Cryptanalysis of Secure and Lightweight Conditional Privacy-Preserving Authentication for Securing Traffic Emergency Messages in VANETs

Mahender Kumar, *Member, IEEE,*

***Abstract*—In their paper, Wei et al. proposed a lightweight protocol for conditional privacy-preserving authentication in VANET. The protocol aims to achieve ultra-low transmission delay and efficient system secret key (SSK) updating. Their protocol uses a signature scheme with message recovery to authenticate messages. This scheme provides security against adaptively chosen message attacks. However, our analysis reveals a critical vulnerability in the scheme. It is susceptible to replay attacks, meaning a malicious vehicle can replay a message multiple times at different timestamps. This action undermines the overall effectiveness of conditional privacy. We suggest possible solutions to address these vulnerabilities and enhance the security of VANET communication.**

***Index Terms*—VANET, privacy-preserving authentication, universal forgery, replay attack.**

I. Introduction

VEHICULAR Ad Hoc Networks (VANETs) have been developed to enhance transportation safety and efficiency. However, the wireless channels they use are susceptible to attacks, making it essential to secure VANETs. Privacy is also a significant concern in VANETs, and although Pseudo-identity techniques can address this issue, it is challenging to manage them on resource-constrained vehicles. Conditional privacy-preserving authentication (CPPA) schemes are a promising solution for securing VANETs. However, the computational overhead of bilinear pairing operations is a significant barrier, making developing low-latency solutions for CPPA schemes necessary.

A recent CPPA scheme, developed by Wei et al. [1], aimed to address these challenges. Unfortunately, a recent analysis by Zhang et al. [2] revealed that this scheme is vulnerable to universal forgery. This flaw allows attackers to forge valid signatures on any message, making it possible to disseminate false information undetected. Our analysis also shows that Wei et al. [1] is insecure against replay attacks, which means that a malicious vehicle can replay a message multiple times at different timestamps, undermining the overall effectiveness of conditional privacy. Our analysis highlights the need for robust security mechanisms in VANETs and uncovers the reasons behind these vulnerabilities.

M Kumar was with the Warwick Manufacturing Group, University of Warwick, United Kingdom, CV47AL USA e-mail: mahender.kumar@warwick.ac.uk.

Manuscript received .

II. Reviews of Wei et al.'s Conditional Privacy-Preserving Authentication in VANET

This section briefly outlines Wei et al.'s CPPA scheme [1]. For comprehensive details, readers are encouraged to refer to the original work [1].

A. System Setup Phase

In this phase, a trusted authority (TA) generates an elliptic curve group G over a finite field F_p, where p is a large prime, and selects a generator P. TA then randomly chooses a system secret key (SSK) $s \in \mathbb{Z}q$ and computes its public key $Ppub = -sP$. Each vehicle V_i registers with TA by providing its identity I_{Di} and password PW_i. TA implants the SSK s into the tamper-proof device (TPD) of vehicle V_i. Finally, TA publishes the system public parameters $Para = (G, P, P_{pub}, q, H_1, H_2, H_3, H_4, H_5)$ in VANET.

B. Signature Generation

During signature generation, vehicle performs the following steps:

- First, the vehicle V_i inputs its identity I_{Di} and password PW_i into TPD to verify the legality of its identity by checking whether $H_1(I_{Di}, PW_i)$ equal to the stored value. If the verification fails, the TPD aborts it.
- The TPD of vehicle V_i randomly chooses a number $r_i \in \mathbb{Z}_q$ to compute $R_i = r_iP$ and its pseudo-identity $PID_i = H_2(r_iP_{pub}, T_i) \oplus I_{Di}$, where T_i denotes the current timestamp. Then, it uses its SSK s to compute $k_i = r_i + s \cdot H_1(PID_i, T_i)$ and $(R_i)_x$, where $(R_i)_x$ is the x-coordinate of point R_i. Finally, the TPD returns $(PID_i, k_i, (R_i)_x, T_i)$ to vehicle V_i.
- On receiving $(PID_i, k_i, (R_i)_x, T_i)$ from its TPD, the vehicle V_i randomly chooses $u_i \in \mathbb{Z}_q$ to compute its one-time public key $U_i = -u_iP$ and then computes the signature $\delta_i = (\delta_{1i}, \delta_{2i})$ of the traffic emergency message $m_i \in \{0, 1\}^n$, where $\delta_{1i} = ((R_i)_x \oplus (H_3(m_i)||(H_4(H_3(m_i)) \oplus m_i))), \delta_{2i} = k_i + u_i \cdot H_5(PID_i, T_i, \delta_{1i}, U_i)$. Finally, V_i sends $(PID_i, U_i, T_i, \delta_i)$ to the vehicles around it.

C. Signature Verification Process

After receiving $(PID_i, U_i, T_i, \delta_i)$, to obtain the traffic emergency message m_i and verify its validity, a nearby vehicle V_j executes the following steps:

- First of all, V_j needs to verify the validity of the timestamp T_i by checking whether the relation $|T_i - T_c| \leq T$ holds, where T_c denotes the current timestamp, and T denotes the allowed maximum transmission delay of the traffic emergency message. If it is not satisfied, the message received is rejected. Otherwise, V_j goes on to the next step.
- Next, to recover the R_i, V_j computes the equation $R_i = \delta_{2i} \cdot P + H_1(PID_i, T_i) \cdot P_{\text{pub}} + H_5(PID_i, T_i, \delta_{1i}, U_i) \cdot U_i = r_i P + H_1(PID_i, T_i) \cdot sP + H_1(PID_i, T_i) \cdot (-sP) + H_5(PID_i, T_i, \delta_{1i}, U_i) \cdot u_i P + H_5(PID_i, T_i, \delta_{1i}, U_i) \cdot (-u_i P) = r_i P$. Then, it computes string $= \delta_{1i} \oplus (R_i)_x$ and extracts message m_i by computing $m_i = \text{Right}(string, n) \oplus H_4(\text{Left}(string, |q| - n))$, where $\text{Right}(str, x)$ and $\text{Left}(str, x)$ denote the least significant x bits of str and the most significant x bits of str, respectively.
- Finally, V_j verifies whether the equation $H_3(m_i) = \text{Left}(string, |q| - n)$ holds. If it holds, the signature δ_i and message m_i are valid; otherwise, V_j rejects the message.

III. Proposed Replay Attack on Wei et al. Scheme

Suppose X represents all valid messages a vehicle can generate ($X = \{M_1, M_2, ..., M_n\}$). Let adversary (Adv) capture a valid message $M_v \in X$. The replay attack window is represented by the interval $W = \{T_i - T | T_i \in timestamps(X), T_c \in current\_time\}$. The verification process might succeed if Adv replays the message within this window ($T_c \in W$). Suppose two timestamps T_1 and T_2 such that $T_1 < T_2$. We will demonstrate how Adv can exploit the vulnerability in the Wei et al. scheme [1] to execute a replay attack. Adv captures a valid message at timestamp T_1, denoted as $M_{T_1} = (PID_i, U_i, T_1, \delta_1)$, where PID_i, U_i, and δ_1 are the pseudo-identity, one-time public key, and signature respectively. The Adv replays M_{T_1} at timestamp T_2, forming a replayed message $M_{T_2} = (PID_i, U_i, T_2, \delta_1)$.

According to the Wei et al. scheme [1], the verification process checks the validity of the timestamp T_i by comparing it with the current timestamp T_c. The message is valid if $|T_i - T_c| \leq T$ holds, where T is the maximum transmission delay. Since the replayed message M_{T_2} has a timestamp T_2, and the verification window T allows for messages within a certain time range, $|T_2 - T_c| \leq T$, the algorithm accepts M_{T_2} as a valid message. Accepting the replayed message M_{T_2} allows the Adv to disseminate false information or disrupt the normal operation of the VANET system without being detected.

To illustrate how vehicle V_j can accept the same message twice at timestamps T_1 and T_2 within the allowed maximum transmission delay T, we consider a scenario where a replay attack occurs. Let's assume that vehicle V_j receives the identical message M at timestamps T_1 and T_2, where $T_1 < T_2$. This message M comprises the components $(PID_i, U_i, T_i, \delta_i)$.

Here's how V_j would accept the same message twice:

Verification of Timestamps: V_j verifies the validity of the timestamp T_i for both messages M_1 and M_2 by checking whether $|T_i - T_c| \leq T$, where T_c is the current timestamp and T is the maximum transmission delay. If $|T_1 - T_c| \leq T$ and $|T_2 - T_c| \leq T$, V_j proceeds to the next step.

Recovery of R_i and Message Extraction: V_j computes R_i using the equation:

$$\begin{aligned} R_i &= \delta_{2i} \cdot P + H_1(PID_i, T_i) \cdot P_{\text{pub}} + H_5(PID_i, T_i, \delta_{1i}, U_i) \cdot U_i \\ &= r_i P + H_1(PID_i, T_i) \cdot sP + H_1(PID_i, T_i) \cdot (-sP) \\ &\quad + H_5(PID_i, T_i, \delta_{1i}, U_i) \cdot u_i P \\ &\quad + H_5(PID_i, T_i, \delta_{1i}, U_i) \cdot (-u_i P) = r_i P. \end{aligned}$$

After computing R_i, V_j derives the string $string = \delta_{1i} \oplus (R_i)_x$ and extracts the message m_i from it.

Verification of Message Validity: V_j verifies whether the equation $H_3(m_i) = \text{Left}(string, |q| - n)$ holds. If the equation holds for both messages M_1 and M_2, V_j accepts both messages as valid.

In this scenario, V_j accepts both messages M_1 and M_2 because they fall within the allowed maximum transmission delay T and satisfy the message validity checks. This proves how the replay attack allows V_j to accept the same message multiple times at different timestamps.

Discussion and solution: While timestamps provide a basic level of freshness, they can still be vulnerable to replay attacks within a short window. We can combine timestamps with nonces for better protection.

During signature generation (step II.B), each vehicle V_i incorporates a random nonce (N_i) alongside the timestamp (T_i) in the message ($m_i||T_i||N_i$). This nonce, unique for each message, adds an additional layer of randomness. The concatenated string ($m_i||T_i||N_i$) undergoes hashing using H_3 before further signature generation. Subsequently, V_i transmits $(PID_i, U_i, T_i, N_i, \delta_i)$ to other vehicles in the network.

During verification (step II.C), upon receiving $(PID_i, U_i, T_i, N_i, \delta_i)$, each vehicle V_j follows a process similar to Wei et al.'s scheme [1]. It verifies timestamps, recovers R_i, and extracts m_i. During message verification, V_j ensures that the equation $H_3(m_i||T_i||N_i) = \text{Left}(string, |q| - n)$ holds. If this equation holds for both messages M_1 and M_2, V_j deems both messages as valid.

IV. Conclusion

In our analysis of Wei et al.'s privacy-preserving authentication protocol in VANET, we have identified a major security flaw. Despite claims of being secure, the protocol is vulnerable to replay attacks. This means malicious vehicles can replay messages multiple times, leading to a DOS attack. Additionally, the identity of the malicious vehicle cannot be traced, making the protocol unreliable in ensuring authentication privacy.

References

[1] L. Wei, J. Cui, Y. Xu, J. Cheng, and H. Zhong, "Secure and lightweight conditional privacy-preserving authentication for securing traffic emergency messages in VANETs," IEEE Trans. Inf. Forensics Security, vol. 16, pp. 1681–1695, 2021, doi: 10.1109/TIFS.2020.3040876.

[2] Zhang, Jianhong, and Qijia Zhang. "Comment on "Secure and Lightweight Conditional Privacy-Preserving Authentication for Securing Traffic Emergency Messages in VANETs"." IEEE Transactions on Information Forensics and Security 18 (2021): 1037-1038.