Comments on "An Efficient and Provably Secure Authenticated Key Agreement Protocol for Fog-Based Vehicular Ad-Hoc Networks"

1st Syed Muhammad Awais
School of Microelectronics and Communication Engineering
Chongqing University
Chongqing, China
syedmowais87@gmail.com

2nd Wu Yucheng
School of Microelectronics and Communication Engineering
Chongqing University
Chongqing, China
wuyucheng@cqu.edu.cn

3rd Khalid Mahmood*, *Senior Member, IEEE*
School of Psychology and Computer Science and Graduate School of Intelligent Data Science
University of Central Lancashire and National Yunlin University of Science and Technology
Preston, United Kingdom and Yunlin 64002, Taiwan
khalidm.research@gmail.com

4th Rupak Kharel, *Senior Member, IEEE*
School of Psychology and Computer Science and Faculty of Electrical and Electronics Engineering
University of Central Lancashire and Ton Duc Thang University
Preston, United Kingdom and Ho Chi Minh City, Vietnam
r.kharel@hud.ac.uk

***Abstract*—Vehicle ad-hoc networks (VANETs) have experienced rapid growth due to the advancement of cloud computing, IoT technologies, and intelligent transportation systems (ITS). Vehicles are required to have enhanced storage capacity, onboard computing capabilities, improved sensing power, and communication systems. To address real-world demands like low latency, affordable storage, and mobility in VANET deployments, There have been efforts to integrate fog computing with VANETs in a practical implementation. "An Efficient and Provably Secure Authenticated Key Agreement Protocol for Fog-Based Vehicular Ad-Hoc Networks" was proposed by Ma et al. (IEEE Internet of Things Journal, pp 8065–8075, 10.1109/JIOT.2019.2902840). According to their claims, the use of their secure authentication technique can help prevent security threats. However, after careful investigation, we discovered that their authentication protocol is susceptible to vehicle user impersonation attacks and also does not provide vehicle anonymity. In light of this, we have provided some recommendations to address the current flaws in the protocol developed by Ma et al.**

***Index Terms*—Privacy preserving, Mutual Authentication, Information Security, VANET**

I. Introduction

THE internet of Things (IoT) technology is the third wave of the global information industry, following the computer and the Internet. It is a significant driver of productivity and global growth. Through the application of numerous sensing technologies, including radio frequency identification (RFID) and sensors, as well as different communication modes, IoT enables the connection of objects to the network. This connection allows for remote monitoring, automatic alerts, diagnostics, and other functionalisties. IoT has found applications in diverse industries, including environmental protection, smart home technology, intelligent healthcare, and intelligent transportation systems (ITS).

Intelligent transportation systems (ITS) has attracted the interest of both the business community and the academic community [1]. The main objective is to provide a range of road services via cloud-based V2V and V2I communications between vehicles and infrastructure. While V2I is more appropriate for non-critical services, V2V is actually more beneficial for localized emergency services [2]. The solutions for cloud-based vehicular networks have several problems with the transfer of considerable real-time traffic data from the road infrastructures to the cloud servers, which results in delays and is extremely expensive in terms of bandwidth [3]. Furthermore, scalability and mobility support difficulties for vehicular communications were highlighted by the IEEE 802.11p Long-Term Evolution (LTE) standards, which were first proposed for vehicular communications [4]. Therefore, it is expected that the 5G cellular networks will enhance ITS-based services through features like enormous bandwidth, massive connectivity, and low latency [5], [6].

Fog computing is a novel paradigm in computing that was introduced. The traditional cloud computing model and associated services are extended to the network level by this

TABLE I
NOTATION TABLE

Notation	*Description*
r_i	Set of Random numbers
U_i, FN_j	Vehicle user and Fog node
CS	Cloud Server
ID_{U_i}	U_i Identity
$D_{ID_i}, D_{ID_j}, SK_{cs}$	Secret keys of U_i , FN_j and CS
SC	Smart card
A	Adversary
$h(.)$	Secure one-way hash function
$\oplus$	Bitwise XOR operation
$\|$	Concatenation operation

computing architecture. The characteristics that this paradigm offers include reduced latency, extensive geo-distribution, position awareness, greater mobility, and real-time service procedures [7]. The fog-based approach enables the sensors to transfer data to the closest fog devices, in contrast to the convectional central cloud-based systems. These fog devices have the ability to compute using the data gathered and assist in decision-making [8].As a result, fog computing offers a decentralized approach that lowers processing costs, bandwidth usage, and transmission latency. In the context of VANETs, fog computing also offers real-time traffic control, fast exposure of unsafe driving, early warnings, and immediate assistance.

When it comes to Vehicular Ad-Hoc Networks (VANETs), it is crucial to have strong security. Numerous scholars have put forth diverse approaches to address the particular difficulties presented by VANETs, each entailing a unique set of trade-offs and security considerations. In the context of VANET security, this data provides a comparative study of these systems, stressing their advantages and disadvantages as well as their areas of use.

Table II provides a comparison of security protocols in domains like VANETs. Key protocols include Zhen Li et al.'s [9] for insider attack resistance but no traceability and Xiong Li et al.'s [10] emphasizing anonymity without unlikeability support. Wazid et al.'s scheme [11] is cost-effective but lacks mutual authentication. Heetal [12] introduced an identity-based VANET authentication protocol in 2015, eliminating the need for bilinear pairing, with subsequent enhancements. [13] protects the OBU privacy but suspectible to conditional privacy.

The remaining sections of our paper are organized as follows: Section-II deals with motivation and contributions. In Section-III reviewing the protocol of Ma et al.'s. Section-IV presents the pitfalls of Ma et al.'s devised protocol. Section V presents the countermeasures to address security flaws in Ma et al.'s scheme and Section-VI concludes this paper.

II. MOTIVATION AND CONTRIBUTIONS

Ma et al. [14] developed a simple authentication protocol for the VANETs by combining a hash function and an XOR operation. They claim that their protocol meets all security requirements and privacy regulations for $VANET$. However, we have discovered that their protocol lacks vehicle anonymity and is vulnerable to impersonation attacks. In the following subsections, we will briefly discuss the shortcomings of Ma et al.'s protocol, while Table I provides a list of common notations.

A. Threat Assumption Model

An adversary A is considered as a potential attacker. He could be a member of the staff, a system administrator, or an outside attacker who listens in and takes information. An attacker can send or forge messages, listen in on discussions in the public channel, and participate in protocol operations as a legitimate protocol participant when he adopts the role of an external attacker. All without being detected by the intended protocol. We suppose that A is capable of the following:

- The public channel can be used to eavesdrop on and intercept information, and A has the ability to forge, change, delete, divert, or replay communications that are sent over it.
- A can retrieve saved parameters and data from a smart card that has been lost or stolen.
- A might be an administrator or privileged user behaving falsely, but legally.

III. REVIEWING THE MA ET AL.'S SCHEME

The vehicle, the fog node, and the cloud server are the three participants in the Ma et al. [14] protocol. Four phases of their protocol are discussed in the following subsections. Table I contains a list of the symbols used in the protocol.

A. Initialization

When the CS is employed to build system parameters, the security parameter k is used as input.

1) Through CS, a q-order additive group G with a generator P is chosen.
2) CS chooses $s \epsilon Z_q^*$ arbitrarily and determines $P_{pub} = sP$.
3) CS selects six cryptographic hashing techniques $h_i(i = 1, 2, 3, 4, 5, 6)$, where h_1 :{0,1}*×{0,1}* → Z_q^*, $h_2 : G \times G \rightarrow Z_q^*$, h_3 :{0,1}*×{0,1}$^* \times G \times G \times G \rightarrow Z_q^*$, h_4 :{0,1}*×{0,1}$^* \times G \times G \times G \times G \rightarrow Z_q^*$, $h_5 : G \times G \times G \times G \rightarrow Z_q^*$, h_6 :{0,1}*×{0,1}$^* \times G \times G \times G \times G \rightarrow Z_q^*$, System information is published by CS, prms= $\{k, q, P, G, P_{pub}, h_i\}$ while s remain a secret.

TABLE II
COMPARISON OF AUTHENTICATION SCHEMES

Author	Techniques used / Application area	Benefits	Drawbacks
Zhen li et al. [9]	lightweight mutual authentication protocol in fog-enabled social Internet of vehicles	Resist insider attacks	Does not Provides Traceability .
Xiong Li et al. [10]	Privacy-Preserving Authentication Protocol for VANETs	Anonymity	Unlikeability.
Wazid et al. [11]	Key management and user authentication scheme for fog computing services	Less communication and computation cost	Does not provide mutual authentication.
Heetal et al. [12]	Identity-based	less computational cost	Replay-attack
Lee et al. [13]	Honey List-Based Authentication Protocol for Vehicular AdHocNetworks	Protects OBU privacy against adversaries	Limited to conditional privacy; requires a trusted authority TA for identity tracking

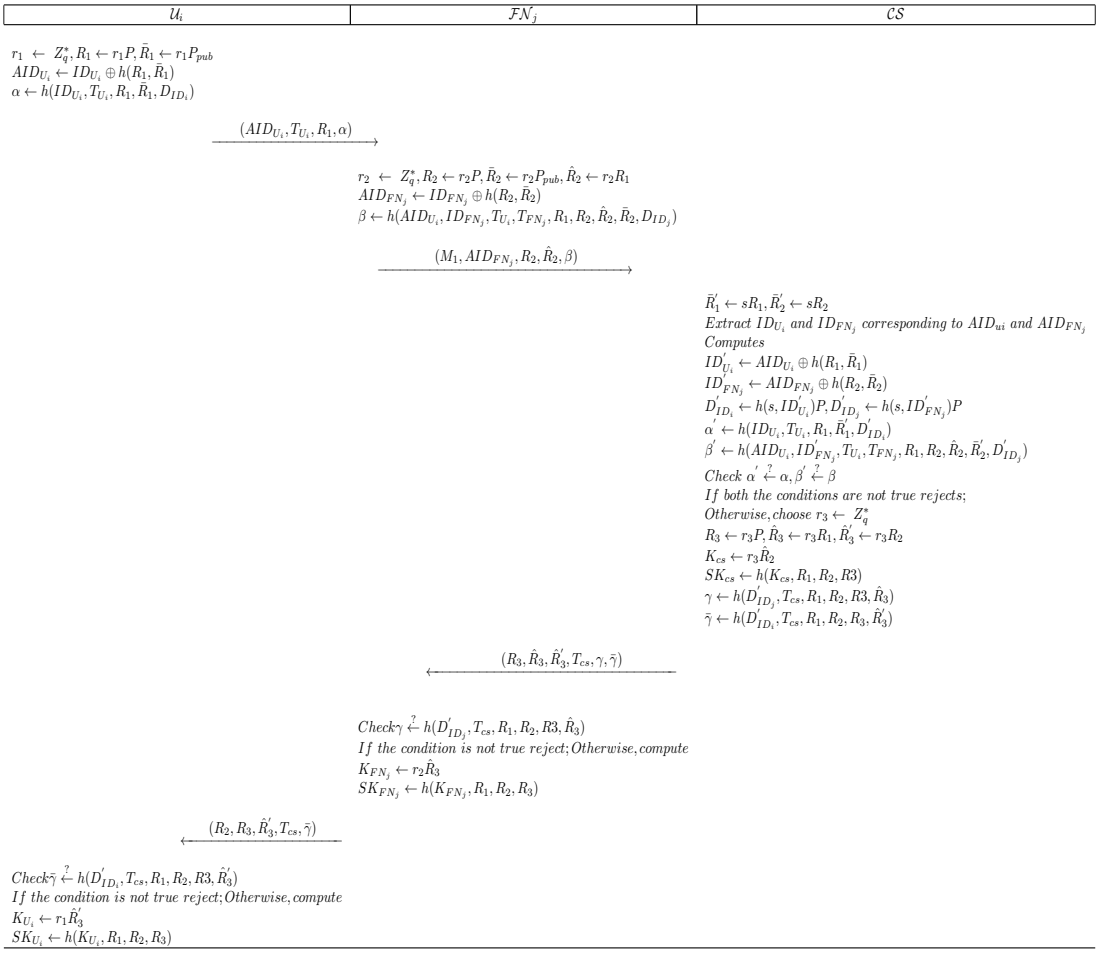

Fig. 1. Authentication and Key Agreement Phase

B. V_i Registration Phase

To receive a private key, the vehicle user U_i, registers with CS.

1) The identification ID_{U_i} of U_i is transmitted to the CS.
2) When CS receives ID_{U_i}, it computes $D_{ID_i} = h(s, ID_{U_i})P$ and stores (ID_{U_i}, D_{ID_i}) on a smart card. The smart card is finally given to U_i via CS.

C. FN_j Registration Phase

The fog node FN_j registers with CS and receives a secret key.

1) FN_j sends CS its ID_{FN_j} identity.
2) CS determines $D_{ID_j} = h(s, ID_{FN_j})P$ and returns D_{ID_j} to CS over a private medium.
3) FN_j completes the registration and secretly stores D_{ID_j}.

D. Authentication and Key Agreement Phase

The authentication and key agreement phases are performed independently by the cloud server CS, the fog node FN_j, and the vehicle user U_i in order to create a secure connection and set up a shared session key.

1) U_i chooses a arbitrary nonce $r_1 \epsilon Z_q^*$. T_{U_i} represents the present time-stamp. The U_i compute $R_1 \leftarrow r_1 P$, $\bar{R}_1 \leftarrow r_1 P_{pub}$, $AID_{U_i} \leftarrow ID_{U_i} \oplus h(R_1, \bar{R}_1)$, $\alpha \leftarrow h(ID_{U_i}, T_{U_i}, R_1, \bar{R}_1, D_{ID_i})$ and transmits $(AID_{U_i}, T_{U_i}, R_1, \alpha)$ to FN_j.

2) After determining the T_{U_i} freshness, FN_j chooses $r_2 \leftarrow Z_q^*$ arbitrarily. The current time-stamp is represented by T_{FN_j}. $R_2 \leftarrow r_2 P, \bar{R}_2 \leftarrow r_2 P_{pub}, \hat{R}_2 \leftarrow r_2 R_1$, $AID_{FN_j} \leftarrow ID_{FN_j} \oplus h(R_2, \bar{R}_2)$ and $\beta \leftarrow h(AID_{U_i}, ID_{FN_j}, T_{U_i}, T_{FN_j}, R_1, R_2, \hat{R}_2, \bar{R}_2, D_{ID_j})$ are all calculated by FN_j. Finally, FN_j transmits $(M_1, AID_{FN_j}, R_2, \hat{R}_2, \beta)$ to cloud server.

3) Cloud server CS verifies the freshness of T_{U_i} and T_{FN_j}. Afterward CS computes $\bar{R}_1^{'} \leftarrow sR_1, \bar{R}_2^{'} \leftarrow sR_2$, $ID_{U_i}^{'} \leftarrow AID_{U_i} \oplus h(R_1, \bar{R}_1)$, $ID_{FN_j}^{'} \leftarrow AID_{FN_j} \oplus h(R_2, \bar{R}_2)$, $D_{ID_i}^{'} \leftarrow h(s, ID_{U_i}^{'})P, D_{ID_j}^{'} \leftarrow h(s, ID_{FN_j}^{'})P$, $\alpha^{'} \leftarrow h(ID_{U_i}, T_{U_i}, R_1, \bar{R}_1^{'}, D_{ID_i}^{'})$, $\beta^{'} \leftarrow h(AID_{U_i}, ID_{FN_j}^{'}, T_{U_i}, T_{FN_j}, R_1, R_2, \hat{R}_2, \bar{R}_2^{'}, D_{ID_j}^{'})$. CS verifies $\alpha^{'} \stackrel{?}{\leftarrow} \alpha, \beta^{'} \stackrel{?}{\leftarrow} \beta$ CS denies the request if one of the two equations is wrong. If not, CS chooses $r_3 \leftarrow Z_q^*$ arbitrarily and computes $R_3 \leftarrow r_3 P, \hat{R}_3 \leftarrow r_3 R_1, \hat{R}_3^{'} \leftarrow r_3 R_2$, $K_{cs} \leftarrow r_3 \hat{R}_2$, $SK_{cs} \leftarrow h(K_{cs}, R_1, R_2, R3)$, $\gamma \leftarrow h(D_{ID_j}^{'}, T_{cs}, R_1, R_2, R3, \hat{R}_3)$, $\bar{\gamma} \leftarrow h(D_{ID_i}^{'}, T_{cs}, R_1, R_2, R_3, \hat{R}_3^{'})$, where T_{cs} time-stamp. Finally, CS transmit $(R_3, \hat{R}_3, \hat{R}_3^{'}, T_{cs}, \gamma, \bar{\gamma})$ to FN_j.

4) FN_j verifies the current time-stamp T_{cs} and determines whether $\gamma \stackrel{?}{\leftarrow} h(D_{ID_j}^{'}, T_{cs}, R_1, R_2, R3, \hat{R}_3)$ holds. If not, the request is canceled by FN_j. Otherwise, FN_j determines $K_{FN_j} \leftarrow r_2 \hat{R}_3$ and $SK_{FN_j} \leftarrow h(K_{FN_j}, R_1, R_2, R_3)$. FN_j finally transmit $(R_2, R_3, \hat{R}_3^{'}, T_{cs}, \bar{\gamma})$ to U_i.

5) U_i examines T_{CS} freshness and versifies $\bar{\gamma} \stackrel{?}{\leftarrow} h(D_{ID_i}^{'}, T_{cs}, R_1, R_2, R3, \hat{R}_3^{'})$ If not valid, U_i terminate the session. Else U_i computes $K_{U_i} \leftarrow r_1 \hat{R}_3^{'}$ and $SK_{U_i} \leftarrow h(K_{U_i}, R_1, R_2, R_3)$.

IV. Pitfalls of Ma et al.'s Scheme

The study evaluates the fog-based vehicle ad hoc network protocol proposed by Ma et al.'s [14]. In this analysis, we examine the limitations of the devised protocol by Ma et al. Upon thorough examination, we demonstrate the various vulnerabilities of their protocol, including the absence of vehicle anonymity and susceptible to vehicle user impersonation attack.

A. Vehicle User Impersonation Attack

According to the Ma et al. [14] approach, during the registration phase as stated above in sub-section III-B, the user identity, ID_{U_i} and secret key, D_{ID_i}, are stored on the U_i smart card by cloud server CS. Since ID_{U_i} and D_{ID_i} is kept in plain-text on U_i smart card, an A can use a smart card stolen attack to access ID_{U_i} and D_{ID_i}. As a result, an A can steal these parameters from the U_i smart card and use them to launch an U_i impersonation attack. Thus, an A can easily impersonate a legal U_i after having ID_{U_i} and D_{ID_i}. The following actions are taken by the attacker in order to pretend as an authentic U_i:

Step1: After accessing ID_{U_i} and D_{ID_i} A can quickly create a legitimate request message. A performs the following calculations:

$$r_1 \leftarrow Z_q^*, R_1 \leftarrow r_1 P, \bar{R}_1 \leftarrow r_1 P_{pub} \tag{1}$$

$$AID_{U_i} \leftarrow ID_{U_i} \oplus h(R_1, \bar{R}_1) \tag{2}$$

$$\alpha \leftarrow h(ID_{U_i}, T_{U_i}, R_1, \bar{R}_1, D_{ID_i}) \tag{3}$$

A sends $(AID_{U_i}, T_{U_i}, R_1, \alpha)$ to FN_j.
Step2: Upon receiving $(AID_{U_i}, T_{U_i}, R_1, \alpha)$ the FN_j, inspects the freshness of T_{U_i}. Upon confirmation, FN_j selects arbitrary nonce:

$$r_2 \leftarrow Z_q^*, R_2 \leftarrow r_2 P, \bar{R}_2 \leftarrow r_2 P_{pub}, \hat{R}_2 \leftarrow r_2 R_1 \tag{4}$$

$$AID_{FN_j} \leftarrow ID_{FN_j} \oplus h(R_2, \bar{R}_2) \tag{5}$$

$$\beta \leftarrow h(AID_{U_i}, ID_{FN_j}, T_{U_i}, T_{FN_j}, R_1, R_2, \hat{R}_2, \bar{R}_2, D_{ID_j}) \tag{6}$$

Step3: A transmits $(M_1, AID_{FN_j}, R_2, \hat{R}_2, \beta)$ to CS. Then CS determines:

$$\bar{R}_1^{'} \leftarrow sR_1, \bar{R}_2^{'} \leftarrow sR_2 \tag{7}$$

$$ID_{U_i}^{'} \leftarrow AID_{U_i} \oplus h(R_1, \bar{R}_1) \tag{8}$$

$$ID_{FN_j}^{'} \leftarrow AID_{FN_j} \oplus h(R_2, \bar{R}_2) \tag{9}$$

$$D_{ID_i}^{'} \leftarrow h(s, ID_{U_i}^{'})P, D_{ID_j}^{'} \leftarrow h(s, ID_{FN_j}^{'})P \tag{10}$$

$$\alpha^{'} \leftarrow h(ID_{U_i}, T_{U_i}, R_1, \bar{R}_1^{'}, D_{ID_i}^{'}) \tag{11}$$

$$\beta^{'} \leftarrow h(AID_{U_i}, ID_{FN_j}^{'}, T_{U_i}, T_{FN_j}, R_1, R_2, \hat{R}_2, \bar{R}_2^{'}, D_{ID_j}^{'}) \tag{12}$$

Next, check in CS to see if $\alpha^{'} \stackrel{?}{\leftarrow} \alpha, \beta^{'} \stackrel{?}{\leftarrow} \beta$ is either true or false. If it is correct, Next, CS calculates:

$$r_3 \leftarrow Z_q^*, R_3 \leftarrow r_3 P, \hat{R}_3 \leftarrow r_3 R_1, \hat{R}_3^{'} \leftarrow r_3 R_2 \tag{13}$$

$$K_{cs} \leftarrow r_3 \hat{R}_2 \tag{14}$$

$$SK_{cs} \leftarrow h(K_{cs}, R_1, R_2, R3) \tag{15}$$

$$\gamma \leftarrow h(D_{ID_j}^{'}, T_{cs}, R_1, R_2, R3, \hat{R}_3) \tag{16}$$

$$\bar{\gamma} \leftarrow h(D^{'}_{ID_i}, T_{cs}, R_1, R_2, R_3, \hat{R}^{'}_3) \quad (17)$$

CS transmits $(R_3, \hat{R}_3, \hat{R}^{'}_3, T_{cs}, \gamma, \bar{\gamma})$ to FN_j

Step4: After receiving, $(R_3, \hat{R}_3, \hat{R}^{'}_3, T_{cs}, \gamma, \bar{\gamma})$, CS validate the freshness of T_{cs} and then verifies:

$$\gamma \stackrel{?}{\leftarrow} h(D^{'}_{ID_j}, T_{cs}, R_1, R_2, R3, \hat{R}_3) \quad (18)$$

The session is ended by the FN_j if this verification fails. If not, it calculates:

$$K_{FN_j} \leftarrow r_2 \hat{R}_3 \quad (19)$$

$$SK_{FN_j} \leftarrow h(K_{FN_j}, R_1, R_2, R_3) \quad (20)$$

Step5: After receiving, $(R_2, R_3, \hat{R}^{'}_3, T_{cs}, \bar{\gamma})$, U_i verifies the freshness of time-stamp T_{cs} and then verifies:

$$\bar{\gamma} \stackrel{?}{\leftarrow} h(D^{'}_{ID_i}, T_{cs}, R_1, R_2, R3, \hat{R}^{'}_3) \quad (21)$$

$$K_{U_i} \leftarrow r_1 \hat{R}^{'}_3 \quad (22)$$

$$SK_{U_i} \leftarrow h(K_{U_i}, R_1, R_2, R_3) \quad (23)$$

The A can easily pass for an authorized vehicle user in this manner. The system of Ma et al. [14] provides the potential for a vehicle-user impersonation attack, which is proven.

B. User Anonymity violation

The privacy of user identities is a significant concern in VANETs because malicious entities can exploit them to track the users' location, movement patterns, login history, and transaction history, simply by knowing the vehicle users' identity. As we have discussed in sub-section III-B, user identity is revealed through smart card stolen attacks; therefore, based on that, we can claim that user anonymity is violated here. Hence, Ma et al.'s protocol fails to ensure the users' anonymity.

V. Countermeasure for Flaws in Ma et al.'s protocol

In Ma et al.'s [14] devised protocol, a major concern is the storage of ID_{U_i} and D_{ID_i} in plain text on U_i's smart card, which compromises user anonymity and exposes them to vehicle user impersonation attacks. To address issues, it is vital to design the scheme in a way that encrypts the secret credentials by XOR-ing them with other parameters. Additionally, a verification check should be embedded into the smart card to detect incorrect data input, such as erroneous identity information, and display an error message immediately. By implementing these measures, the devised protocol would effectively protect the anonymity and resilient against vehicle users impersonation attack.

VI. Conclusion

A fog-based authentication and key agreement protocol in vehicular ad-hoc networks was presented by Ma et al. Our cryptanalysis reveals that the system proposed by Ma et al. is vulnerable to a vehicle user impersonation attack, and it does not ensure user anonymity, Consequently, Ma et al.'s protocol is not practical for VANETs. We have proposed several solutions to address the vulnerabilities in Ma et al.'s protocol.

References

[1] K.-K. R. Choo, R. Lu, L. Chen, and X. Yi, "A foggy research future: Advances and future opportunities in fog computing research," pp. 677–679, 2018.

[2] A. Alrawais, A. Alhothaily, C. Hu, and X. Cheng, "Fog computing for the internet of things: Security and privacy issues," *IEEE Internet Computing*, vol. 21, no. 2, pp. 34–42, 2017.

[3] M. Abdalla, P.-A. Fouque, and D. Pointcheval, "Password-based authenticated key exchange in the three-party setting," *IEE Proceedings-Information Security*, vol. 153, no. 1, pp. 27–39, 2006.

[4] A. Armando, D. Basin, J. Cuellar, M. Rusinowitch, and L. Viganò, "Avispa: automated validation of internet security protocols and applications," *ERCIM News*, vol. 64, no. January, pp. 66–69, 2006.

[5] T. A. de Melo, F. D. de Oliveira, R. S. Semente, X. C. Benjamim, and A. O. Salazar, "Winss: A simulation tool of the ieee 802.15. 4 standard for network simulator 2," in *2016 1st International Symposium on Instrumentation Systems, Circuits and Transducers (INSCIT)*. IEEE, 2016, pp. 43–48.

[6] P. Hu, H. Ning, T. Qiu, H. Song, Y. Wang, and X. Yao, "Security and privacy preservation scheme of face identification and resolution framework using fog computing in internet of things," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1143–1155, 2017.

[7] W. Abdul, Z. Ali, S. Ghouzali, B. Alfawaz, G. Muhammad, and M. S. Hossain, "Biometric security through visual encryption for fog edge computing," *IEEE Access*, vol. 5, pp. 5531–5538, 2017.

[8] D. Koo and J. Hur, "Privacy-preserving deduplication of encrypted data with dynamic ownership management in fog computing," *Future Generation Computer Systems*, vol. 78, pp. 739–752, 2018.

[9] Z. Li, Q. Miao, S. A. Chaudhry, and C.-M. Chen, "A provably secure and lightweight mutual authentication protocol in fog-enabled social internet of vehicles," *International Journal of Distributed Sensor Networks*, vol. 18, no. 6, p. 15501329221104332, 2022.

[10] X. Li, T. Liu, M. S. Obaidat, F. Wu, P. Vijayakumar, and N. Kumar, "A lightweight privacy-preserving authentication protocol for vanets," *IEEE Systems Journal*, vol. 14, no. 3, pp. 3547–3557, 2020.

[11] M. Wazid, A. K. Das, J. J. Rodrigues, S. Shetty, and Y. Park, "Iomt malware detection approaches: analysis and research challenges," *IEEE access*, vol. 7, pp. 182 459–182 476, 2019.

[12] D. He, S. Zeadally, B. Xu, and X. Huang, "An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 12, pp. 2681–2691, 2015.

[13] J. Lee, G. Kim, A. K. Das, and Y. Park, "Secure and efficient honey list-based authentication protocol for vehicular ad hoc networks," *IEEE Transactions on Network Science and Engineering*, vol. 8, no. 3, pp. 2412–2425, 2021.

[14] M. Ma, D. He, H. Wang, N. Kumar, and K.-K. R. Choo, "An efficient and provably secure authenticated key agreement protocol for fog-based vehicular ad-hoc networks," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8065–8075, 2019.