A Lightweight Mutual Authentication Protocol for Internet of Vehicles

Myasar Tabany * and Mohiuddin Syed *

Networks, Security, and Systems Research Group, School of Physics, Engineering, and Computer Science, University of Hertfordshire AL10 9AB, Hatfield, Hertfordshire, UK
Email: m.tabany@herts.ac.uk (M.T.); sm19ahl@herts.ac.uk (M.S.)
*Corresponding author

Abstract—**In recent times, growth in the number of vehicles equipped with smart and complex electronics has been exponential and will only further increase in the future, resulting in more and more connected vehicles on road. This has led to the rise of a concept called Internet of Vehicles (IoV) capable of providing a wide range of applications, such as driver/passenger safety, entertainment, traffic efficiency, reduced traffic, pollution control etc. Basically, IoV is a large network containing multiple entities such as vehicles, portable electronic devices carried by pedestrians, Road-Side Units (RSU), traffic lights etc. Such a large concept involves a lot of effort, research, planning, and challenges. One out of many challenges in IoV is the strong and secure authentication of the vehicles attempting to connect to the network. This project proposes a lightweight mutual authentication scheme which enables the vehicle and the server to mutually authenticate each other before establishing a connection. Since it is a crucial requirement in IoV scenario, the proposed protocol combines eXclusive OR (XOR) and hashing operations to ensure lightweightness. Furthermore, the protocol is designed to protect against common attacks that entities in IoV suffer from. The security and performance analysis of the proposed protocol conducted in this project demonstrates that the authentication scheme satisfies the performance and security requirements of IoV. Throughout the security analysis phase, the protocol was found to defend against all common attacks in IoV. During computational cost calculation, it was found that the protocol consumes 0.018ms to execute on a single desktop setup, making it suitable to be used in the IoV environment.**

Keywords—**Internet of Vehicles (IoV), mutual authentication, security, communication**

I. Introduction

In today's world, the internet can be accessed from almost everywhere in a city. With more and more devices being internet enabled, it has paved the way for the emergence of Internet of Things (IoT). IoT is a worldwide network which enables the communication between such smart objects. When the concept of IoT is restricted to only vehicles, it is called as Internet of Vehicles (IoV) [1]. The number of cities, vehicles and population of smart devices are growing at an exponential rate resulting in more traffic management problems. IoV is an attempt to provide better traffic management by enabling the communication between vehicles, vehicles and vehicle owners, vehicles and a centralized server along with the communication between the centralized server and third parties such as police, ambulance and fire-engine services [1]. Having components of several types and in large numbers involved in such a widespread network poses two major drawbacks:

(a) Security: IoV may become extremely vulnerable to cyber-attacks [2]. Zhang *et al.* [3] stated several vulnerabilities, threats, and challenges present in IoV, specifically in vehicle-to-vehicle communication. Since there are large numbers of connection points present in the IoV network, just one loophole in any of the connection points can expose the system to the threat of being compromised by malicious actors. Presently, the attacks on authentication in IoV are as follows:

(i) Camouflage attack: Wu *et al.* [4] states that attackers use login credentials of existing users to enter the system and spread false messages.

(ii) Sybil attack: "A node (component of the network) behaves like a legitimate one but creates numerous number of false identities which confuses the centralized authority (server) to mistake the attacking node as a real node and vice-versa";

(iii) Tunnel attack: The attacker connects two or more entities of the network which are physically distant from each other through a tunnel or other communication channel to make those entities behave like neighbours [4];

(iv) GPS Spoofing: Most navigation systems use the strongest signal; in this attack the attacker creates a strong false signal which overrides the legitimate satellite signal. Thus, spoofing the vehicle to make it available in different locations [4];

(v) Location tracking attack: "the attacker collects data broadcast from the vehicle Multiple messages track the driving route of the vehicle by using its pseudo-identity to obtain private information about the owner" [4].

(b) Network: Installing every vehicle with a device and sensors is required for the deployment of IoV. While this is already a very difficult task, a bigger challenge is presented with the load generated by so many vehicles on the server(s) [1]. Other challenges include small computing capacity of the devices installed in the vehicles which

Manuscript received June 21, 2023; revised August 4, 2023; accepted October 20, 2023; published February 5, 2024.

doi: 10.12720/jait.15.2.155-163

requires lightweight communication protocols with lesser computation costs to be designed in order to perform various operations involved in IoV environment. Interference in wireless communications from neighbouring vehicles and infrastructure in a highly dense urban scenario may result in packet loss and signal attenuation [5]. Hence, it is necessary to develop an authentication scheme which is secure, fast and does not require a lot of computation by devices of smaller capacities. This criterion is held for all devices that wants to exchange information with the cloud.

This paper is focused on registering and authenticating a vehicle to the IoV network using a mutual authentication scheme and conducting a security review to evaluate security of the protocol against common authentication attacks in IoV.

In this paper, a secure and lightweight authentication protocol is proposed that enables mutual authentication and session key agreement for an IoV scenario. The protocol is purely based on cryptographic hash functions and eXclusive OR (XOR) operations, which reduce computational costs and communication costs.

Our major contributions are:

- We designed a mutual authentication protocol for an IoV scenario.
- We recognised the significance of the lightweight characteristic and included only those cryptographic operations that satisfy the property.
- A key agreement is made between the entities in order to improve security.
- To demonstrate the accuracy, we created the full system for registration and authentication into a python program.
- The performance metrics based on communication and computation costs demonstrate the effectiveness of the proposed protocol.

The rest of the paper is organised as follows. In Section II, we describe the existing works. In Section III, we explain the architecture of our proposed model. This includes defining the participants involved and the flow of communication that takes place among them. In Section IV, we describe our protocol containing two phases. In Section V, we perform the security analysis of the proposed authentication scheme and examine how it performs against the different possible attacks. Section VI deals with the protocol implementation, which is done using the python programming language on a single desktop. In Section VII, we observe the performance of the proposed protocol based on the total cost incurred while performing computation and communication. Finally, in Section VIII, we include a conclusion and future works.

II. Related Works

A. Existing Works in IoV

The existing research works in IoV are based on various concepts. Some of the works were reviewed and are as follows: Several studies have been carried out in the field of privacy protection. Their work focusses on the protection of privacy of the user when they travel from their home country to another country. They introduced an authentication scheme which registers a user on the foreign server without the involvement of their home server.

B. Lightweight Authentication Based IoV Research

In 2008, Wu *et al.* [6] introduced an anonymous authentication scheme. In 2012, Mun *et al.* [7] proposed an improved scheme which uses Elliptic Curve Diffie–Hellman (ECDH) to overcome the weaknesses of Chia-Chun work. The advantage of this scheme was that it was resistant to man-in-the-middle attacks and provided mutual authentication.

In 2014, Zhao *et al.* [7, 8] found that the scheme proposed by Mun was vulnerable to impersonation attacks and insider attacks and could not provide proper mutual authentication. Therefore, Zhao [8] proposed an anonymous authentication scheme for roaming service in global mobility networks. The scheme's main features are anonymity, local password verification, resilience to various attacks, and so on. They claim that the scheme is appropriate for low-power and resource-constrained mobile devices and hence ready for real-world deployment. The scheme's computation cost, on the other hand, is high.

In 2017, Shen and Mu [9] proposed a two-party roaming authentication agreement based on Elliptic Curve Cryptography and session key encryption. They claimed that their proposed protocol had lower computational cost when compared to other existing protocols. The protocol adopted a mixed-key cryptosystem to improve a two-party roaming authentication agreement.

In 2019, Chen *et al.* [10, 11] introduced an improvement patch on Ying and Nayak's authentication protocol for IoV and claimed to have overcome the short comings of the original protocol. However, Vasudev *et al.* [12] claimed in 2020 that the storage cost of the patched protocol was too high and that their protocol performed better than the existing ones. They designed a lightweight mutual authentication and key agreement protocol based entirely on hash and XOR functions. A smart card is issued to the vehicles based on their identity and passwords, which are then used for authentication and communication.

This project is built on Vasudev *et al.* [12], system model while adapting the lightweight mutual authentication protocol proposed by Wu *et al.* [13]. The scheme was originally made for Wireless Body Area Network (WBAN) and this project aims to use the mutual authentication scheme in IoV environment [13]. This scheme only uses XOR and one-way hash operations, which not only reduces communication consumption but also ensures security and realizes a truly lightweight anonymous mutual authentication and key agreement protocol.

III. Proposed Model Architecture

In this section, we explain the architecture model used in the communication between vehicle and the Trusted Authority (T.A). The system model in this project includes three entities: (i) Trusted Authority (T.A); (ii) Registration Authority (R.A); (iii) Vehicle device (V). Each vehicle is fitted with a vehicle device which enables the communication between the vehicle and the T.A/R.A. They communicate with each other through wireless interface such as Wi-Fi or Bluetooth. The R.A is responsible for registering a vehicle and providing a smart card to the vehicle owner to authenticate themselves and log into the network. The T.A is responsible for mutually authenticating itself and the vehicle, and also acts as a medium to provide Vehicle to Vehicle (V2V), vehicle to Road-Side Unit (RSU) and Vehicle to Mobile (V2M) device communications.

IV. Proposed Lightweight Protocol in an IoV

This section explains the proposed mutual authentication scheme in a step-by-step format starting with the system model, adversary model and moving onto explaining the various phases involved in the proposed protocol.

This protocol is designed to enable mutual authentication between T.A and V. The authentication process will determine the legitimacy of various entities involved in the IoV network while ensuring that the security and hardware requirements in IoV are satisfied. Table I conveys the notations used in the communication process.

TABLE I. Symbols Used in the Proposed Protocol

Symbol	Description
T.A	Trusted authority
R.A	Registering authority
V	Vehicle/Car
IDc	User ID of car
PWc	Password of car
a_n , b_n	Authentication parameters
$K_{R.A}$	Master key for registration authority
$ID_{R.A}$	ID provided to registration authority
⊕	XOR operation
$\Vert$	Concatenation operation
h(.)	Secure one-way hash
r_c	Random number generated by car
r_c*	When T.A calculates r_c for verification
t_1	Time stamp
x_n	Auxiliary parameter required for authentication
x_n*	When T.A calculates x_n for verification
tid_n	Temporary ID of car
tid_n*	When T.A calculates tid_n for verification
Δt	Average time taken for message to be transferred between V and T.A
t*	Time when the T.A receives the message
r^+	Random number generated by T.A
r*	When vehicle calculates r^+ during session key verification
k^+	Temporary key generated by T.A
$n_{T.A}$	Nonce generated by T.A
α, β, γ, H	Authentication parameters
H*	When vehicle calculates H during session key verification
a_N^+, b_N^+	Authentication parameters
K_s	Session key calculated by T.A
K_s*	Session key calculated by V

A. System Model

After registration of the vehicle, the R.A forwards some parameters to T.A which provides an advantage to R.A by not involving every time at the authentication process, reducing the computations taking place at R.A. Authenticity checks are conducted using the forwarded parameters. Similarly, some parameters are stored on a smart card which is provided to the user of each vehicle to make the process secure and time efficient. The values stored on the smart card are used during authentication checks. The network model of the proposed protocol is shown in Fig. 1. Here, the left portion depicts registration, and the right portion shows communication. It is clear that R.A is only involved in the registration and forwards values to T.A. Similarly, in the communication phase, the vehicle should communicate with the T.A and prove authenticity. On successful authentication, the vehicle can request information from the T.A. All communications are bidirectional. So, the vehicles and R.A, R.A and T.A and vehicles and T.A are shown in double arrows. The system model is based on the following assumptions:

- R.A and T.A are trusted entities and cannot be compromised.
- Only the registered vehicles can take part in the IoV communication.
- The registered users never share their credentials (smart card) with an untrusted person.

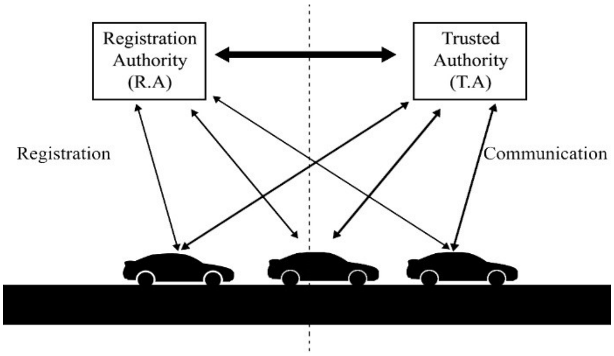

Fig. 1. Registration phase.

B. Adversary Model

IoVs are open wireless networks, which makes it prone to several adversarial behaviours, these adversarial behaviours can critically affect the working of the system.

Following are the assumptions on the types of attacks an attacker/adversary (**Å**) can perform:

- Exchange of information is done through insecure channels, therefore, the **Å** can attempt all attacks possible in IoV.
- If an **Å** gains access to essential credentials such as user id, passwords, nonce etc., they can cause delays in information exchange and attack the entire system.
- **Å** can pose as a trusted entity and perform impersonation attack(s).
- If **Å** steals a smart card, they can use it to make further computations and calculate other values.
- **Å** can perform a password guessing attack.
- **Å** can perform a man-in-the-middle attack by intercepting messages from various sessions.

C. Phases Involved in the Proposed Protocol

The proposed protocol consists of various phases such as registration, login, authentication, and session key verification.

1) Registration phase: In order to exchange information from the T.A, the vehicles are required to register themselves with the R.A. The R.A issues a smart card consisting of parameters required for authentication and communication when a vehicle registers itself. Following is a description of the registration process shown in Algorithim 1.

- The user/vehicle (V) chooses a user ID and password < ID_c, PW_c >. These parameters are sent to R.A over a secure channel. A channel is considered secured if it ensures the confidentiality and integrity of the data that is being transmitted.
- The R.A calculates two parameters an and bn which are unique for each vehicle. The value of an is calculated as < $a_n = K_{R.A} \oplus PW_c$ > ,where $K_{R.A}$ is a secret key assigned to the R.A by T.A during system set up and b_n is calculated as < $b_n = ID_c \oplus h(PW_c \parallel K_{R.A})$ >. The R.A stores a_n and b_n as parameters in a smart card and sends the smart card to the user through a secure channel, it also forwards those parameters to T.A along with ID_c.

Algorithm 1. Registration Phace

Vehicle (V) **Registration Authority (R.A)**

Input ID_c, PW_c

$\{ID_c, PW_c\}$ →

Secure Channel Secret Key: $K_{R.A}$

$a_n = K_{R.A} \oplus PW_c$

$b_n = ID_c \oplus h(PW_c \parallel K_{R.A})$

Smart Card (SC)= $\{a_n, b_n\}$

Smart Card -{a_n, b_n ← {Smart Card}

Secure Channel

2) Login and authentication phase: After registration, if the V wishes to login, it needs to authenticate itself with the T.A to ensure validity of V and provide defence againstimpersonation frommalicious party. Authentication is also performed by V when it receives information from the T.A to make sure that it is the actual server and not an impersonator. Following is a description of the login and authentication phase shown in Algorithim 2.

- The user/vehicle (V) logs in using the smart card provided to them. The V generates a random number r_c and current time stamp t_1. V calculates two parameters: < $x_n = r_c \oplus a_n$ > and < $tid_n = h(ID_c \oplus r_c \parallel t_1)$ >, which are used to authenticate V. Finally, $\{x_n, tid_n, t_1, ID_c\}$ is forwarded to T.A as a message through an insecure channel.
- The T.A checks the validity of the timestamp t_1 by calculating < $t^*- t_1$ >. If the difference between t^* and t_1 is more than the threshold value, the connection is refused. The server recalculates three parameters: < $r_c^* = x_n \oplus a_n$ >, < $x_n^* = r_c^* \oplus a_n$ > and < $tid_n^* = h(ID_c \oplus r_c^* \parallel t_1)$ >, this ensures integrity and verifies that the request is coming from an actual user and not a malicious one. The T.A then compares the values of < x_n^* and tid_n^* > with < x_n and tid_n >. If any of these values do not match, the connection is denied.
- The T.A generates three parameters: Random number r^+, temporary key k^+ and nonce $n_{T.A}$ and calculates < $\alpha = r^+ \oplus a_n$ > , < $a_n^+ = k^+ \oplus n_{T.A}$ > , < $b_n^+ = ID_c^* \oplus h(k^+ \parallel K_{T.A})$ > , < $\beta = a_n^+ \oplus h(r^+ \parallel ID_c^*)$ > , < $\gamma = b_n^+ \oplus r^+$ > , < $H = h(r^+ \parallel ID_c^* \parallel \alpha \parallel \beta \parallel \gamma)$ > and session key < $K_s = h(r^+ \parallel ID_c^* \parallel b_n^+ \parallel x_n \parallel r_c)$. Finally, T.A forwards { α , β , γ , H , K_s} to V.
- The V calculates < $r^* = \alpha \oplus a_n$ > , < $H^* = h(r^* \parallel ID_c \parallel \alpha \parallel \beta \parallel \gamma)$ > , < $a_N^+ = \beta \oplus h(r^* \parallel ID_c)$ > and < $b_N^+ = \gamma \oplus r^*$ > all these values are calculated so that the V can calculate the value of $K_s^* = h(r^* \parallel ID_c \parallel b_N^+ \parallel x_n \parallel r_c)$. Finally, V compares the values of K_s and K_s^* to authenticate the T.A this protects the system from impersonation and man-in-the-middle attacks. The connection is successful if the values of K_s and K_s^* are equal, else connection is denied. Since this protocol involves authentication of both V and T.A with each other, it is a mutual authentication protocol.

Algorithm 2. Login and Authentication Phace

Vehicle (V) **Registration Authority (R.A)**

Input ID_c, PW_c

Generate random number: r_c

Generate time stamp: t_1

$x_n = r_c \oplus a_n$

$tid_n^* = h(ID_c \oplus r_c^* \parallel t_1)$

$\{x_n, tid_n, t_1, ID_c\}$

→ **Generation time stamp: t***

Insecure channel

$t^* - t_1$

$r_c^* = x_n \oplus a_n$

$x_n^* = r_c^* \oplus a_n$

$tid_n^* = h(ID_c \oplus r_c^* \parallel t_1)$

$tid_n = tid_n^*$

Generate random number r^+

Temporary key k^+

Nonce $n_{T.A}$

$\alpha = r_+ \oplus a_n$

$a_{n+} = k_+ \oplus n_{T.A}$

$b_{n+} = ID_{c^*} \oplus h(k_+ \; k_{T.A})$

$\beta = a_{n+} \oplus h(r_+ \; ID_{c^*} \parallel \alpha \parallel \beta \parallel \gamma)$

$\gamma = b_{n+} \oplus r_+$

$H = h(r_+ \parallel ID_{c^*} \parallel \alpha \parallel \beta \parallel \gamma)$

$K_s = h\,(r_+ \parallel ID_{c^*} \parallel b_{n+} \parallel x_n \parallel r_c)$

$\{\alpha, \beta, \gamma, H, Ks\}$

Insecure channel ←

$r^* = \alpha \oplus a_n$

$H^* = h\,(r^* \parallel ID_c \parallel \alpha \parallel \beta \parallel \gamma)$

$a_N^+ = \beta \oplus h(r^* \parallel ID_c)$

$b_k = \gamma \oplus r^*$

$K_s^* = h\,(r^* \parallel ID_c \parallel b_{n+} \parallel x_n \parallel r_c)$

$K_s^* = K_s$

V. Security Analysis

In this section, a brief discussion of the security requirements and relevant attacks in IoV is provided and how the proposed protocol defends against those attacks. This section also provides an overview of the computation and communication cost incurred by the protocol. Furthermore, this chapter also includes detail on how the protocol was implemented.

A. Security Requirements in IoV Environment

1) Confidentiality: Although certain information in IoV needs to be public, still the privacy and the security of the customers or the business involved in IoV is the utmost important part of the paradigm. Hence, the private or delicate data should not be known by the adversary (encryption being the solution). Eavesdropping will allow the adversary to analyse the traffic or the data without interfering in the network, ID disclosure, traffic analysis, and malware [14]. The proposed scheme provides confidentiality by using encryption. Encryption is done using XOR and hashing operations. Furthermore, random numbers, nonce and temporary key is used to make encryption stronger.

2) Integrity: The data sent, and the data received should be identical, that is, no distorting of the data in the way on the network. Attacks like message tampering, masquerading, black hole, grey hole, fabrication, and malware (use of hashing technologies) are possible [14]. To ensure integrity, the proposed protocol uses hashing on encrypted information.

3) Availability: One of the basic responsibilities of the system is to be available to all the legitimate users. Few possible attacks on availability are DoS, black hole, grey hole, spamming throws spam messages throughout the network which consumes lot amount of bandwidth affecting the latency of the normal packets in the network, jamming and malware attacks [14, 15]. Availability is provided by the use of symmetric key encryption along with verification and recalculation of messages sent and received between the vehicle and T.A.

4) Authentication: No imitation of the vehicles sending the data should be allowed. The vehicle, actuator or sensor who has sent the data should be the true sender or the vehicle it is claiming to be. The receiving sensor should not be spoofed by the false sender of the data claiming the innocent sender without Right Identity (ID) [14]. Some attacks on authentication are sybil attacks, Global Positioning System (GPS) spoofing, Black hole attack, Worm hole attack, Fabrication attack, replay attack, message tampering, masquerading attack and malware. The proposed scheme provides mutual authentication between the vehicle and T.A. Both entities, authenticate each other and also verify the information by recalculating values in messages received by each of them.

5) Non-repudiation: Any emergency accidental cases on road requires to identify the correct culprit. In order to fulfil this requirement, it is necessary for all the involved users within the accidental communication range to not be able to deny any sent message [14]. Non-repudiation is provided by including the username of the user/vehicle into encryption parameters during authentication.

6) Scalability: The essence of a good connected vehicular network lies in the fact of ease in increasing the network load and nodes. Hence, an increase in the network size arises security issues on scaling a network. Hence, scalability becomes an important issue in the requirements [16].

7) Time constraint or freshness: IoV is all about real time situations where any delay could be hazardous. Hence, the emergency warnings and signals should be delivered on time without any tampering in order to implement the correct results. This requirement would stop various replay and time-based attacks. Moreover, the foremost requirement of authentication should also be done without delay to flow the authenticated messages in the network [14–16]. Freshness is provided by the proposed scheme by the use of time stamp. The vehicle generates a time stamp and includes it in the message before sending it to the T.A. Later, T.A checks the timestamp against the threshold time value to ensure freshness and the use of timestamp also help in detecting/preventing time-based attacks.

8) Forward secrecy: IoV is a type of network where the nodes are in continuous mobility. Hence, the membership of a node towards a place changes continuously. Thus, it becomes an utmost importance that the network needs to be refreshed every time any node makes an entry or exit in the network to maintain privacy. If any vehicle node leaves an IoV network, the vehicle should not be exposed to the messages after its exit from the network [14]. Forward secrecy is out of the scope of this work since the proposed protocol is focused on authenticating a user into the network and not focused on the exchange of information that takes place after authentication.

9) Backward secrecy: If any new vehicle node joins an existing network, the user of the joined vehicle should not know about the messages flown before its entry in the network [14]. Similar to forwards secrecy, this requirement is not the focus of this work as well.

B. Relevent Attacks in IoV

1) Sybil attack: The attacker creates some fictitious vehicles around a targeted vehicle for generating a jam signal while the path is clear enough which compels the user to take a different route. This fake jamming is done by using enumerable false ids for a single node giving an essence of more than one node [14]. This authentication protocol provides defence against sybil attacks by implementing strong mutual authentication between the T.A and the vehicle.

2) Masquerading attack: Similar to impersonation attack with a difference of having just one entity copying a real id of any node within the network, the adversary can spoof the receiver by creating two different senders with same identity [14]. This protocol provides security against this attack by encrypting usernames with encryption keys concatenated with the vehicle's password. It is difficult for an attacker to predict this. Moreover, the vehicle does not use their plain username to login.

3) Denial-of-Service (DoS) attack: In order to reduce the efficiency of the network, an attacker throws heavy legal message load on a particular communication channel more than its handling capacity to congest it in order to use the limited resources of the network illegally [14]. Protection against this attack is provided by using encryption in the proposed authentication scheme.

4) Distributed Denial-of-Service (DDoS) attack: The advanced version of DoS attack, known as Distributes DoS (DDoS) attack in which the attacker may attack system from outside to a single targeted system to agitate its functionality and network. Similar to the DoS attack, protection against DDoS attack is also provided by the use of encryption.

5) Eavesdropping attack: In this attack, the attacker does not participate actively in the communication within the network but becomes a part of a network from outside in order to attain some private confidential data of the drivers or the customers illegally to use it against their privacy without even letting them know. Protection against eavesdropping attack is provided by the use of encryption and time stamp verification between the vehicle and T.A.

6) Man-in-middle attack: An attacker impersonates between the sender and receiver there by receiving all the messages from the sender and sending forth to the receiver. It could be active or passive attack. Similar to eavesdropping protection against this attack is also provided by the use of encryption and the use of time stamps.

7) Message holding attack: This attack involves an active attacker in which an attacker drops some of the messages with demanding information that could affect the whereabouts of the road condition or the drivers state of requirement and eventually affect the driver's decision. It also lets the drivers save the message and the information with them which can be utilized in future within the network. The proposed protocol protects against such attacks by providing freshness to the messages those are exchanged during authentication.

8) Message deletion attack: An outsider envy, being an attacker, can delete the message which was supposed to be send before it got sent to halt the flow of intended information in the network. Since the proposed protocol provides non-repudiation of messages it provides protection against message deletion attacks.

9) Data manipulation attack: An attacker modifies the content of the messages to harm the decisions of the receiving entity paralyzing the overall system [14]. The use of random numbers, nonce and temporary key in the encryption process ensures that even if a communication is intercepted, the attacker will not be able to guess the correct values of certain parameters.

10) Data falsification attack: It is a type of an integrity attack which can create congestion and jam within the network by a little change in the data [14]. Data integrity is the best way to protect against such attacks. Therefore, this protocol uses hashing to provide integrity and protect against such attacks.

11) Malware attack: This attack corresponds to infusing malicious worms or viruses through files in the system to infect the network in future [14]. Only the most crucial data is exchanged between the vehicle and T.A. Moreover, each message is verified and recomputed to ensure that there is no additional information other than the required ones.

Table II describes how resistance towards different attacks is provided by the protocol:

TABLE II. RESISTANCE TOWARDS DIFFERENT ATTACKS

Attacks on	Types of Attacks	How They are Protected
Authentication	1. Sybil Attack 2. Masquerading Attack	1. This authentication protocol provides defence against sybil attacks by implementing mutual authentication between the T.A and the vehicle. 2. This protocol provides security against this attack by XORing usernames with the hash of $K_{R.A}$ concatenated with the vehicle's password. It is difficult for an attacker to predict this. Moreover, the vehicle does not use their plain username to login.
Availability	1. Denial-of-service (DoS) attack 2. Distributed Denial-of-service (DDoS) attack	1. The best way to protect against DoS attacks is by using an authentication system using Public Key Infrastructure (PKI) [14]. This protocol uses PKI to protect against such attacks. 2. DDoS attacks can be avoided by using symmetric key cryptographic techniques. [14]. This authentication protocol employs symmetric key cryptography
Confidentiality	1. Eavesdropping attack 2. Man-in-the-middle attack. 3. Message holding attack. 4. Message deletion attack	This protocol provides protection against these attacks by using encryption.
Integrity	1. Data manipulation attack 2. Data falsification attack 3. Malware attack	This protocol defends against integrity attacks by using a strong one-way hash function to hash messages during communication between vehicle, R.A and T.A.

C. Resistance towards Different Attacks

1) Impersonation attack

In this attack, the Å attempts to pass themself as one of the communication's participants.

a) Resistance against vehicle impersonation attack: The **Å** attempts to compute x_n and tid_n by randomly selecting rc and adding a time stamp t_1. However, guessing x_n without knowing an will lead to incorrect values. Similarly, guessing tidn without knowing $< h(ID_c \oplus r_c \|$

t_1) > will again lead to incorrect values. Hence, authentication fails at the T.A. The T.A recognises it as a forgery and terminates the communication. As a result, the proposed protocol protects against vehicle impersonation attacks.

b) Resistance against T.A impersonation attack: The **Å** may attempt to impersonate the T.A by intercepting the communication between the T.A and the vehicle. The **Å** tries to compute the values of {α, β, γ, H, K_s} which required them to know the values of a_n^+, b_n^+, ID_c, and x_n. This results in verification failure at the vehicle side because of incorrect values of {α, β, γ, H, K_s}. Hence, **Å** cannot impersonate as the T.A.

2) Stolen smart card attack

If **Å** manages to possess the smart card and gain access to the stored parameters i.e., a_n and b_n. **Å** tries to compute the value of tid_n which requires the knowledge of $h(ID_c \oplus r_c \parallel t_1)$, which the **Å** does not possess. Which would lead to a connection failure. Moreover, even if the **Å** intercepts a communication and gains the value of tid_n they will not be able to recover the value of ID_c due to the non-invertible property of the hash function. Hence, a stolen smart card attack fails.

3) Session key security

The vehicle verifies the value of K_s by recomputing K_s*. Recomputing K_s* requires the **Å** to know the induvial values of r*, ID_c, b_N^+, x_n, r_c which again requires knowing the values of a_n, b_n^+, ID_c, r_c, and x_n. Guessing these values incorrectly would result in connection failure. Thus, an attack on session key would fail.

4) Untraceable attack

An **Å** can intercept messages from various sessions and compare them to find similarities and patterns which would help them to compute other parameters. However, the proposed protocol makes use of random numbers r_c, r^+, temporary key k^+ and nonce $n_{T.A}$ for calculation of the session key which is different for each session. Hence, the proposed protocol provides protection against an untraceable attack.

5) Man-in-the-middle attack

In the event of an **Å** who knows or understands the parameters, which are transferred over insecure channels, then a man-in-the-middle attack can be mounted. However, regardless of the **Å** knowing the parameters passed during communication, the proposed protocol provides integrity of messages that are being sent and received between the vehicle and the T.A by using an irreversible has function, verification of messages on both ends after receiving them and it involves a time stamp check to detect any unusual delays in communication. Hence, the proposed protocol protects against man-in-the-middle attacks.

Since the proposed authentication scheme fulfils the security requirements and provides protection against various common attacks in IoV as mentioned above, it can be said that the proposed protocol can be used in IoV from a security focused perspective.

VI. Protocol Implementation

The entire authentication scheme was implemented on a single desktop running Windows 11 having Intel i7-10750H processor clocked at 2.60GHz and 16 GB memory. The code is implemented using python 3.10.0. It is a client-server program which depicts the communication between a vehicle and T.A, where the client acts as a vehicle and server acts as a T.A. The default hashing algorithm (SipHash) in python was used in the implementation. Execution time required for the authentication protocol as a client-server program in python on a single desktop was 0.062 s.

VII. Performance Analysis

The cost of computation and communication will be utilised as performance indicators. The computation cost is the amount of time required to conduct the required computations, whereas the communication cost is the number of bits/bytes exchanged across the communication channel.

1) Computation cost: The proposed protocol intends to reduce the total calculation cost associated with vehicle authentication. Elements that contribute towards the computation cost are the hash function and cryptography (encryption/decryption). As suggested by Vasudev *et al.* [12], the costs of XOR (⊕) and concatenation (||) operations are negligible; hence, they will be ignored.

"Let C_{se} denotes the cost associated with symmetric encryption, C_{sd} denotes symmetric decryption, C_m as the cost for scalar point multiplication, C_h denotes hash operation, C_{pe} denotes public key encryption, C_{pd} denotes public key decryption, and C_e is the exponential operation. Assuming the cost to be the time required to perform the computation then, the individual operations take the time, such as $C_h \approx 0.0020$ ms, $C_m \approx 0.0268$ms and $C_{se}/C_{sd} \approx 0.01000$ ms, C_{pe} takes 4.4063 ms, C_{sd} takes 7.7613 ms, and C_e takes 0.0399 ms." [12].

Since, the proposed protocol only used hash functions, the total cost is approximately $9C_h$ which is equal to 0.018ms. As a result of the decreased computing cost, the suggested protocol is appropriate for practical applications.

2) Protocol implementation: The entire authentication scheme was implemented on a single desktop running Windows 11 having Intel i7-10750H processor clocked at 2.60 GHz and 16 GB memory. The code is implemented using python 3.10.0. It is a client-server program which depicts the communication between a vehicle and T.A, where the client acts as a vehicle and server acts as a T.A. The default hashing algorithm (SipHash) in python was used in the implementation. "SipHash is a cryptographic hash function with decent performance characteristics, developed by trusted security experts" [17]. Execution time required for the authentication protocol as a client-server program in python on a single desktop was 0.062 s.

3) Communication cost: The proposed protocol uses symmetric key encryption/decryption of 1024 bits, password, timestamp, random numbers, temporary key and nonce of 64 bits. Thus, the communication cost is calculated by the values {ID_c, PW_c, x_n, tid_n, t_1, α, β, γ, H, K_s}. (Due to the lack of resources, communication cost of the proposed protocol was not calculated as it required the protocol to be implemented in a real network consisting of two devices mimicking the T.A and the vehicle).

4) *Resistance towards different attacks*

a) Impersonation attack: In this attack, the Å attempts to pass themself as one of the communication's participants.

i. Resistance against vehicle impersonation attack: The Å attempts to compute x_n and tidn by randomly selecting r_c and adding a time stamp t1. However, guessing x_n without knowing a_n will lead to incorrect values. Similarly, guessing tidn without knowing $< h(IDc \oplus r_c \| t1) >$ will again lead to incorrect values. Hence, authentication fails at the T.A. The T.A recognises it as a forgery and terminates the communication. As a result, the proposed protocol protects against vehicle impersonation attacks.

ii. Resistance against T.A impersonation attack: The Å may attempt to impersonate the T.A by intercepting the communication between the T.A and the vehicle. The Å tries to compute the values of {α, β, γ, H, Ks} which required them to know the values of a_n+, b_n+, ID_c, and x_n. This results in verification failure at the vehicle side because of incorrect values of {α, β, γ, H, Ks}. Hence, Å cannot impersonate as the T.A.

b) Stolen smart card attack: If Å manages to possess the smart card and gain access to the stored parameters, i.e., an and bn. Å tries to compute the value of tidn which requires the knowledge of $h(IDc \oplus r_c \| t1)$, which the Å does not possess. Which would lead to a connection failure. Moreover, even if the Å intercepts a communication and gains the value of tidn they will not be able to recover the value of ID_c due to the non-invertible property of the hash function. Hence, a stolen smart card attack fails.

c) Session key security: The vehicle verifies the value of Ks by recomputing Ks*. Recomputing Ks* requires the Å to know the induvial values of r*, ID_c, b_N+, x_n, r_c which again requires knowing the values of an, b_n+, ID_c, r_c, and x_n. Guessing these values incorrectly would result in connection failure. Thus, an attack on session key would fail.

d) Untraceable attack: An Å can intercept messages from various sessions and compare them to find similarities and patterns which would help them to compute other parameters. However, the proposed protocol makes use of random numbers r_c, r+, temporary key k+ and nonce nT.A for calculation of the session key which is different for each session. Hence, the proposed protocol provides protection against an untraceable attack.

e) Man-in-the-middle attack: In the event of an Å who knows or understands the parameters, which are transferred over insecure channels, then a man-in-the-middle attack can be mounted. However, regardless of the Å knowing the parameters passed during communication, the proposed protocol provides integrity of messages that are being sent and received between the vehicle and the T.A by using an irreversible has function, verification of messages on both ends after receiving them and also it involves a time stamp check to detect any unusual delays in communication. Hence, the proposed protocol protects against man-in-the-middle attacks.

Since the proposed authentication scheme fulfils the security requirements and provides protection against various common attacks in IoV as mentioned above, it can be said that the proposed protocol can be used in IoV from a security focused perspective.

VIII. Conclusion and Future Works

In this project, an authentication protocol was developed that enables lightweight mutual authentication between the vehicle and the trusted authority in an IoV environment. The lightweight property is assured as it is the most crucial condition for dynamic entities. The proposed protocol has a low calculation cost/execution time. Hash functions and XOR operations were used to optimize computation and execution time. Therefore, it can be concluded that the mutual authentication protocol developed for Wireless Body Area Network (WBAN) can be implemented in IoV environment.

The proposed protocol satisfies all the common security requirements in IoV such as confidentiality, integrity, availability, authentication, forward and backward secrecy, non-repudiation, scalability, and freshness. Hence, it can be concluded that the authentication protocol developed for Wireless Body Area Network (WBAN) fulfils the security requirements in IoV environment.

The protocol also provides security against various common attacks in IoV such as impersonation attacks, stolen smart card attacks, attacks on session key, untraceably attack and man-in-the-middle attack. This was achieved by combining XOR operations, concatenation operations and hash functions. Other measures taken to provide security are use of random numbers, nonces, time stamp verification along with recalculation and verification of information after receiving on both ends.

In this work, only the basic and most frequent attacks in IoV were considered. However, there may exist other attacks which are rarer, but more dangerous. Hence, in the future, the number of attacks can be increased, and more sophisticated attacks can be considered. Other future works may focus on the ethical, legal, professional, and social issues in IoV, such as:

Accuracy: Who is responsible if an accident occurs due to an error during exchange of information? If inaccuracy of the system causes an accident, the organisation/government controlling the IoV system should enquire the situation and make a judgement.

Privacy: How much data about ownership, current location, destination, and passengers can a vehicle share with the network is not standardized. Attending to privacy issues is crucial for the system to work because if a user does not agree with sharing their information with the network, they would not be able to be a part of the system.

Property: Who controls the data transmitted across the network? Is it possible to analyse and sell this data? The controllers of the system must be trustworthy and made public to gain trust of the users. If the users cannot trust the controller of the system, they would choose not to register.

Accessibility: What details and to whom may be revealed in the event of an injury, and under what circumstances? In case of emergency, it is very crucial to inform the right people based on the type of accident. Therefore, attending to this issue is the most important.

Conflict of Interest

The authors declare no conflict of interest

Author Contributions

This work is an accumulated efforts for an ongoing research study of the authors both the main and the co-authors. It is a supervisor/ student research study and the contribution for all authors. Myasar Tabany wrote the paper and enhanced the quality of the results while Mohiuddin Syed collected the results and proposed with Myasar Tabany the methodology and the plan for the whole research work. The implementation part was mainly done by Mohiuddin Syed. The practical implementation has been revised by Myasar Tabany. Both authors had approved the final version.

References

[1] T. T. Dandala, V. Krishnamurthy, and R. Alwan, "Internet of Vehicles (IoV) for traffic management," in *Proc. 2017 International Conference on Computer, Communication and Signal Processing (ICCCSP)*, 2017.

[2] J. Contreras-Castillo, S. Zeadally, and J. A. Guerrero-Ibanez, "Internet of vehicles: Architecture, protocols, and security," *IEEE Internet Things J.*, vol. 5, 2018.

[3] T. Zhang, *Securing Connected Vehicles: Challenges and Opportunities*, 2015.

[4] Q. Wu, W. Xiao, X. Hu, P. Zhu, and X. Chen, "A data privacy and authentication scheme based on internet of vehicles," in *Proc. 2021 7th IEEE Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS)*, 2021.

[5] N. Lu, N. Cheng, N. Zhang, X. Shen, and J. W. Mark, "Connected vehicles: Solutions and challenges," *IEEE Internet Things J.*, vol. 1, 2014.

[6] C.-C. Wu, W.-B. Lee, and W.-J. Tsaur, "A secure authentication scheme with anonymity for wireless communications," *IEEE Commun. Lett.*, 2008.

[7] H. Mun, K. Han, Y. S. Lee, C. Y. Yeun, and H. H. Choi, "Enhanced secure anonymous authentication scheme for roaming service in global mobility networks," *Mathematical and Computer Modelling*, vol. 55, 2012.

[8] D. Zhao, H. Peng, L. Li, and Y. Yang, "A secure and effective anonymous authentication scheme for roaming service in global mobility networks," *Wireless Personal Communications*, vol. 78, no. 1, pp. 247–269. 2014.

[9] C. Shen and H. Mu, "A roaming authentication protocol based on elliptic curve cryptography in IoV," in *Proc. 2017 3rd IEEE International Conference on Computer and Communications (ICCC)*, 2017.

[10] C. Chen, B. Xiang, Y. Liu, and K. Wang, "A secure authentication protocol for internet of vehicles," *IEEE Access*, vol. 7, 2019.

[11] B. Ying and A. Nayak, "Anonymous and lightweight authentication for secure vehicular networks," *IEEE Trans. Veh. Technol.*, vol. 66, 2017.

[12] H. Vasudev, V. Deshpande, D. Das, and S. K. Das, "A lightweight mutual authentication protocol for v2v communication in internet of vehicles," *IEEE Transactions on Vehicular Technology*, vol. 69, 2020.

[13] X. Wu, J. Xu, W. Huang, and W. Jian, "A new mutual authentication and key agreement protocol in wireless body area network," in *Proc. 2020 IEEE International Conference on Smart Cloud (SmartCloud)*, 2020.

[14] P. Bagga, A. K. Das, M. Wazid, J. J. P. C. Rodrigues, and Y. Park, "Authentication protocols in internet of vehicles: Taxonomy, analysis, and challenges," *IEEE Access*, vol. 8, 2020.

[15] M. A. Talib, S. Abbas, Q. Nasir, and M. F. Mowakeh, "Systematic literature review on internet-of-vehicles communication security," *International Journal of Distributed Sensor Networks*, 2018.

[16] Y. Sun, L. Wu, S. Wu, S. Li, T. Zhang, L. Zhang, J. Xu, and Y. Xiong, "Security and privacy in the internet of vehicles," in *Proc. 2015 International Conference on Identification, Information, and Knowledge in the Internet of Things (IIKI)*, 2015.

[17] J. Semmlow, "Linear systems analysis in the time domain: Convolution and simulation," in *Signals and Systems for Bioengineers*, 2nd ed. Academic Press, Boston, 2012, ch. 7.