authentication protocol between two vehicles (V_i and V_j). We consider the ones in which the messages are sent through wireless means. Specifically, we consider SPKGen, CLSGen, and CLSVerify (Fig. 2).

Vehicle V_i		Vehicle V_j
SPKGen receive AID_i, PSK_i (from PSKGen) $U_i \leftarrow r_i P$ $\theta_i \leftarrow H_1(AID_i, U_i, P_{pub})$ if $\lambda_i P == U_i + \theta_i P_{pub}$ continue $\mu_i \in \mathbb{Z}_q^*$ $SK_i \leftarrow \{\mu_i, \lambda_i\}$ $X_i \leftarrow \mu_i P_{pub}$ $Y_i \leftarrow \lambda P_{pub}$ $PK_i \leftarrow \{X_i + Y_i\}$	$\xrightarrow{PK_i}$	
CLSGen receive safety message M_i from nearby vehicle or sensor $a_i \in \mathbb{Z}_q^*$ $A_i \leftarrow r_i P_{pub}$ $\delta_i \leftarrow H_2(M_i, AID_i, PK_i, A_i, P_{pub})$ $\eta_i \leftarrow \delta_i(r_i + \mu_i + \lambda_i) \bmod q$ $\Theta_i \leftarrow \{\eta_i, A_i\}$ $u3 \leftarrow M_i, AID_i, PK_i, \Theta_i, t_i$	$\xrightarrow{u3}$	**CLSVerify** continue if timestamps (t_i, T_i) are fresh $\delta_i \leftarrow H_2(M_i, AID_i, PK_i, A_i, P_{pub})$ accept M_i if Θ_i is valid Θ_i is valid if $\eta_i P_{pub} == \delta_i(A_i + PK_i)$

Fig. 2 SPKGen, CLSGen, and CLSVerify [Ali et al. 21]

An adversary that passively observes the messages in SPKGen, CLSGen, and CLSVerify protocols (Fig. 2) gains knowledge of PK_i (the public key of vehicle V_i) and AID_i (the anonymous identity of vehicle V_i). Now, the adversary can generate a nonce r_i and then the corresponding A_i ($= r_i P_{pub}$) since P_{pub} (a public key) is known to the adversary. Next, the adversary can generate a new message M_i, which could be anything of the adversary's choice. The adversary can now generate δ ($= H_2(M_i, AID_i, PK_i, A_i, P_{pub})$) since H_2 and the rest of the terms are known to the adversary. Since $\eta_i P_{pub} == \delta_i(A_i + PK_i)$ (as per the last check in Fig. 2) and the right hand side of this expression is known to the adversary, η_i can be determined as P_{pub} in the left hand side is known to the adversary. With the above, the adversary can generate the message from V_i to V_j ($\{M_i, AID_i, PK_i, \Theta_i, t_i\}$). As AID_i is $\{AID_{i,1}, AID_{i,2}, T_i\}$ and neither $AID_{i,1}$ nor $AID_{i,2}$ incorporate T_i, T_i can be modified to any value that the adversary wants. Similarly, t_i can be modified to any value chosen by the adversary. So, the adversary can generate and broadcast any message of its choice to neighboring vehicles.

These protocols are also vulnerable to relay attacks since neither of the two messages from vehicle V_i has information on V_j or the nearby RSU. Therefore, an adversary can relay the messages from V_i to other vehicles that are not necessarily in physical proximity of V_i.

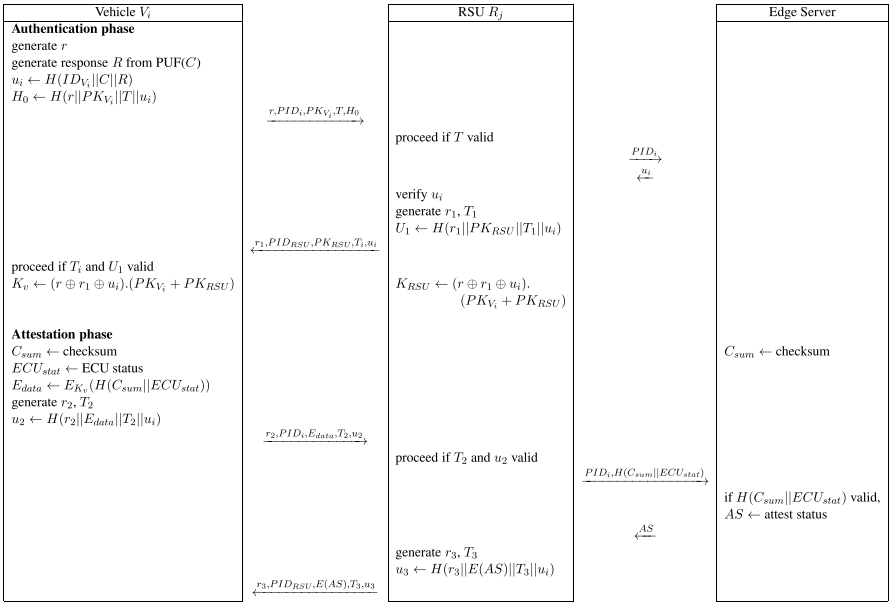

Fig. 3 Authentication and attestation protocol [Alladi et al. 22]

3.3 Authentication and attestation scheme

Alladi et al. [22] propose an authentication and attestation scheme (Fig. 3) with vehicle V_i, RSU R_j, and an edge server. The authentication part is followed by the attestation part. This protocol is vulnerable to relay attack as the messages generated by the vehicle V_i can be easily relayed by an adversary to any other RSU since these messages are not specifically targeted to a given RSU. The adversary can use this method on any vehicle that is broadcasting a message to any other RSU to get authenticated and attested by any RSU.

3.4 Secure and efficient authentication

Asaar et al. [23] identify vulnerabilities in the proxy-based authentication scheme (PBAS) proposed in Liu et al. [24] and then propose an identity-based message authentication scheme using proxy vehicles (ID-MAP) that is claimed to be secure and efficient. However, we identify vulnerabilities in ID-MAP that an adversary can take advantage of to compromise the system.

The proposed ID-MAP authentication scheme comprises five phases that include setup, anonymous identity generation, message generation, verification of messages by proxy vehicles, and verification of proxy vehicles' output by RSUs. We identify vulnerabilities in the anonymous identity generation, message generation, and

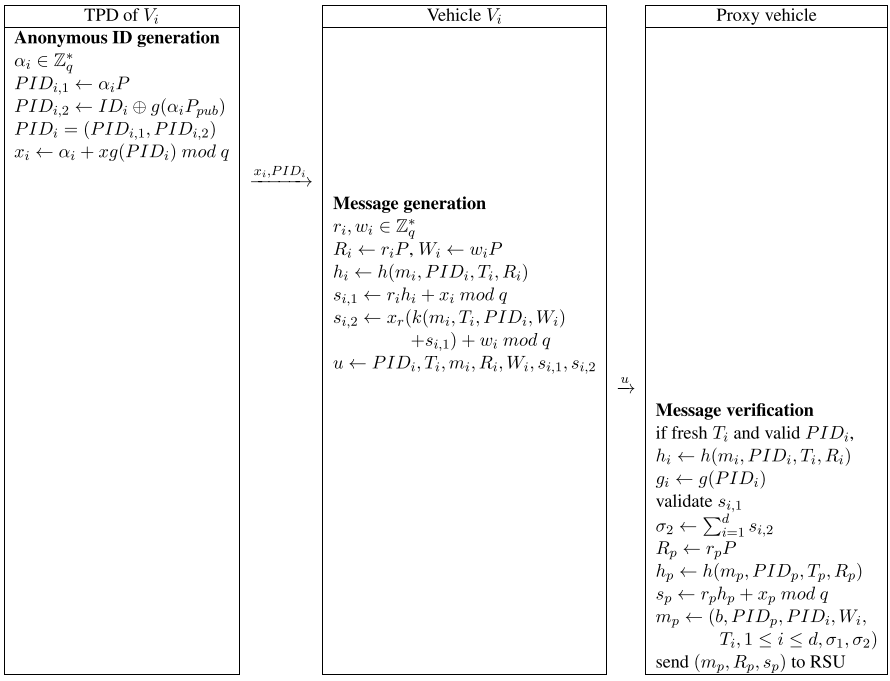

Fig. 4 Authentication protocol [Assar et al. 2018]

verification of messages by proxy vehicles phases. Fig. 4 includes a sketch of these with the tamper-proof device (TPD) of vehicle V_i, V_i, and proxy vehicles.

The vehicle's secret key x_i generated during the anonymous identity generation phase can be determined by the adversary as follows. x_i is given by $\alpha_i + xg(PID_i)\ mod\ q$. The adversary multiplies both sides by P, which is a public parameter and the generator of the group $\mathbb{G}$. Now, the adversary has $x_iP = P\alpha_i + Pxg(PID_i)\ mod\ q$, which is the same as $x_iP = PID_{i,1} + P_{pub}g(PID_i)\ mod\ q$. The right hand side and P are known to the adversary. The adversary can therefore determine x_i.

In the message generation phase, $s_{i,2} = x_r(k(m_i, T_i, PID_i, W_i) + s_{i,1}) + w_i\ mod\ q$ is generated and $(PID_i, T_i, m_i, R_i, W_i, s_{i,1}, s_{i,2})$ is sent to the proxy vehicle. In $s_{i,2}$, the only unknowns are x_r and w_i. Multiplying both sides by P, w_i becomes w_iP, which is the same as the known W_i. Now, the only unknown (x_r) can be determined by the adversary. Once x_r is known, the entire message that is sent to the proxy vehicles can be generated by the adversary with randomly generated r_i and w_i for the next authentication round. Note that r_i and w_i are randomly chosen and an adversary can generate these as well. Then, R_i $(= r_iP)$ is known, W_i $(= w_iP)$ is known, and $h_i = h(m_i, PID_i, T_i, R_i)$ is also known since m_i and T_i can be generated by the adversary. With h_i, x_i, r_i, and q, $s_{i,1}$ can be determined.

The message sent from the proxy vehicle to RSU is: $(b, PID_p, PID_i, W_i, T_i, 1 \le i \le d, \sigma_1, \sigma_2, R_p, s_p)$. Here, σ_1 $(= \sum_{i=1}^{d} s_{i,1})$ and σ_2 $(= \sum_{i=1}^{d} s_{i,2})$ can be determined by the adversary as the d values can be gathered through passive listening of the messages that reach the proxy vehicle. As R_p is fixed, the adversary can copy this through passive observation of message from proxy vehicle to RSU. In the future, the adversary can easily generate the entire message from proxy vehicle to RSU except s_p.

The adversary can do the following to determine s_p. It is known that $R_p = r_pP$, $h_p = h(m_p, PID_p, T_p, R_p)$, and $s_p = r_ph_p + x_p\ mod\ q$. All the elements that make up h_p are known to the adversary. To determine s_p, the adversary needs to know x_p. To accomplish this, the adversary can multiply both sides of the s_p expression by P to get $Ps_p = Pr_ph_p + Px_p\ mod\ q$. Now, the left hand side is known. The right hand side is $R_ph_p + x_pP\ mod\ q$. The only term that is unknown to the adversary in the expression is x_p, which can now be determined. With this knowledge, in the future, the adversary can readily create the message to be sent from the proxy vehicle to RSU.

As none of the messages are specific to any other vehicle or any RSU, these can be successfully relayed by an adversary to other vehicles in any RSU's field to mount a relay attack.

3.5 Privacy-preserving scheme

Azees et al. [25] propose an efficient anonymous authentication scheme with conditional privacy preserving (EAAP) for VANETs. EAAP comprises three components that include system initialization, anonymous authentication of a vehicle, and anonymous authentication of an RSU. We consider the anonymous authentication of

a vehicle since it involves communication between a vehicle and TA through wireless means. This component consists of five stages that include registration and key generation, anonymous certificate generation, signature generation, verification, and conditional tracking. We consider the second, third, and fourth stages and identify vulnerabilities.

The trusted authority (TA) generates $a, b, n_i, v_i \in \mathbb{Z}_q^*$,and publishes the system parameters $(q, e, g_1, g_2, G_1, G_2, G_T, A_1, B_1, H)$. It then generates $E_i \leftarrow g_1^{-n_i} \; mod \; 1$, $T_i \leftarrow g_1^{\frac{1}{v_i+a+b}}$, and $DID_{u_i} \leftarrow g_1^{n_i+a} mod \; q$ and places these in the smartcard of the vehicle's secure device.

An adversary can determine the entire set of values in Fig. 5 through passive observation of the message from the vehicle to the trusted authority (TA) as follows. First, the adversary can use γ_U from $Cert_k$ to determine r since B_1 is known to the adversary. Next, the adversary can determine T_i from γ_V as A_1 and r are known. Since this involves a dot product, the adversary may have to observe repeated such messages from the vehicle to TA to accomplish this. However, it is easier for the adversary to disregard T_i and directly generate γ_V from λ_2 as the rest of the terms in $\lambda_2 \leftarrow \frac{\gamma_U^{r+r_1}}{\gamma_V^{r+r_2}}$ are known to the adversary as is shown below. Even otherwise, the adversary can keep the same γ_V (and, therefore, the same r) in all future messages to TAs. This is not an issue as the rest of the random numbers (r_k, r_1, r_2) are readily generated by the adversary to provide enough variations in

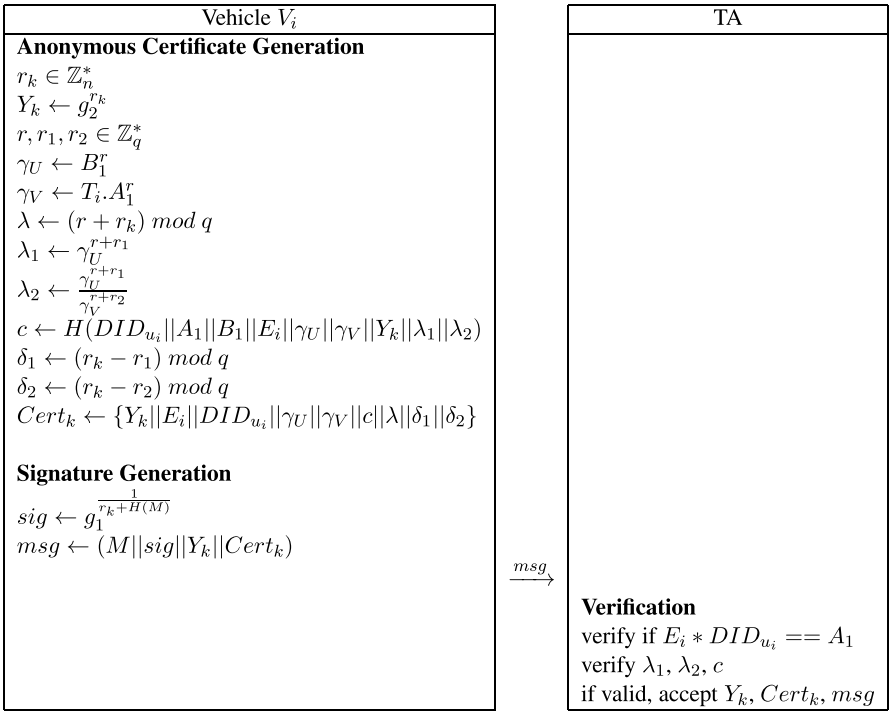

Fig. 5 Anonymous authentication stages [Azees et al. 2017]

msg. From $\lambda = (r + r_k)\ mod\ q$, the adversary can determine r_k, which is the only unknown. With knowledge of δ_1 and δ_2, r_1 and r_2 can be determined. With this knowledge, the adversary can generate λ_1 and λ_2. The adversary can copy $Cert_k$ to generate c for the next authentication round. The adversary can also generate *sig* by now. With the above knowledge, the adversary can easily generate a new *msg* that is acceptable at any new *TA* region it visits next.

An adversary can easily mount a relay attack in this system since none of the messages encode information on a specific RSU or specific other vehicles.

3.6 Blockchain-assisted authentication

Feng et al. [26] propose blockchain-assisted [27] privacy-preserving authentication system (BPAS), which comprises five modules that include system initialization, smart contract deployment, vehicle registration, login and message authentication, and vehicle revocation. Among these modules, the first three (system initialization, smart contract deployment, and vehicle registration) and last (vehicle revocation) are accomplished either within the trusted authority or through secure channels between entities. The fourth module (login and message authentication) is the only one that involves message broadcasting among a vehicle, its on-board unit (OBU), nearby RSUs, and nearby vehicles. We therefore consider only login and message authentication (Fig. 6) and identify a vulnerability. *BiO* is a biometric sample and σ is a deterministic retrieve function with inputs of a biometric sample and a public string (ρ).

An adversary can passively observe the message from the OBU to nearby RSUs and vehicles and record $(\Upsilon, M, R, T_1, \omega)$. Here, Υ and SK_V are constant. Among the inputs to α, the adversary can generate new T_i and M and then pick an r such that α is the same as what was observed earlier. Now, the adversary can update ω with the new r value and send $\{\Upsilon, M, R, T_1, \omega\}$ to nearby RSUs and vehicles for successful reception of the adversary-generated message M.

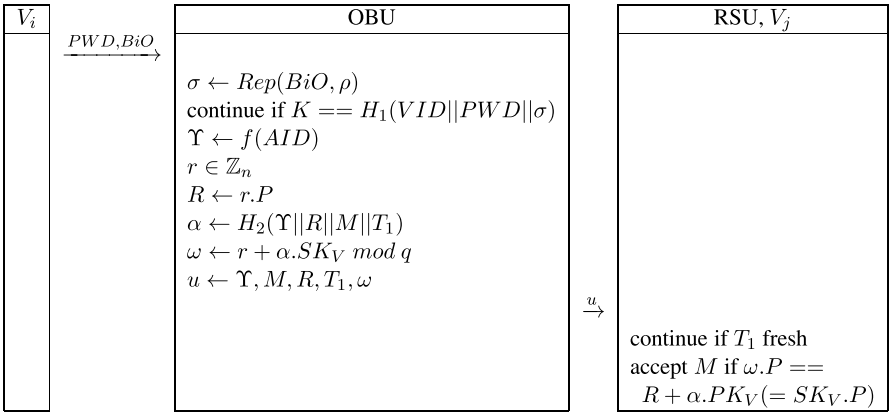

Fig. 6 BPAS authentication protocol [Feng et al. 2020]

As Υ is fixed for each vehicle, an adversary can use this information to track and trace a vehicle. Moreover, as none of the messages from the vehicle or OBU encodes information on any specific RSU or other vehicles, an adversary can successfully relay these messages to any other RSU or vehicles.

3.7 Identity-based authentication

He et al. [28] develop an identity-based authentication protocol that involves the tamper-proof device (TPD) of a vehicle (V_i), the vehicle itself (i.e., V_i), and *RSU* as well as other vehicles (Fig. 7). Note that $AID_i = \{AID_{i,1}, AID_{i,2}\}$.

An adversary can passively observe a broadcast (i.e., $M_i, AID_i, T_i, R_i, \sigma_i$) from a vehicle to nearby vehicles and RSUs to determine the vehicle's *RID* as follows. $AID_{i,2} = RID \oplus h_1(w_i.P_{pub})$. Multiplying $w_i.P_{pub}$ by P, we get $P(w_i.P_{pub})$, which is the same as $(Pw_i).P_{pub}$ (i.e., $AID_{i,1}.P_{pub}$) since dot product is homogeneous under scaling in each variable. Dividing this by P, we get $(w_i.P_{pub}) = (AID_{i,1}.P_{pub})/P$. Now, $AID_{i,2} = RID \oplus h_1((AID_{i,1}.P_{pub})/P)$. *RID* can be determined from this expression as it is the only unknown to the adversary. Moreover, $w_i = AID_{i,1}/P$. As $sk_i = w_i + \alpha_i.x \; mod \; q$, we know $sk_i - w_i = \alpha_i.x \; mod \; q$. The left hand side of this expression is known to the adversary. For the right hand side, α_i is known and $x \; mod \; q$ is the only unknown. So, x can be determined by the adversary in the number of authentication rounds equal to at most the length of the vector x (in binary form). Since the secrets (*RID*, x) are now known, the adversary can pick random

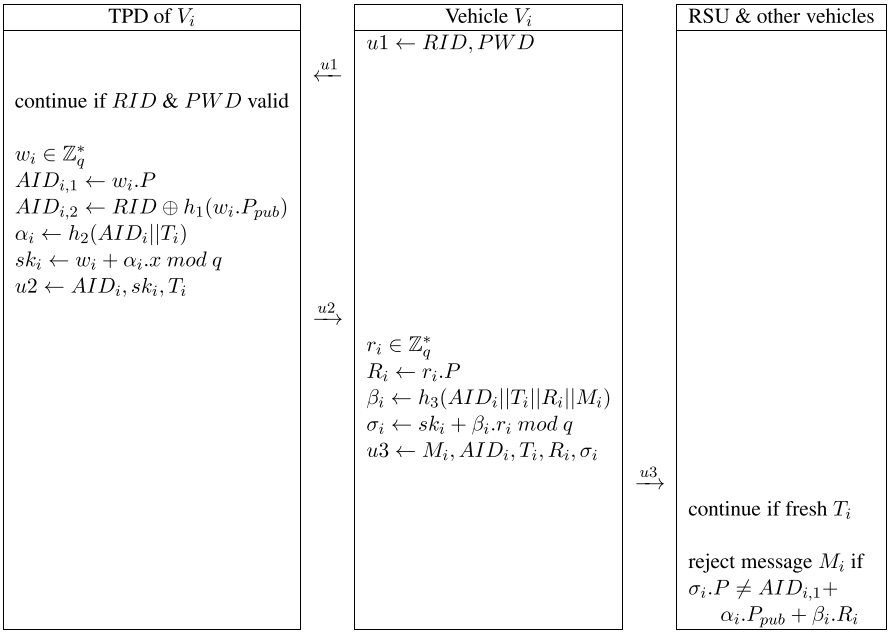

Fig. 7 Identity-based authentication protocol [He et al.28]

$w_i, r_i \in \mathbb{Z}_q^*$ and compute $AID_{i,1}$, $AID_{i,2}$, α_i, sk_i, R_i, β_i, and σ_i. The adversary is now able to send any message M_i to nearby RSUs and vehicles.

The message from vehicle V_i to other vehicles and RSU does not encode nor target a specific RSU or a specific set of vehicles. Therefore, this protocol is vulnerable to relay attack by an adversary whereby the message can be relayed to any other RSU or any other set of vehicles.

3.8 Key management with blockchain

The modeled system (Fig. 8) consists of a vehicle and the BN (blockchain network) node. We consider the authentication and key agreement protocols and identify vulnerabilities in both.

SK_v is sent in the open from the vehicle. And, SK_{RSU} is also broadcast as per the following statement. "Step 1: First, the vehicle V can get the RSUs key value KV_{RSU} [here, SK_{RSU}] and the public key $PubK_{RSU}$ through the broadcast message from the RSU" (*Authentication Phase* p.5840 [29])

The identifiers (ID_v, ID_{RSU}) of both vehicle and BN Node are broadcast in the open. While the consequences of this public information may not be bad for the BN Node, the vehicle could potentially be exposed to privacy and security violations.

The signed parts of messages from vehicle to BN Node and vice versa are decrypted through the public keys of the other entity. As the public keys are, by their nature, public, an adversary can decrypt these (S_1, S_2) messages and retrieve their content. Based on this, K_{RSU} and K_v are known to the adversary. An adversary can use the predictable/constant information across authentication rounds to track and trace the vehicle.

In Fig. 9, the random number r is stated in [29] to be generated by the vehicle and is first used by the BN Node. However, it is not clear how the BN Node knows the value of r. Here, (f_i, KV_i) is a polynomial that is randomly selected from the

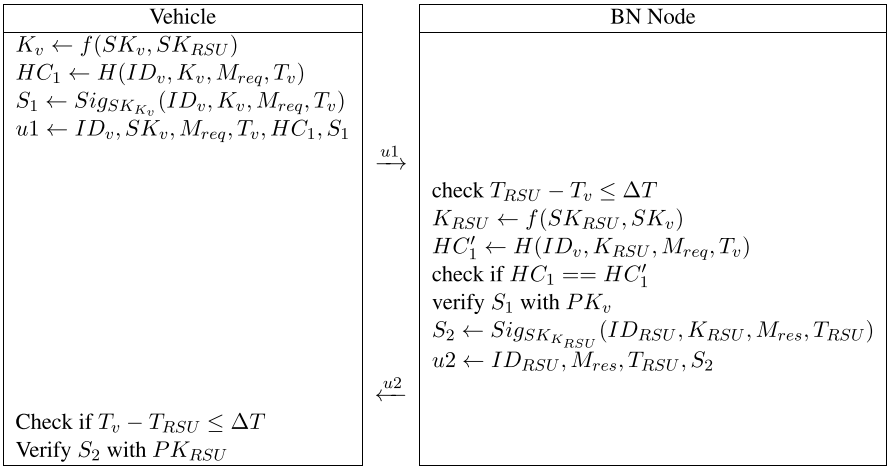

Fig. 8 Authentication protocol [Ma et al. 2017]

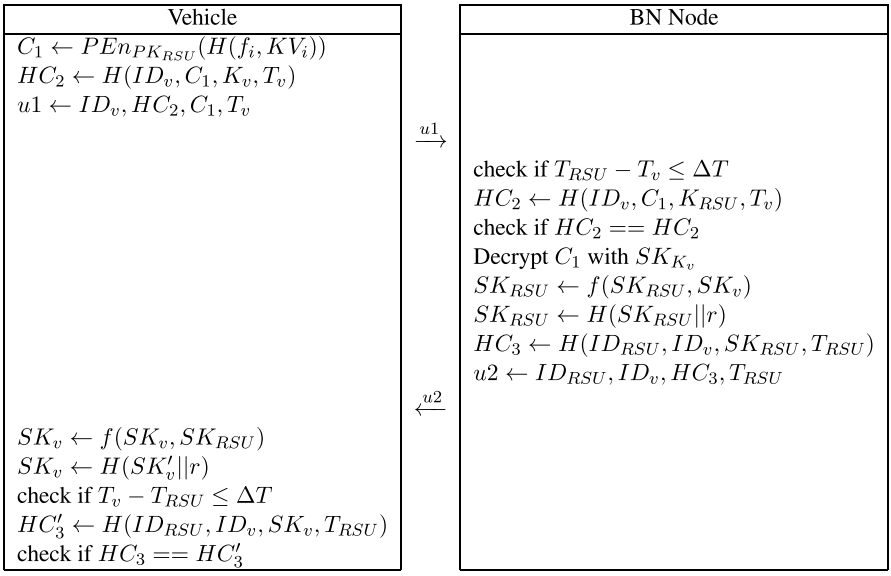

Fig. 9 Key Agreement protocol [Ma et al. 2017]

polynomial sets assigned to the vehicle V by the vehicle service provider and is fixed for a given vehicle. Therefore, in the Key Agreement protocol, an adversary can passively observe the two messages that are passed between a vehicle and BN node and copy C_1. Now, the adversary can impersonate the vehicle to the BC Node and vice versa. This is accomplished as follows. For the first message from vehicle to BN Node, ID_v, HC_2, C_1, T_v are required. Time stamp (T_v) can be generated by the adversary and the rest (ID_v, H, HC_2, C_1, K_v) are known to the adversary. Similarly, an adversary can impersonate the BN Node to the vehicle as follows. The only message that is sent from the BN Node includes $ID_{RSU}, ID_v, HC_3, T_{RSU}$. Here, ID_{RSU} and ID_v are known to the adversary and the time stamp T_{RSU} can be easily generated by the adversary. The adversary can also generate HC_3 since $H, ID_{RSU}, ID_v, SK_{RSU}, T_{RSU}$ are all known.

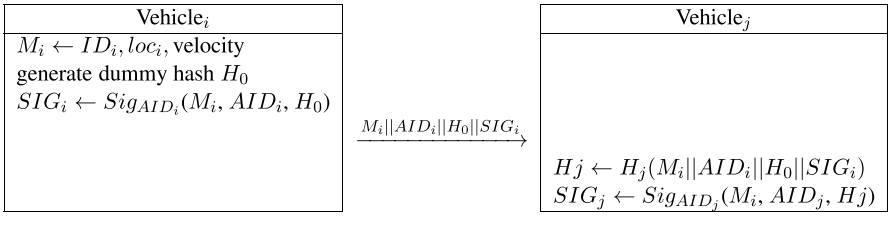

Fig. 10 MPFSLP protocol [Singh et al.30]

3.9 Source-location privacy

Singh et al. [30] develop Masqueraded Probabilistic Flooding for Source-Location Privacy (MPFSLP) to protect the identity and location of the source node for a message in VANET with the claim that the message (here, location information and velocity) is important and not the node (here, vehicle) that broadcast that message. A message from a node is resent as a masqueraded packet to the next node, which resends the message as a masqueraded packet to another node, and so on until the last node. In this process (Fig. 10), any intermediate node only knows its previous node (i.e., the node which sent that message) and nothing about earlier nodes in this "chain." The setup also ensures that the originator cannot deny having sent that message (i.e., nonrepudiation).

The message (M_i) includes the identity (ID_i) of the vehicle (V_i) that generates the message, its location, and its velocity. The packet that is sent from the origin node (i.e., the vehicle V_i that generates the message M_i) to the next node (i.e., the next vehicle V_j in the chain of this message) includes the message (M_i), the origin vehicle's pseudonym (AID_i), a dummy hash (H_0), and digital signature of these three ($SIG_i \leftarrow Sig_{AID_i}(M_i, AID_i, H_0)$). Upon reception of this packet, the next vehicle (V_j) generates the hash of the entire packet that was received $Hj \leftarrow H_j(M_i \| AID_i \| H_0 \| SIG_i)$. It then generates a digital signature $SIG_j \leftarrow Sig_{AID_j}(M_i \| AID_j \| Hj)$. Next, V_j sends M_i, AID_j, Hj, and SIG_j to the next vehicle in the chain. This continues until the endpoint is reached.

Since the hash of the packet received from the previous vehicle is the only link between the two vehicles for a given message, a serious vulnerability in this protocol is that an adversary can easily insert itself in the chain or start a new chain by generating a new message M_A, AID_A, a dummy hash H_0, and a signature of these three ($SIG_A \leftarrow Sig_{AID_A}(M_A, AID_A, H_0)$). The adversary can then send the packet with (M_A, AID_A, H_0, SIG_A), which will be accepted by the next vehicle as there is no check on the authenticity of the message. The nonrepudiation claim for the origin node is that it contains the dummy hash and its signature (SIG_i) contains the dummy hash as well as its pseudonym. However, these are not constraints for an adversary to generate a dummy hash along with a new message and then generate the corresponding packet for the next vehicle in the chain.

An adversary can also modify the message and assign H_0 to a random node (say, V_k) in the chain since it can block and capture the packet from that node (i.e., $M_i||AID_k||H_k||SIG_k$), modify M_i to M_i', generate a new SIG_k' that is signed with AID_k just captured, and send $M_k'||AID_k||H_0||SIG_k'$ to the next node, which will accept this packet as valid.

Since the destination vehicle V_j is not specified in the protocol, an adversary can relay the message from any vehicle in the message chain to any other vehicle for successful relay attack.

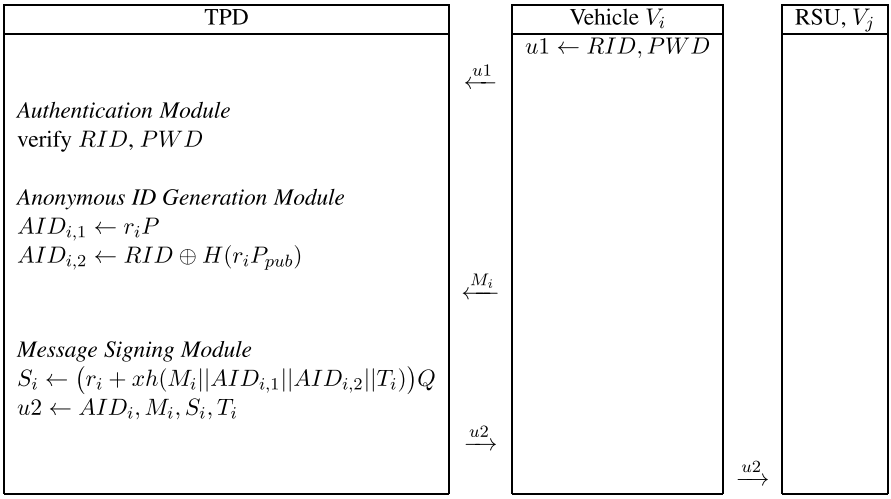

Fig. 11 Batch verification scheme [Tzeng et al. 2017]

3.10 Identity-based batch verification scheme

The modeled system (Fig. 11) includes vehicles, tamper-proof device (TPD) in vehicles, and roadside units (RSU) [31]. The vehicle, represented by a user, initiates the process with *RID*, *PWD* entered in its TPD. The TPD verifies the input in its Authentication Module and then generates $AID_{i,1}$, $AID_{i,2}$ in its Anonymous ID Generation Module. Later, when the vehicle inputs the message it wants sent to adjacent RSU and other vehicles in its vicinity, the TPD generates a signature (S_i) that incorporates the message and current timestamp (T_i) and sends $\{AID_i, M_i, S_i, T_i\}$ to the vehicle, which then forwards the same to adjacent RSU and nearby vehicles. The public parameters include $\{P, Q, P_{pub}, h(.)\}$

The goal of the protocol is to securely send the message M_i from vehicle V_i to adjacent RSU and vehicles. However, as we show below, an adversary can easily compromise the system and send a different message that will be accepted as valid. To accomplish this, the adversary first multiplies S_i by P to get

$PS_i = \big(Pr_i + Pxh(M_i||AID_{i,1}||AID_{I,2}||T_i)\big)Q$

The adversary knows that $P_{pub} = xP$ and $AID_{i,1} = r_i P$. So,

$PS_i = \big(AID_{i,1} + P_{pub}h(M_i||AID_{i,1}||AID_{I,2}||T_i)\big)Q$

From the above expression, S_i can be generated as all the other terms are known to the adversary who listens in on the message from this vehicle. This signifies that the adversary can impersonate this vehicle (V_i) to easily send any message it wants to the RSU and other vehicles from now on.

The adjacent RSU is not defined in the message from TPD of V_i or V_i. Therefore, a relay attack can be mounted by an adversary by relaying the broadcast message from V_i to any other RSU and set of vehicles in the system.

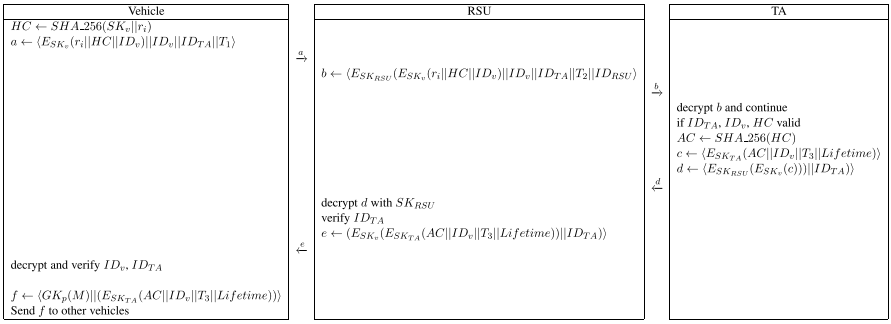

Fig. 12 Dual authentication [Vijayakumar et al. 32]

3.11 Dual authentication

Vijayakumar et al. [32] develop a dual authentication protocol (Fig. 12) that involves vehicle, RSU, and a trusted authority (TA). Tan et al. [33] had critically considered this protocol and identified a vulnerability.

As noted by Tan et al. [33], and incorrectly refuted by Azees [34], T_1 is not encrypted when sent from the vehicle to the RSU. Therefore, this message $(\langle E_{SK_v}(r_i||HC||ID_v)||ID_v||ID_{TA}||T_1\rangle)$ can be copied once and replayed several times to any *RSU* by an adversary with the modification of T_1 to an appropriate value. This is possible since T_i is not a part of any other term (SK_v, r_i, HC, ID_v, or ID_{TA}) in the entire message $(\langle E_{SK_v}(r_i||HC||ID_v)||ID_v||ID_{TA}||T_1\rangle)$. Since the adversary chooses a T_1 that is current, the *RSU* will accept this entire message as valid and proceed to the next step. Another vulnerability here is the vehicle identifier, which is a constant, is sent in the open. An adversary can readily use (ID_v) to track and trace this vehicle.

Yet another vulnerability is in the use of a group key. A vehicle generates and sends safety message (M) encrypted with a group key (GK_p). A rogue vehicle with knowledge of this group key can capture this entire message $(\langle GK_p(M)||(E_{SK_{TA}}(AC||ID_v||T_3||Lifetime))\rangle)$, modify just the $GK_p(M)$ part with a different message (M') and send $(\langle GK_p(M')||(E_{SK_{TA}}(AC||ID_v||T_3||Lifetime))\rangle)$ to other vehicles. The other vehicles will evaluate this message to be from an honest vehicle and accept M' as true. The vulnerability is similar to the one mentioned above. Here, the safety message (M) is present only in $GK_p(M)$ and the rogue vehicle knows GK.

The message between vehicle and RSU does not include any information on the RSU. Therefore, an adversary can mount a relay attack by relaying the message from the vehicle to any RSU for successful validation by the TA.

3.12 Messaging service in VANET clouds

This system [35] comprises vehicles (V_i, $i \in [1, n]$), roadside units (R_j, $j \in [1, n]$), and content provider (CP). The paper presents a set of protocols for efficient key distribution in VANET clouds. The scheme consists of eight phases that include setup, registration, multicast authentication, session-key generation, RSU-based key

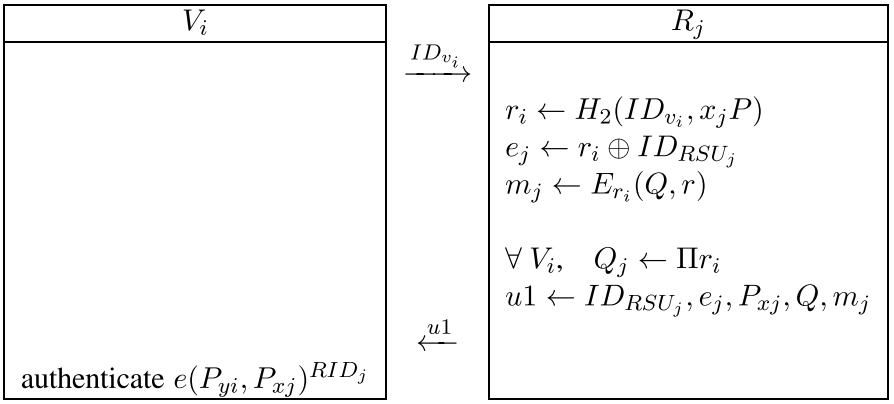

Fig. 13 Multicast authentication [Wu 2017]

exchange, key request from other RSUs, anonymous request, and secret push messaging transmission.

In the first (setup) phase, the three types of entities (*CP*, *RSU*, and *V*) select their random secret keys that are, respectively, s ($\in Z_q^*$), x_j ($[1, q-1]$), and y_i ($[1, q-1]$). The respective public keys of *CP*, *RSU*, and *V* are P_{pub} ($= sP$), P_{xj} ($= x_jP$), and P_{yi} ($= y_iP$).

The vehicles and roadside units register with the content provider during the second (registration) phase and this process is conducted in a secure channel.

Multicast authentication is performed in the third phase between the j^{th} *RSU* (i.e., R_j) and all vehicles in its "area."

A vulnerability in the multicast authentication protocol (Fig. 13) is the vehicle i sending its fixed identifier ID_{v_i} in the open as this can be used by an adversary

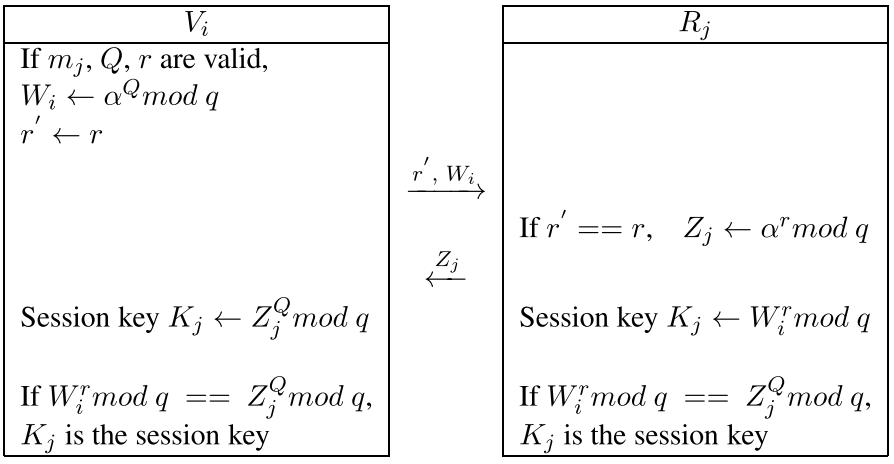

Fig. 14 Session-key generation [Wu 2017]

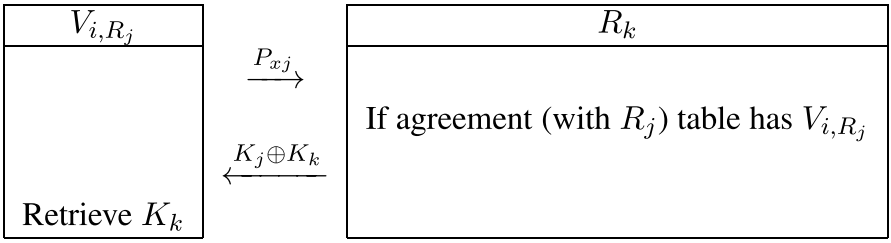

Fig. 15 Key request from nearby RSU [Wu 2017]

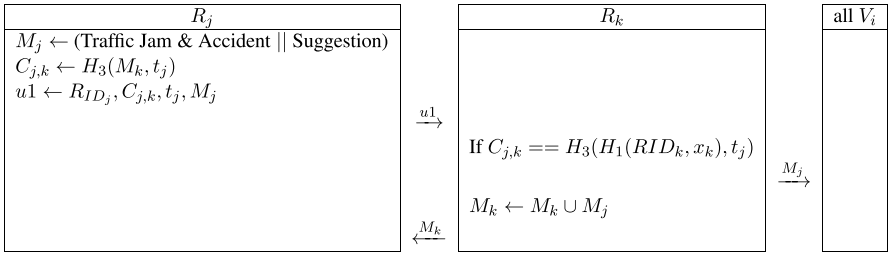

Fig. 16 Secret push messaging transmission [Wu 2017]

to track the presence of this vehicle in that area. This also signifies that an adversary can easily impersonate any vehicle to any roadside unit with knowledge of its identifier. This is a vulnerability since the authentication is only one-way and not mutual - the vehicle authenticates the roadside unit whereas the roadside unit does not authenticate the vehicle. In Fig. 13, r_i includes ID_{v_i} and both e_j and m_j use r_i. Since the message from RSU to the vehicles is multicast to all vehicles in the area, it is not clear which i is selected in the generation of e_j and m_j.

The fourth phase involves session-key generation (Fig. 14). Since q and α (a primitive element mod q) are public and $r^{'}$ is in the message from V_i (Fig. 14), an adversary can easily generate Z_j. With knowledge of Z_j and the public knowledge of q and Q, the adversary can readily generate the session key.

The fifth phase is RSU-based key exchange through secure channels.

The sixth phase involves key request from nearby RSU. A vehicle V_i which moves from the area covered by roadside unit R_j to that covered by R_k (represented by V_{i,R_j}) needs to establish its new session key (K_k). This process is illustrated in Fig. 15.

Since P_{xj} (Fig. 15) is RSU_j's public key, an adversary who was in R_j's area can easily use that public key to send the first message to RSU_k. When R_k checks to see if the adversary was at R_j's area before, it'll check out to be true and so R_k sends $K_j \oplus K_k$ to the adversary impersonating V_{i,R_j}. With the knowledge of K_j, it

is easy for the adversary to retrieve K_k. Clearly, from now on, the adversary can generate the session key corresponding to the areas that it visits next.

The seventh phase is anonymous request through a secure channel where RSU R_k sends an anonymous request to CP to provide R_j's identifier (ID_{RSU_j}).

The eighth and last phase is secret push messaging transmission in which R_j transmits a safety-related message M_j to R_k, which forwards this message to V_is in its signal range. This message could include information on traffic conditions such as congestions and accidents.

In Fig. 16, the safety-related message from R_j to R_k is sent unencrypted. Unless this part of the protocol is through a secure channel which is not mentioned in the paper, an adversary can easily capture or block and modify this safety-related message (M_j), and then retransmit it to R_k. The same can be done with the message from R_k to all V_is.

4 The proposed protocol

We develop an authentication protocol (Fig. 17) that is secure against attacks that are discussed in this paper, with specific focus on relay attacks. This mutual authentication protocol authenticates a vehicle to an RSU and vice versa. The trusted authority (TA) is used to verify the anonymous identifier of the vehicle to the RSU. To ensure resistance against relay attacks, we make use of ambient condition information (A_i)

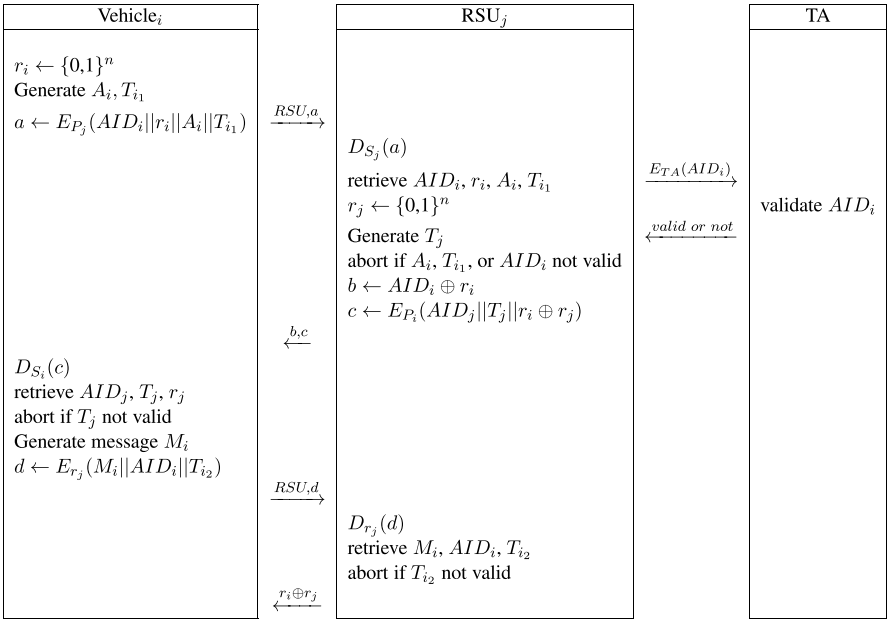

Fig. 17 Protocol for message from vehicle to RSU

since cryptography alone cannot address relay attacks as these attacks do not modify any of the passed messages between entities. Our rationale for ambient condition use is that since both the sender and receiver (here, vehicle and RSU) are at a certain level of physical proximity to each other (i.e., an RSU communicates with vehicles that are in its signal field), the ambient conditions at reader and vehicles are bound to be similar. For example, temperature and atmospheric pressure at vehicle and RSU locations are most likely not that different. Similarly, an RSU's GPS (Global Positioning System) coordinates can be used to delineate valid vehicle GPS locations as these vehicles have to be within communication range from the RSU. The developed protocol is indifferent to the number and types of A_i used.

Communication between vehicles and RSUs occur through wireless channel, which may not be secure whereas those between RSUs and TA occur through secure channels. Since message-passing is an important facet of VANETs, our protocol is designed to ensure secure transmission of messages between vehicles and RSU. To ensure randomness in the messages that are passed between vehicle and RSU, each message includes nonce (r_i, r_j) or current timestamp (T_{i_1}, T_{i_2}, T_j). Such randomness in messages secures the protocol against replay attacks. We also do not update any of the values after each authentication round to prevent desynchronization attacks. We do not send any identification information in the open to prevent tracking and tracing. To prevent replay attacks, we include dependencies among the messages: r_i in b and c; r_j in d; r_i and r_j in the last message from RSU to vehicle. A message that is meant for an RSU includes "RSU" in the header so it is easy to distinguish those from messages that are meant for vehicles. We intentionally define A_i to include the concatenation of as many ambient conditions as are available or are necessary for a given context. We use b to reference c to vehicle i. Message d includes r_j and AID_i so the RSU knows that this message is from vehicle i, in the presence of race conditions. Given the possibly large number of vehicles, the TA validates AID_i. Here, E_{TA} is the shared (symmetric) key between RSU and TA.

To verify the security correctness of the proposed protocol and its assumptions with respect to message source and beliefs of the message recipients and senders, we use the GNY logic [36]. GNY logic helps prove that the authentication protocol meets its specifications by showing that all entities learn what they should learn, and what the entities learn are indeed true. We begin with the individual messages that are passed between any two entities, the explicit assumptions that are inherent in the messages, the goals, followed by the proofs of these goals. The objectives are to ensure that each of the messages is from a trusted source and that each message is fresh.

Protocol messages:

M1: $RSU_j \lhd \star(RSU), \star(E_{P_j}(AID_i||r_i||A_i||T_{i_1}))$

M2: $TA \lhd E_{TA}(AID_i)$

M3: $RSU_j \lhd$ valid

M4: $V_i \lhd \star(AID_i \oplus r_i), \star(E_{P_i}(AID_j||T_j||r_i \oplus r_j))$

M5: $RSU_j \lhd \star(RSU), \star(E_{r_j}(M_i||AID_i||T_{i_2}))$

M6: $V_i \lhd ri \oplus r_j$

Assumptions:

A1: $V_i \ni r_i$
A2: $V_i| \equiv \#r_i$
A3: $RSU_j \ni r_j$
A4: $RSU_j| \equiv \#r_j$
A5: A5: $V_i| \equiv V_i \overset{r_i}{\leftrightarrow} RSU_j$
A6: A6: $RSU_j| \equiv RSU_j \overset{r_i}{\leftrightarrow} V_i$
A7: A7: $V_i| \equiv V_i \overset{A_i}{\leftrightarrow} RSU_j$
A8: A8: $RSU_j| \equiv RSU_j \overset{A_i}{\leftrightarrow} V_i$
A9: $V_i \ni T_{i_1}$
A10: $V_i| \equiv \#T_{i_1}$
A11: $V_i \ni T_{i_2}$
A12: $V_i| \equiv \#T_{i_2}$
A13: $RSU_j \ni T_j$
A14: $RSU_j| \equiv \#T_j$
A15: A15: $RSU_j| \equiv RSU_j \overset{r_j}{\leftrightarrow} V_i$
A16: A16: $V_i| \equiv V_i \overset{r_j}{\leftrightarrow} RSU_j$
A17: $V_i \ni A_i$
A18: $V_i| \equiv \#A_i$
A19: $V_i \ni M_i$
A20: $V_i| \equiv \#M_i$

Goals of the correctness proof: With belief (| ≡) and freshness (#) of each of the messages that are passed between pairs of entities (V_i, RSU_j, TA) as the primary goals, belief ensures that the message is from a trusted source and freshness ensures that the message is fresh in that authentication session.

G1: $RSU_j| \equiv V_i| \sim \#(RSU)$
G2: $RSU_j| \equiv V_i| \sim \#(E_{P_j}(AID_i||r_i||A_i||T_{i_1}))$
G3: $TA| \equiv RSU_j| \sim \#(E_{TA}(AID_i))$
G4: $RSU_j| \equiv TA| \sim \#(valid)$
G5: $V_i| \equiv RSU_j| \sim \#(AID_i \oplus r_i)$
G6: $V_i| \equiv RSU_j| \sim \#(E_{P_j}(AID_j||T_j||r_i \oplus r_j))$
G7: $RSU_j| \equiv V_i| \sim \#(RSU)$
G8: $RSU_j| \equiv V_i| \sim \#(E_{r_j}(M_i||AID_i||T_{i_2}))$
G9: $V_i| \equiv RSU_j| \sim \#(r_i \oplus r_j)$

Proof The logical postulate numbers (e.g., M1, T1,..) referred to in the following are from [36]

[D1:] $RSU_j \lhd RSU, E_{P_j}(AID_i||r_i||A_i||T_{i_1})$ /* M1,T1 */
[D2:] $RSU_j \ni RSU, E_{P_j}(AID_i||r_i||A_i||T_{i_1})$ /* D1,P1 */
[D3:] $RSU_j| \equiv \#RSU, \#E_{P_j}(AID_i||r_i||A_i||T_{i_1})$ /* D2,F1 */

[D4:] $RSU_j| \equiv V_i \mid \sim \#RSU$ /* D3,I1,P2 */
[D5:] $RSU_j| \equiv V_i| \sim \#E_{P_j}(AID_i||r_i||A_i||T_{i_1})$/*A2,A6,A8,A10, D3,I1,P2*/
[D6:] $TA \lhd E_{TA}(AID_i)$ /* M2,T1 */
[D7:] $TA \ni E_{TA}(AID_i)$ /* D6,P1 */
[D8:] $TA| \equiv \#E_{TA}(AID_i)$ /* D6,F1 */
[D9:] $TA| \equiv RSU_j| \sim \#E_{TA}(AID_i)$ /* D8,I1,P2 */
[D10:] $RSU_j \lhd valid$ /* M3,T1 */
[D11:] $RSU_j \ni valid$ /* D10,P1 */
[D12:] $RSU_j| \equiv \#valid$ /* D11,F1 */
[D13:] $RSU_j| \equiv TA| \sim \#valid$ /* D12,I1,P2 */
[D14:] $V_i \lhd AID_i \oplus r_i, E_{P_i}(AID_j||T_j||r_i \oplus r_j)$ /* M4,T1 */
[D15:] $V_i \ni AID_i \oplus r_i, E_{P_i}(AID_j||T_j||r_i \oplus r_j)$ /* D14,P1 */
[D16:] $V_i| \equiv \#AID_i \oplus r_i, \#E_{P_i}(AID_j||T_j||r_i \oplus r_j)$ /*D14,F1*/
[D17:] $V_i| \equiv RSU_j \mid \sim \#AID_i \oplus r_i$ /* A2,D16,I1,P2 */
[D18:] $V_i| \equiv RSU_j| \sim \#E_{P_i}(AID_j||T_j||r_i \oplus r_j)$/*A2,A4, A14,D16,I1,P2*/
[D19:] $RSU_j \lhd RSU, E_{r_j}(M_i||AID_i||T_{i_2})$ /* M5,T1 */
[D20:] $RSU_j \ni RSU, E_{r_j}(M_i||AID_i||T_{i_2})$ /* D19,P1 */
[D21:] $RSU_j| \equiv \#RSU, \#E_{r_j}(M_i||AID_i||T_{i_2})$ /* D20,F1 */
[D22:] $RSU_j| \equiv V_i \mid \sim \#RSU$ /* D21,I1,P2 */
[D23:] $RSU_j| \equiv V_i| \sim \#E_{r_j}(M_i||AID_i||T_{i_2})$/*A4,A12,A20, D21,I1,P2*/
[D24:] $V_i \lhd r_i \oplus r_j$ /* M6,T1 */
[D25:] $V_i \ni r_i \oplus r_j$ /* D24,P1 */
[D26:] $V_i| \equiv \#r_i \oplus r_j$ /* D25,F1 */
[D27:] $V_i| \equiv RSU_j \mid \sim \#r_i \oplus r_j$ /* A2,A4,D26,I1,P2 */

The proof of goals G1–G9 is shown, respectively, by the verification steps D4, D5, D9, D13, D17, D18, D22, D23, D27. □

5 Discussion

VANETs involve the spontaneous creation, self-organization, and evolution of a wireless network of mobile nodes comprising vehicles and roadside infrastructure. Vehicles form the core of VANETs and these vehicles communicate with other vehicles (V2V), roadside infrastructure (V2I), and other entities (V2X). VANETs are essential for a future with connected and automated driving vehicles. VANETs facilitate safety-related applications such as the provision of safety messages on traffic information, cooperative driving, and accidents, collision avoidance and lane merging, traffic optimization, (toll) payment services, location-based services (e.g., determine nearest exit), and overall trust that is required among participating entities [17].

As vehicular communication occurs through wireless medium in VANETs, it is necessary to secure these to avoid unintended consequences. Authentication of all participants is also necessary to identify the source of every message to ensure non-repudiation. Given the significance of authentication, it is critical to ensure that there

Table 1 VANET authentication protocols and possible attacks

	Full-disclosure Attack	Impersonation Attack	Relay Attack	Replay Attack	Track & Trace
Ali et al. [20]	✗	✗	✗	✗	✗
Ali et al. [20]	✗	✗	✗	✗	✗
Alladi et al. [22]			✗		
Asaar et al. [23]	✗	✗	✗	✗	✗
Azees et al.[25]	✗	✗	✗	✗	✗
Feng et al. [26]		✗	✗		✗
He et al. [28]	✗	✗	✗	✗	✗
Ma et al. 2020	✗	✗	✗	✗	✗
Singh et al. [30]	✗	✗	✗	✗	✗
Tzeng et al. 2017	✗	✗	✗	✗	✗
Vijayakumar et al. [32]		✗	✗		✗
Wu 2017		✗			✗
Our method					

are no loopholes or vulnerabilities in the authentication protocols that could expose the system to serious attacks by resourceful adversaries. Security and privacy of VANETs rely on the strength of authentication protocols. Authentication protocol design should therefore ensure that there are enough dependencies among the messages to thwart replay attacks; none of the identifiers are sent in the open as these can be readily used for tracking and tracing purposes; the messages in each round have enough variations to avoid predictability; secrets are not disclosed, especially against a full-disclosure attack; relay attacks are prevented through appropriate means. With this perspective, we set out to evaluate VANET authentication protocols. Security analysis of authentication protocols that have been carefully designed and proved to be secure is not a trivial task. In the process, we identified several non-intuitive vulnerabilities that expose these VANET authentication protocols to attacks. Table 1 provides a summary of the identified attacks.

Table 1 shows that these authentication protocols are not secure for implementation with such identified vulnerabilities. These protocols need to be redesigned with, at a minimum, the countermeasures discussed above. It is worth noting that the number of wireless messages in a protocol should be kept to a minimum as more messages only help increase the attack surface and therefore associated vulnerabilities and related attacks. Inference control must be carefully operationalized with the identification of all possible inferences that could be generated from the wireless messages in the system to ensure that subsets or the set of all wireless messages together do not reveal any compromising information. We developed our authentication protocol to follow these guidelines as discussed in the first paragraph of Sect. 4.

6 Conclusion

We critically evaluated several VANET authentication protocols that were proposed over the last several years and identified vulnerabilities in each of these protocols. The identified vulnerabilities in these protocols include vehicle or RSU impersonation, transmission of identities in the open that can result in tracking and tracing attacks, full-disclosure attack, and relay attack. Impersonation attacks can generally be prevented by ensuring the presence of variations in messages across different authentication rounds and that these variations are not predictable. Variations (i.e., unpredictability) in messages across authentication rounds and avoidance of identification information in the open together prevent tracking and tracing attacks. The messages passed in the open need to be carefully designed to prevent revelation of secret key and other information. Full-disclosure attacks are the worst as nothing remains secret. Relay attacks are difficult to prevent even with protocols that are designed specifically against such attacks. As the protocols evaluated in this paper did not specifically consider the possibility of relay attacks, their design does not preclude such attacks. In addition to being secure against other types of attacks, the proposed authentication protocol is secure against relay attacks. Future development of novel VANET authentication protocols must ensure that they are not vulnerable to attacks from adversaries. A first step is to consider the recommendations mentioned in the previous and this section of this paper.

Acknowledgements We thank the ten anonymous reviewers for their constructive comments and suggestions that helped us improve the content and presentation of this paper.

Declarations

Conflict of interest: None.

References

1. Mohar SS, Goyal S, Kaur R (2022) Localization of sensor nodes in wireless sensor networks using bat optimization algorithm with enhanced exploration and exploitation characteristics. J Supercomput 332:22
2. Ahmed S, Shamshad S, Ghaffar Z, Mahmood K, Kumar N, Parizi RM, Choo K-KR (2021) Signcryption based authenticated and key exchange protocol for EI-Based V2G environment. IEEE Trans Smart Grid 12(6):5290–5298
3. Mahmood K, Shamshad S, Kumari S, Khan MK, Obaidat MS (2020) Comment on lightweight secure message broadcasting protocol for Vehicle-to-Vehicle communication. IEEE Syst J 15(1):1366–1368
4. Shamshad S, Saleem MA, Obaidat MS, Shamshad U, Mahmood K, Ayub MF, On the security of a lightweight privacy-preserving authentication protocol for VANETs. *IEEE Int Conf Artif Intell Smart Syst (ICAIS)*, 1766-1770, 2021
5. Shamshad S, Obaidat MS, Saleem MA, Shamshad U, Mahmood K, (2021) Security analysis on an efficient and provably secure authenticated key agreement protocol for Fog-based Vehicular Ad-Hoc Networks. *Int Conf Artif Intell Smart Syst (ICAIS)*, 1754-1759
6. Umar M, Islam SKH, Mahmood K, Ahmed S, Ghaffar Z, Saleem MA (2021) Provable secure identity-based anonymous and privacy-preserving inter-vehicular authentication protocol for VANETS using PUF. IEEE Trans Veh Technol 70(11):12158–12167

7. Krishnan PR, Kumar PAR (2021) A collaborative strategy for detection and eviction of Sybil attacker and Sybil nodes in VANET. Int J Commun Syst 34(3):4621
8. Haydari A, Yilmaz Y (2018) Real-time detection and mitigation of DDoS attacks in intelligent transportation systems. *IEEE Int Conf Intell Trans Syst (ITSC)*, 157-163
9. Greenberg A (2015) Hackers remotely kill a Jeep on the highway-with me in it.*WIRED*. https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/
10. A. Greenberg, Securing driverless cars from hackers is hard. Ask the ex-Uber guy who protects them. https://www.wired.com/ 2017/04/ubers-former-top-hacker-securing-autonomous-cars-really-hard-problem/
11. Golson J (2016) Car hackers demonstrate wireless attack on Tesla Model S.http://www.theverge.com/2016/9/19/12985120/teslamodel-s-hack-vulnerability-keen-labs
12. Nie S, Liu L, Du Y,Free-fall: hacking tesla from wireless to CAN bus. In: *Proceedings of the Black Hat USA 2017*, Las Vegas, 1-16, 2017
13. Miller C, Valasek C, Adventures in automotive networks and control units. http://illmatics.com/car_hacking.pdf
14. Watchdog C (2019) Kill switch: Why connected cars can be killing machines and how to turn them off.https://www.consumerwatchdog.org/sites/default/files/2019-07/KILL
15. Mikavika B, Kostić-Lyubisavljević A (2021) Blockchain-based solutions for security, privacy, and trust management in vehicular networks: a survey. J Supercomput 77:9520–9575
16. Saravanan M, Kumar SM (2021) Improved authentication in vanets using a connected dominating set-based privacy preservation protocol. J Supercomput 77:14630–14651
17. Raya M, Hubaux J-P (2007) Securing vehicular ad hoc networks. J Comput Secur 15(1):39–68
18. Nayak RP, Sethi S, Bhoi SK, Mohapatra D, Sahoo RR, Sharma PK, Putha D (2022) TFMD-SDVN: a trust framework for misbehavior detection in the edge of software-defined vehicular network. J Supercomput 78:7948–7981
19. Beth T, Desmedt Y(1990) Identification tokens - or: solving the chess grandmaster problem. *Advances in Cryptology-CRYPTO'90*, Springer LNCS 537, 169-177
20. Ali I, Lawrence T, Omala AA, Li F (2020) An efficient hybrid signcryption scheme conditional privacy-preservation for heterogeneous vehicular communication in VANETs. IEEE Trans Veh Technol 69(10):11266–11280
21. Ali I, Chen Y, Ullah N, Kumar R, He W (2021) An efficient and provably secure ECC-based conditional privacy-preserving authentication for vehicle-to-vehicle communication in VANETs. IEEE Trans Veh Technol 70(2):1278–1291
22. Alladi T, Chakravarty S, Chamola V, Guizani M (2020) A lightweight authentication and attestation scheme for in-transit vehicles in IoV scenario. IEEE Trans Veh Technol 69(12):14188–14197
23. Asaar MR, Salmasizadeh M, Susilo W, Majidi A (2018) A secure and efficient authentication technique for vehicular ad-Hoc networks. IEEE Trans Veh Technol 67(6):5409–5423
24. Liu Y, Wang L, Chen H-H (2015) Message authentication using proxy vehicles in vehicular ad hoc networks. IEEE Trans Veh Technol 64(8):3697–3710
25. Azees M, Vijayakumar P, Deborah LJ (2017) EAAP: efficient anonymous authentication with conditional privacy-preserving scheme for vehicular ad hoc networks. IEEE Trans Intell Transp Syst 18(9):2467–2476
26. Feng Q, He D, Zeadally S, Liang K (2020) BPAS: blockchain-assisted privacy-preserving authentication system for vehicular ad hoc networks. IEEE Trans Industr Inf 16(6):4146–4155
27. Chen C-M, Deng X, Gan W, Chen J, Islam SKH (2021) A secure blockchain-based group key agreement protocol for IoT. J Supercomput 77:9046–9068
28. He D, Zeadally S, Xu B, Huang X (2015) An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks. IEEE Trans Inf Forensics Secur 10(12):2681–2691
29. Ma Z, Zhang J, Guo Y, Liu Y, Liu X, He W (2020) An efficient decentralized key management mechanism for VANET with blockchain. IEEE Trans Veh Technol 69(6):5836–5849
30. Singh PK, Agarwal A, Nakum G, Rawat DB, Nandi S (2020) MPFSLP: masqueraded probabilistic flooding for source-location privacy in VANETs. IEEE Trans Veh Technol 69(10):11383–11393
31. Tzeng S-F, Horng S-J, Li T, Wang X, Huang P-H, Khan MK (2017) Enhancing security and privacy for identity-based batch verification scheme in VANETs. IEEE Trans Veh Technol 66(4):3235–3248
32. Vijayakumar P, Azees M, Kannan A, Deborah LJ (2016) Dual authentication and key management techniques for secure data transmission in vehicular ad hoc networks. IEEE Trans Intell Transp Syst 17(4):1015–1028

33. H. Tan, D. Choi, P. Kim, S. Pan, I. Chung, "Comments on "Dual authentication and key management techniques for secure data transmission in vehicular ad hoc networks". " *IEEE Transactions on Intelligent Transportation Systems*, 19(7), 2149-2151, July 2018
34. Azees M (2019) Reply to comments on "Dual authentication and key management techniques for secure data transmission in vehicular ad hoc networks. IEEE Trans Intell Transp Syst 20(9):3595
35. Wu W-C (2017) A secret push messaging service in VANET clouds. Journal of Supercomputing 73:3085–3097
36. L. Gong, R. Needham, R. Yahalom, "Reasoning about belief in cryptographic protocols." *Proceedings of the IEEE Symposium on Security and Privacy*, 234-248, 1990