

## Retraction

# Retracted: A Mathematical Queuing Model Analysis Using Secure Data Authentication Framework for Modern Healthcare Applications

### Journal of Sensors

Received 23 January 2024; Accepted 23 January 2024; Published 24 January 2024

Copyright © 2024 Journal of Sensors. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

- (1) Discrepancies in scope
- (2) Discrepancies in the description of the research reported
- (3) Discrepancies between the availability of data and the research described
- (4) Inappropriate citations
- (5) Incoherent, meaningless and/or irrelevant content included in the article
- (6) Manipulated or compromised peer review

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.



The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

### References

- [1] A. S. A. Raj, R. Venkatesan, S. Malathi et al., "A Mathematical Queuing Model Analysis Using Secure Data Authentication Framework for Modern Healthcare Applications," *Journal of Sensors*, vol. 2022, Article ID 8397635, 15 pages, 2022.

## Research Article

# A Mathematical Queuing Model Analysis Using Secure Data Authentication Framework for Modern Healthcare Applications

A. Samson Arun Raj,<sup>1</sup> R. Venkatesan,<sup>1</sup> S. Malathi,<sup>2</sup> V. D. Ambeth Kumar ,<sup>3</sup> E. Thenmozhi,<sup>4</sup> Anbarasu Dhandapani ,<sup>5</sup> M. Ashok Kumar,<sup>6</sup> and B. Chitra<sup>3</sup>

<sup>1</sup>Computer Science and Engineering, Karunya University, Coimbatore 641114, India

<sup>2</sup>Artificial Intelligence and Data Science, Panimalar Engineering College, Anna University, Chennai 600123, India

<sup>3</sup>Computer Science & Engineering, Panimalar Engineering College, Anna University, Chennai 600123, India

<sup>4</sup>Department of Information Technology, Panimalar Institute of Technology, Anna University, Chennai 600123, India

<sup>5</sup>Department of Electrical and Computer Engineering, Institute of Technology, Jigjiga University, 1020 Somali, Ethiopia

<sup>6</sup>Faculty of Computer Science and Software Engineering, Skyline University Nigeria (SUN), Kano, Nigeria

Correspondence should be addressed to Anbarasu Dhandapani; [anbarasudhandapani@jju.edu.et](mailto:anbarasudhandapani@jju.edu.et)

Received 28 July 2022; Accepted 24 August 2022; Published 16 September 2022

Academic Editor: Sweta Bhattacharya

Copyright © 2022 A. Samson Arun Raj et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Healthcare application is one of the most promising developments to provide on-time demand services to the end users, vehicles, and other Road Side Units (RSUs) in the urban environment. In recent years, several application interfaces have been developed to connect, communicate, and share the required services from one source to another. However, the urban environment holds a complex entity of both homogenous and heterogeneous devices to which the communication/sensing range between the devices leads to connectivity breakage, lack of needed service in time, and other environmental constraints. Also, security plays a vital role in allowing everyone in the urban area to access/request services according to their needs. Again, this leads to a massive breakthrough in providing reliable service to authentic users or a catastrophic failure of service denial involving unauthorized user access. This paper proposes a novel topological architecture, Secure Authentication Relay-based Urban Network (S-ARUN), designed for healthcare and other smart city applications for registered transportation stakeholders. The registered stakeholders hold a built-in data security framework with three subsystems connected to the S-ARUN topology: (1) authentication subsystem: the stakeholder must identify themselves to the source responder as part of the authentication subsystem before transmitting the actual data service request; (2) connectivity subsystem: to periodically check the connection state of stakeholders as they travel along with the road pattern; and (3) service subsystem: each source responder will keep a separate queue for collecting data service requests, processing them quickly, and sending the results to the appropriate stakeholder. The Kerberos authentication method is used in working with S-ARUN's model to connect the stakeholders securely and legitimately. The performance of the proposed S-ARUN is assessed, and the performance metric toward key generation and other data security-related metrics is tested with existing schemes.

## 1. Introduction

In networking, "data" refers to a collection of multimedia data streams. Data can be text, image, audio, video, or other document-type material ready for transmission with the appropriate stakeholders in the field. However, data transmission from one source to another is not easy but plays a vital role in various design applications [1]. The possible number of data

can be tapped, altered, or worse, rerouted by the third-party member. Researchers have introduced several algorithms and mathematical formulation ways of securing the wired and wireless communication channel from which the third party cannot alter the data shared among its stakeholders.

Recently, smart city application under various operational purposes has gotten the attention of constructing an effective topology by introducing a hybrid infrastructure in

the transportation environment. As a result, the stakeholders can easily interact with the nearest substation of RSUs anywhere and anytime. Jeong et al. [2] have addressed the standardization initiatives for smart transportation systems, protocols, applications, and security which have been thoroughly examined by researchers. However, this hybrid infrastructure faces certain topological flaws of its own such as lack of communication, mobility speed, network coverage, limited resources, data contention, and data congestion.

Since the transportation environment mode of communication and equipment changes, the stakeholder's evolution changes. However, the infrastructure from which the data is relayed is still conventional. The working mechanism of the existing transportation environment is like a flooding mechanism. If one RSU receives the service request to access the data, the source data of that particular is broadcasted to all its neighboring RSUs and finally reaches the appropriate stakeholder. Thus, it creates a huge security risk of revealing the service access throughout neighboring RSUs that find themselves unrelated to the store and unnecessary acceptance of information to relay the communication. The third party finds these weak RSUs node gains access and listens to all the surpassed information.

Moreover, most RSUs have limited and few operational resources to classify and process the needed information to be delivered in time. Hence, these RSUs undergo certain eco-friendly and communication difficulties as the on-road vehicles move quickly along the road. Furthermore, the potential increase/decrease in on-road vehicles entering and exiting the transportation environment makes maintaining the network topology and data flow critical. As a result, there are several technical challenges with RSUs providing dependable data service to on-road vehicles in the transportation environment. Surely, we can consider the end-user terminal for requesting the needed service. Since the topological design deals with vehicles and aerial nodes, the end user can also be considered a ground node depending on the configuration devices used in the application scenario.

*1.1. Usage of UAVs.* As intelligent transportation systems become more sophisticated with digital streams, each transport mode needs to cooperate under various application platforms to form a global network of hybrid-vehicular systems. Flying Ad-Hoc Networks (FANETs) have recently focused on civilian and military-based systems (<https://blog.rgbsi.com/what-is-v2i-technology>) [3]. FANET is a subclass of Vehicular Ad-Hoc Networks (VANETs) that use flying anchor nodes or small-scale Unmanned Aerial Vehicles (UAVs), as an intermediary agent in harsh locations where establishing infrastructure is nearly impossible. However, there are certain difficulties that the VANET system faces daily. For example, the transportation environment conditions and node behavior between ground vehicles and aerial vehicles change dynamically, leading to the isolation of stakeholders in the transportation environment. Therefore, an extensible wireless communication gateway must integrate existing technologies and make modern transportation systems more sustainable, ecofriendly, and safe for on-road vehicles to obtain the sought service promptly [1].

On the other hand, the height of RRSU nodes plays a vital role in providing network connectivity to vehicular nodes, which is one of the issues encountered in the contemporary application environment. Surely, deploying aerial nodes is quite challenging in the urban environment as the altitude against skyscrapers should be maintained with constant observation. Several mobility models with artificial intelligence are under development to address this issue. Few automobile nodes, for example, have poor network connectivity throughout their journey as they follow road patterns. Because the distance from the RRSU network in the transportation environment exceeds 300 meters, it is not considered to offer or receive the requested data service. Furthermore, the present ITS service system's incoming arrival rate indicates that the requested service lacks data priority due to significant data conflict from several vehicular nodes, resulting in a buffer overflow and packet loss.

*1.2. Data Authentication in VANETs.* In a vehicle ad hoc network, authentication is crucial. A VANET's basic structure comprises three primary elements: the Trusted Authority (TA), roadside units, and automobiles. The VANET's real-time, dynamic communication properties allow for efficient and continuous information sharing and attractive application services, which could significantly improve the driving experience of drivers. The TA is in charge of registering all RSUs and cars and assigning secret keys. To validate the participating automobiles, TA uses a twofold authentication process. Meanwhile, RSU serves as a communication hub. There are four rounds to the authentication process.

The connection between multiple vehicles is at the heart of VANETs, and the security of such communication is ensured via message authentication. Several approaches have been developed to improve message authentication efficiency. However, both techniques have the drawback of redundant authentication. The same message is authenticated several times, and they fail to identify erroneous messages in a batch of messages. Because VANETs are vulnerable to malicious assaults, the security of vehicular ad hoc networks has gotten much attention in wireless mobile networking. Several safe authentication systems based on asymmetric cryptography have been proposed to counter such attacks.

On the other hand, these techniques are not ideal for extremely dynamic environments such as VANETs since they cannot handle the authentication operation efficiently. As a result, an efficient authentication system for VANETs is still required. Furthermore, message authentication, a common mechanism for verifying information reliability, such as data integrity and authenticity, has a problem in VANETs.

When a vehicle receives many messages, typical exhaustive (or per message) authentication might cause unacceptably high processing overhead on the car, causing unacceptable delays in time-critical applications like accident warnings. For vehicular ad hoc networks, the trade-off between reliance on the tamper-proof device (TPD) and storage space in authentication schemes has recently become a hot topic [4]. Because the intelligent transportation systems of smart city technologies, vehicular ad hoc networks, and Internet of Vehicle (IoV) technologies are drawing special interest from industry communities [5], VANET's vehicle-to-vehicle (V2V) connectivity can help traffic

management and road safety. However, because V2V communication cannot handle many cars simultaneously, it must be split and communicated by region. As a result, essential agreements are created for V2V communication between the same or different regions, considering the locale. Furthermore, standard public key infrastructure and Kerberos systems incur computational costs to be used in a real setting.

Existing vehicular ad hoc network (VANET) authentication systems are not scalable to high-density and safety-critical VANETs. In their design, these methods overlook critical and unique VANET properties such as frequent path disconnections due to high mobility, bandwidth-limited channels, ultra-low latency applications, high channel-error rate, and much more. Furthermore, due to the usage of an open wireless communication medium where messages are transferred in plain text, which allows attackers to intercept, manipulate, replay, and delete them, VANET's security and privacy are of the utmost importance [6]. As a result, there is a good chance that the security of a VANET-based smart transportation system may be jeopardized.

*1.3. Objectives of the Research Work.* The primary objectives of the proposed topological design are listed as follows:

- (i) To introduce a secure authentication mechanism to all the registered stakeholders connected to the SARUN topology in the transportation environment
- (ii) To perform the data packet request by analyzing its parameters based upon the data security framework introduced in every RSU node
- (iii) The proposed work is compared with the existing schemes to verify the performance metric, and merits and demerits are notified in detail

## 2. Related Works

The deployment of vehicle networks in practice is still a work in progress. This study [7] presents a new self-organized authentication approach for VANETs that enables ubiquitous, quick, and safe deployment. Because the nodes themselves certify the authenticity of the public keys of the other nodes, there is no need for a central certification authority. On the one hand, researchers have devised a mechanism that each node must employ when selecting public key certificates for its local storage.

Because of the variety and severity of prospective assaults, communication security in VANETs is one of the essential concerns to enable their effective deployment. On the one hand, erroneous traffic warning messages can influence drivers' judgments, waste time and fuel, and even result in traffic accidents. As a result, VANETs must guard against attackers sending false information about road conditions, such as traffic jams, to deceive other vehicles. On the other hand, as a result, VANETs should not provide complete vehicle anonymity since the risk of sending misleading signals would jeopardize their practical implementation.

With promising technologies that provide rich multimedia data streams of information to all searching vehicular

nodes in the transportation environment, the need for intelligent transportation system services has grown dramatically worldwide [8, 9]. The existing intelligent transportation system has two application scenarios: pole infrastructure-based [8] and aerial mobility-based [7]. The data packets that convey the message flow from the source, i.e., the base control station (BCS), are sent through a sequence of communication RSU agents to reach and communicate with relevant vehicular traffic nodes in both application scenarios. In addition, the RSU agents have the authority to process data packets and alert the nearest subunits to monitor, track, and direct the vehicular nodes in the event of hazards, warnings, or event notifications.

In various intelligent transportation system applications, the roadside units are stationary constructed at the intersection points along with the road pattern. Over time, these stationary RSU agents lack the priority in establishing the desirable network connectivity and cannot provide the necessary reliable data service among the vehicular nodes. The RSU is a stationary unit normally permanently installed along the side of the road. Ad hoc domain is used for single/multihop communication between automobiles. A Dedicated Short-Range Communication (DSRC) technology is used to communicate between V2V and V2I. The DSRC is a short- to medium-range wireless communication system utilized in the VANET for data transfer. The DSRC system uses a spectrum of 75 MHz with a communication range of DSRC that is 100 to 1000 meters, and the data rate is 6 to 27 megabits per second [10]. Since the technological equipment and mode of communication changes, the existing RSU agents are packed with numerous amounts of information leading to a processing overload of limited resources and incapable of tracking high-speed vehicular nodes pursuing the transportation environment. Thus, replacing or reconstructing the entire ITS service system operating in the transportation environment over the years is impractical.

Fotohi et al. [11] talked about an agent-based self-protective technique for UAVNs called ASP-UAVN, based on the Human Immune System (HIS). In ASP-UAS, a self-protective system chooses the safest route from the source UAV to the destination UAV. Using an Artificial Immune System (AIS), a multiagent system identifies the attacking UAV and picks the safest approach. Furthermore, [3] covered the various sorts of attackers and security assaults in the VANET. The attackers are categorized based on their network activities. A node is considered adversarial if it injects or modifies any messages, causing the entire network to be disrupted. The attackers' primary goal is to cause network disruptions for personal gain. According to their actions and scope, the three types of attackers are insiders vs. outsiders, aggressive vs. passive, and malicious vs. reasonable attackers.

Authentication is a critical security issue for VANETs [12]. Over the last few years, many authentication systems based on public key infrastructure (PKI) or identification (ID) have been presented. The digital signature provides message authentication, integrity, and nonrepudiation. Knowing the signer's public key allows anyone to verify the signature's legitimacy. This property makes it possible to use the digital signature in one-to-one (unicast) and one-to-many (multicast) applications. In some multicast applications, the root node

may be required to gather messages from leaf nodes, resulting in many-to-one communication.

Lall et al. [8] concentrated on the many authentication techniques used in VANET because they are critical for safe communication. The three main authentication schemes are cryptography techniques, digital signatures, and message verification techniques. A taxonomy of authentication systems is also thoroughly examined. Also, authentication is necessary for accepting safety messages from legitimate VANET users. Authentication is divided into two parts: part 1 is the sender vehicle's signature, and part 2 is the receiver vehicle's signature verification of the message received. Authentication can be done at two levels in a VANET communication system: first at the node level, referred to as node authentication, and second at the message level, message authentication. Authentication of nodes and messages ensures a node's legitimacy and a message's integrity, respectively. Verifying the message's integrity and the node legitimacy check is critical to increasing VANET security. As a result, the most critical security aspect in VANET is message authentication.

Azees [13] and Tan et al. [14] have introduced a two-factor authentication and key management strategy for safe data transfer in vehicular ad hoc networks. According to the authors, the proposed approach is immune to replay and masquerade attacks. Chuang and Lee [15] have introduced a decentralized lightweight authentication technique for vehicle-to-vehicle communication networks dubbed trust-extended authentication mechanism (TEAM). To increase the efficiency of the authentication operation, TEAM uses the concept of transitive trust connections and only requires a few storage spaces. TEAM also meets the following security requirements: anonymity, location privacy, mutual authentication, forgery, modification, and replay attack resistance, no clock synchronization problem, no verification table, fast error detection, perfect forward secrecy, man-in-the-middle attack resistance, and session key agreement.

Lin and Li [16] have proposed an effective cooperative authentication strategy for VANETs that minimizes redundant authentication efforts on the same message by various vehicles while reducing the authentication overhead on individual cars and shortening the authentication delay. Because it simultaneously provides mutual authentication and privacy protection, the conditional privacy-preserving authentication (CPPA) technique [17] is appropriate for handling security and privacy-preserving challenges in VANETs. On the other hand, the bilinear pairing process is renowned as one of the most difficult operations in modern cryptography. Therefore, constructing a CPPA scheme for the VANET environment that does not require bilinear pairing becomes a challenge to improve performance and reduce the computational complexity of information processing in VANET.

Zhu et al. [18] discussed an efficient privacy-preserving authentication technique for automotive ad hoc networks based on group signature (VANETs). Although group signatures are commonly used in VANETs to achieve anonymous authentication, existing systems based on group signatures suffer from substantial calculation delays in the CRL checking and signature verification processes, resulting in high message loss. Liu et al. [4] talked about using identity-based encryption

and a short-lifetime region-based certificate to create a realistic distributed conditional privacy-preserving authentication mechanism for VANETs.

Lee et al. [5] presented a lightweight technique for managing regional segmentation and overhead resolution using dynamic features of vehicles. Furthermore, because vehicle data is sent through public networks, our protocol employs mutual authentication and honey list technology to protect against various threats. The concept of edge computing has been discussed in the message-authentication process of VANETs [19]. Even if the VANET is attacked, the suggested system can not only perform well in an ideal scenario where the attacker is not present but it can also swiftly distinguish valid and invalid messages.

Shao et al. [20] developed a new authentication protocol for VANETs in a decentralized group architecture that employs a novel group signature mechanism to address these difficult issues. VANET must have an authentication mechanism to protect against attacks and maintain privacy to enable safe communication. Azam et al. [21] examined security, privacy, and scalability requirements with a complete taxonomy for authentication systems in VANET. Shen et al. [22] has addressed the issues of high computing overhead caused by safety message authentication in the cooperative message authentication protocol (CMAP), which was developed to reduce the computational burden on automobiles.

Ying and Nayak [23] have developed a smart card (ASC) protocol-based anonymous and lightweight authentication system. ASC uses low-cost cryptographic operations to authenticate the legitimacy of users (vehicles) and validate data communications. ASC also has a way of changing passwords that do not rely on a trusted authority. As a result, it can withstand an offline password guessing attack. Finally, a formal security model is developed to demonstrate that our protocol is secure when the computational Diffie-Hellman problem is assumed. Asaar et al. [24] have proposed a new identity-based message authentication system based on proxy vehicles (ID-MAP) that satisfies the message authentication condition against adaptively chosen messages.

Al-Shareeda et al. [6] thoroughly examined the many authentications and privacy systems implemented over time. Vijayakumar et al. [25] have created a trusted authority to supply clients with various online premium services via VANETs. The security and authentication of messages exchanged between the TA and the VANET nodes are critical. As a result, we focus on the situation in which the TA divides users into primary, secondary, and unauthorized users to address the security issue. Lee et al. [5] stated that two public-key cryptosystems have developed a privacy-preserving localized hybrid authentication (PLHAS) mechanism for PKI and CL-PKC. Li et al. [26] have proposed a composite fault diagnosis methodology based on detecting and identifying the fault of the vehicle ad hoc network's onboard unit.

Certificateless public-key cryptography is used to tackle the complex certificate management problem in classical public-key cryptography and the key escrow problem in identity-based encryption [27]. The aggregate signature notion comes in handy when the signatures on various messages generated by various users must be compressed. Because it allows for

considerable bandwidth and calculation time reductions, this feature is highly appealing for authentication in a resource-constrained setting. A novel certificateless signature system is proposed in this paper. The new certificateless signature technique gives a novel certificate less aggregate signature scheme for vehicle-to-infrastructure communication in vehicular ad hoc networks.

Due to the high dynamics in topology, mobility, and link connectivity, data dissemination in VANET is a difficult issue. Due to the host/address-centric, connection-oriented communication mechanism primarily built for reliable wired networks, the Internet paradigm (i.e., TCP/IP) is inefficient for VANET data dissemination [28]. Arshad et al. [29] has developed a full block chain-based 5G vehicular network architecture that is cost-effective, scalable, and secure and addresses various vehicular network concerns in smart cities. All necessary components, such as a reputation system, an incentive mechanism, and priority-based strategies, are included in the proposed design. Soleymani et al. [30], as well as a trust model, have addressed a privacy-preserving node and message authentication approach. In addition, fog nodes were placed along the highway by the fog computing concept to reduce latency and enhance throughput.

The Password-Authenticated Key Exchange (PAKE) protocol is widely used to offer secrecy, data integrity, and authentication services in various settings. On the other hand, preshared passwords are insecure in a practical self-organized network because mass-produced devices frequently have similar default passwords, such as 0000 or 1234, which are seldom changed [31].

Eftekhari et al. [32], Ogundoyin and kamil [33], and Peixoto et al. [34] have developed a fog computing-based data clustering framework for traffic information reduction at the edge of vehicular networks. Rao and Ram [35] have improved the time synchronization and freshness plan for Kerberos 5 authentication using symmetric encryption keys in a client-server scenario. Also, [36] have proposed a secure protocol based on tickets for rigorous mutual authentication and session key establishment tokens that incorporate Kerberos' strong qualities. Based on their architecture and implementation specifics, [37] has comprehensively evaluated VANET, SDN, and SDN-based VANETs.

Section 3 describes the internal design and operation of the RSU agent's data security framework.

### 3. Data Security Framework and Their Working Process

The model for the data security framework we will use in our research effort is represented in Figure 1 in the application scenario [1]. Base control station, satellite relay station, aerial networks, and vehicular nodes (i.e., on-road vehicles) are the four primary components of the application scenario. However, these components are interrelated, each having a specific role in preserving data security and obtaining requested data packets in diverse mobility patterns.

- (i) Base control station: the transportation field station, also known as the base control station, organizes

and retains information concerning aerial nodes, vehicular nodes, situation awareness, and other relay subunits. In addition, the base control station monitors and guides the aerial network in a dedicated way-point lane in the transportation environment

- (ii) Satellite relay station: satellites provide a backbone relay communication across civilian platforms across the transportation environment in modern transportation applications. Depending on the necessity, the satellite can be utilized as a backbone transceiver, processing all microwave data into the proper data format between the source and destination platform communicators
- (iii) Aerial nodes: the aerial nodes, also referred to as Relay-Road Side Unit (RRSU) network, act as a buffer between the vehicle nodes. It improves network connectivity to all vehicular nodes and takes the initiative to process data packet requests and deliver road-assisted service messages on time. A single RSU network comprises many RSU nodes separated by a defined distance and travels at an ideal pace to avoid colliding with the RSU substation and each other
- (iv) Vehicular nodes: a vehicular node can be a commercial, semiautonomous, or fleet management vehicle that leads a group of subunits in the transportation environment. Autonomous vehicles have been created for various ITS service applications, including field support, exploration, search, and rescue

In this paper, we will be considering this application scenario for healthcare usage in which these aerial nodes have the following advantages as follows,

- (i) Aerial access points: unlike traditional networks, these aerial nodes are equipped with all communication functionalities to communicate to the nearest hospital if a vehicle or user requires an emergency service to the nearest hospital or doctors. Thus, it provides seamless and anytime connectivity who seek service
- (ii) Built-in data storage: since the urban environment is pouring with vehicles requesting service access, the aerial nodes are embedded with predefined information on how, when, where, and whom to process the request in time. Table 1 illustrates some of the information predefined in every aerial node to process
- (iii) Computation: once the connection establishment of the stakeholder is authentic, the request for the service is granted with priority. If the service is requested from an unauthorized user, the aerial nodes seek out other nodes for supporting service

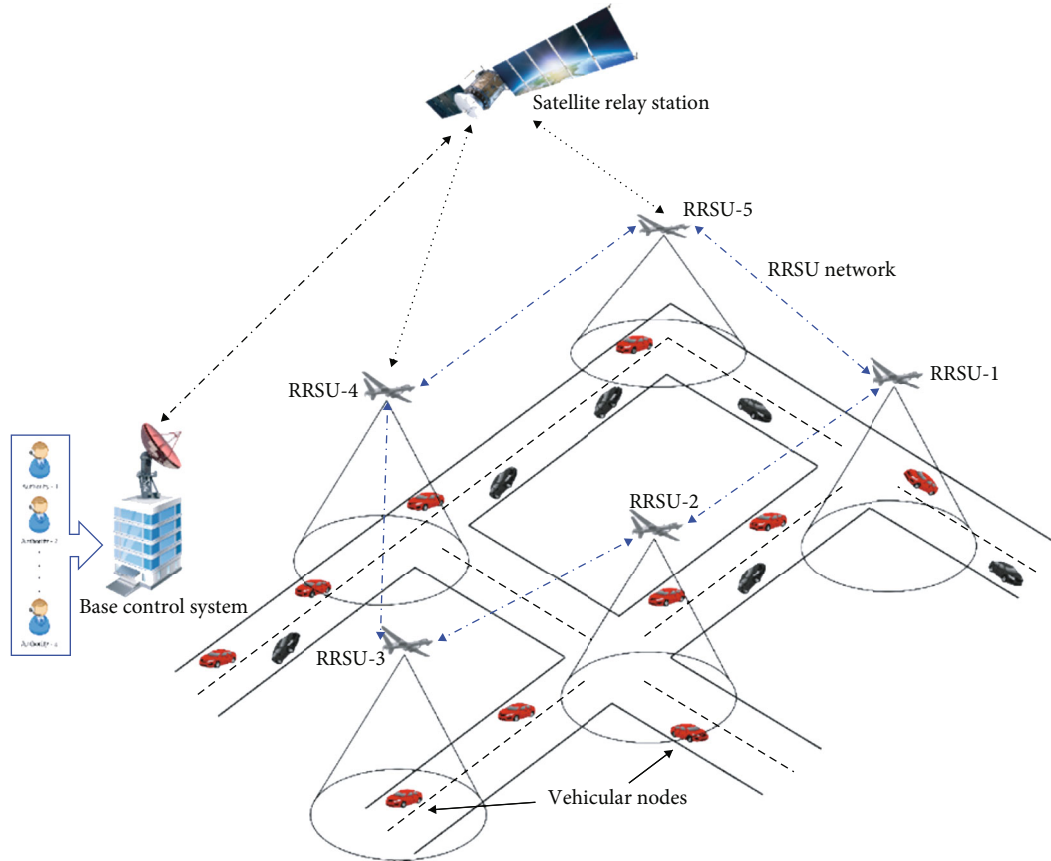


FIGURE 1: Application scenario [1].

- (iv) Service transmission: since the urban environment deals with moving vehicles, the requested service must be delivered in time. If the aerial node cannot transmit the service in time, the neighboring nodes will notify, providing service reliably

The working process of the data security framework in S-ARUN topology is of a three-stage level of subsystem process. At first, all the stakeholders must be connected to the nearest RSU agents for registration confirmation. The RSU agents first broadcast a series of control beacon messages (CBM) to all stakeholders by establishing unified network communication. The registered transportation stakeholders will quickly establish the connection apart from the non-registered stakeholders who seek data service must go through a secure authentication verification before offering the actual network connection, which will be explained in detail.

After connecting to their nearest RSU agent, vehicular nodes can request data service application information/messages, such as infotainment, location guidance, and safety awareness. The RSU agents process the data packet request according to their priority index of vehicle type and then respond to message/service to the appropriate vehicular node within the specified time frame. Figures 2 and 3 depict the information flow of data service packets and the internal subsystems of a data security framework inside a single RSU agent.

**3.1. Authentication Subsystem.** The authentication service provided in this subsystem follows the working principle concept of Kerberos. The Kerberos authentication scheme authenticates all the stakeholders who present an open distributed environment. In the case of nonregistered stakeholders seeking service, it is mandatory to prove that it has been identified for each service request to acquire the data service, or else their access request will be denied. Any stakeholder can request any RSU agent for data service if the topology is unprotected. Thus, the RSU agent cannot easily deny the data service requests without proper constraints. Every RSU agent is provided with an inbuilt Stakeholders Service Authentication (SSA) to ensure safety measures. This authentication server knows the true identity of the stakeholder and logs all the possible information maintained in a centralized database. In addition, every RSU agent provides a unique key in a ticket for granting access to the requested data service.

The following steps describe how the stakeholder's service authentication ticket is generated for stakeholders who seek service. This mechanism can be applied to registered and nonregistered stakeholders in the transportation environment. Table 2 illustrates the notations used for service access ticket generation under the authentication scheme, and Pseudocode 1 outlines the functional approach of the data security framework in a single RSU agent.

TABLE 1: Types of MPLS labels used in data security framework.

MPLS header label bits						
Emergency	Cater	Government	Private	Specific	Clinic	Shelter
	Bits	00001	00010	00011	00100	00101
Early warning	Cater	Accident zone	Intersections/roundabouts	Road bumps	Speed alerts	Collision alerts
	Bits	00110	00111	01000	01001	01010
Service application	Cater	Location of substations	Alternative routes	Navigation	Pedestrian crossing	Lane restrictions
	Bits	01011	01100	01101	01110	01111
On-the-Move (OTM)	Cater	Infotainment	Service access	Traffic status	Cruise control	Smart sensors
	Bits	10000	10001	10010	10011	10100

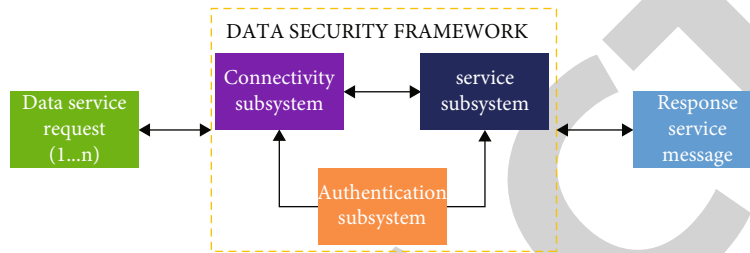


FIGURE 2: Overview of data security framework.

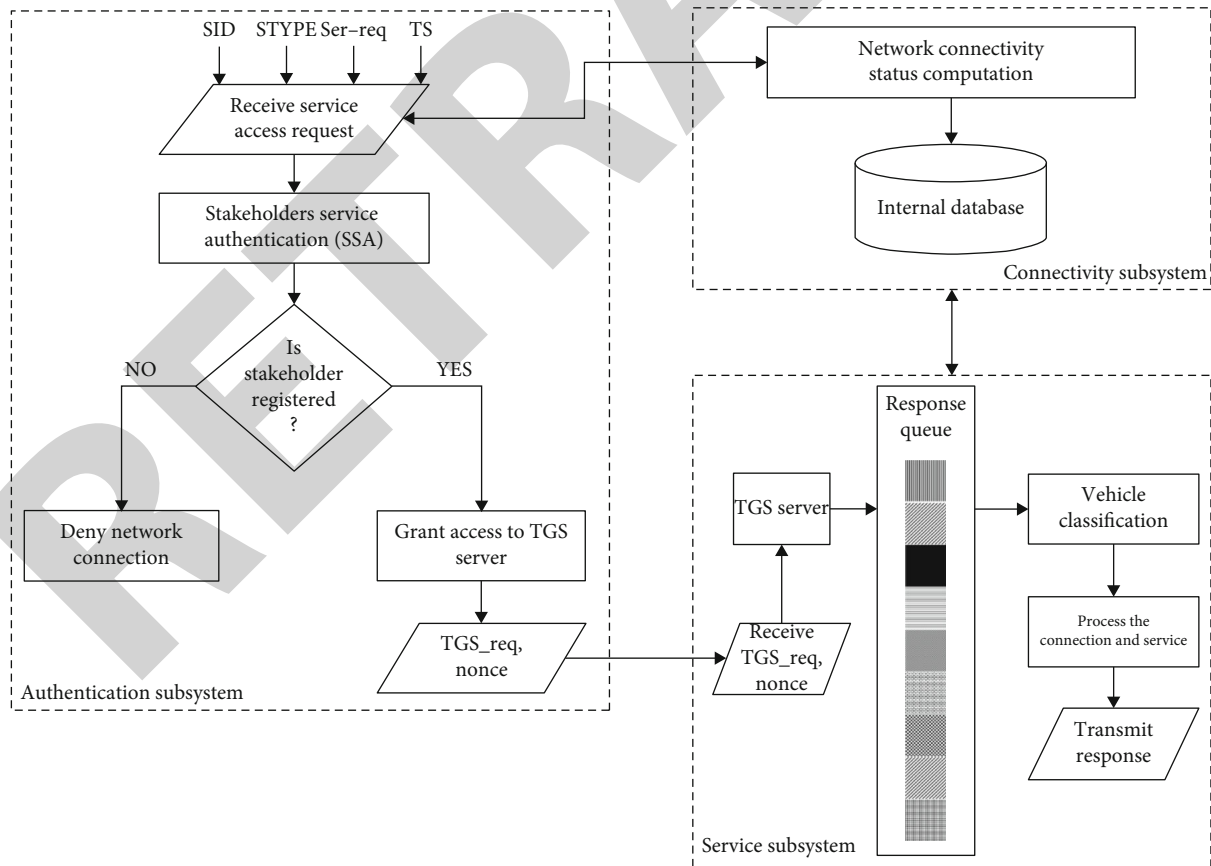


FIGURE 3: Internal architecture of the data security framework.



TABLE 2: List of notations used in authentication server.

S	Stakeholder
Kv	Secret encryption key shared by SSA
NDS	Network address of the stakeholder
Nonce	The lifetime of the TGS_Req
REG_DB	RSU registered database
REQ_Conn	Request connection
Req_Type	Service request type
RRSU <sub>i</sub>	RSU agents
SA_Req <sub>L</sub>	Service access request, $L = 1, 2, \dots$
SER	Service message
Ser_Auth	Service authentication
SID	Identifier of stakeholder
SSA	Stakeholder service authentication
TGS	Ticket granting server
TGS_Req	Ticket granting server request
TGSID	ID of ticket granting server
TS	Time stamp
V	Server
VID	Identifier of server
VTYPE	Type of stakeholder/vehicular node

Step 1.  $S = > SSA:SID||STYPE||VID$ .

Step 2.  $SAA = > S:Ticket$ .

Step 3.  $S = > V :SID||Ticket$ .

$$Ticket = E (K_v, [SID||NDS||VID]) \quad (1)$$

The above steps provide data service access to registered and nonregistered stakeholders in the transportation environment—the data security framework provides this simple authentication scheme. However, the problem encountered in this simple scheme is that the stakeholder would need a new ticket for every different data service. Therefore, the RSU agents hold a Ticket Granting Server (TGS) in the service subsystem to extend its authentication service needs to access different data services. However, its process of granting is quite similar to the previous simple authentication scheme.

Once per requesting data service access is as follows:

Step 1.  $S = > SSA:SID||TGSID$ .

Step 2.  $SSA = > S:E (K_s, Ticket_{tgs})$ .

Once per requesting the type of data service is as follows:

Step 3.  $S = > TGS:SID||VID||Ticket_{tgs}$ .

Step 4.  $TGS = > S:Ticket_v//Ticket$  to access any RSU agent for service.

Once per requesting the type of data service is as follows:

Step 5.  $S = > V:SID||Ticket_v$ .

$$\begin{aligned} Ticket_{tgs} &= E (K_{tgs}, [SID||NDS||TGSID||Nonce]) \\ Ticket_v &= E (K_{tgs}, [SID||NDS||VID||Nonce]). \end{aligned} \quad (2)$$

The stakeholders can access the data service through a secure authentication scheme upon the application design and usage. The stakeholders can either go for one-time access to the server or access multiple servers for different types of data services by authenticating themselves and acquiring the  $Ticket_{tgs}$ .

At first, the authentication subsystem of every RSU agent obtains the service access request as a collective input from the stakeholders. On obtaining the service access request, the RSU agent crossverifies with the connectivity subsystem and notifies its connection status by updating its internal connectivity database. The service access requests are passed through the SSA for authentication verification. For example, suppose the requesting stakeholder is a registered member of the transportation environment or a regular authenticated user. In that case, the TGS\_Req for the TGS server of every RSU agent is automatically granted full access. On the other hand, if the requesting stakeholder is not a member or unregistered, its network connectivity towards the RSU agents gets disconnected without any sign.

3.2. *Connectivity Subsystem.* In the application scenario, there are cases where vehicular nodes will be connected to their nearest RSU agents without requesting service. Thus, the network connectivity to such vehicular nodes leads to resource depletion. The proposed data security framework categorizes the incoming control beacon messages based on the vehicular node type and its service allocated upon the priority level to avoid such resource consumption. In this research work, we have not considered the authentication time limit for each packet to be served for accessing the data service. However, we have computed the connectivity time limit for each vehicular node connected with the aerial access points. Upon the connectivity time limit, the aerial nodes know where to process the request packet or not. The network connectivity status and vehicle types will prioritize data service for the vehicular nodes as they move along the road pattern. Table 3 illustrates various vehicular nodes that enter/exit the transportation environment.

3.3. *Service Subsystem.* The service subsystem is a functional module for processing and granting the service request to the TGS server. Every RSU agent holds a set of multimedia instructions and a limited number of services to be communicated with the appropriate stakeholders in the transportation environment. Once the authentication subsystem grants the TGS request for access, the TGS server classifies the service request based on their MPLS header labels, as shown in Table 1. The incoming service requests are discriminated with a 5-bit MPLS header label holding 20 possible data service messages that the stakeholders would need to access in time. For real-world applications, the MPLS header labels are defined as 6-bits, and some labels are reserved for research

**Input:** Transmission of Service Access Request  
**Output:** Transmission of Service Grant TGS\_Req or Connection Termination

1. **BEGIN**
2. Initialize SID, VTYPE, TS, Req\_Type, SA\_Req, SER, TGS\_Req, Nonce, RRSUi
3. **Loop**
4. RRSUi  $\leftarrow$  **Process:** SA\_Req<sub>i</sub> (SER<sub>1</sub>, SER<sub>2</sub>, SER<sub>3</sub>... SER<sub>N</sub>)
5. Ser\_Auth  $\leftarrow$  **Extract:** SER (SID, VTYPE, TS, Req\_Type)
6. REQ\_Conn  $\leftarrow$  Ser\_Auth: **Compare** (SER, REG\_DB)
7. **if** (REQ\_Conn == Registered) **then**
8. RRSUi  $\leftarrow$  **Return** REQ\_Conn (SER, TGS\_Req, Nonce)
9. **else**
10. RRSUi  $\leftarrow$  **Return** REQ\_Conn (SER, Terminate)
11. **end if**
12. **End Loop**
13. **END**

PSEUDOCODE 1: Authentication check for service request from stakeholders.

TABLE 3: Classification types of vehicular nodes.

Sl. No.	Vehicle types (VTYPE)	Vehicle names	Priority level
1	A	Ambulance	1
2	B	Government	2
3	C	Patrols	3
4	D	Subunits	4
5	E	Commercial	5
6	F	Logistics	6
7	G	Bicycles (optional)	7

TABLE 4: Simulation parameters.

Parameters	Value
Simulation environment	2000*2000*500
Number of RSU nodes	5, 10, 15, ...
Number of vehicular nodes	50, 100, 150, ...
Total number of packets	500, 1000, 1500, ...
The velocity of vehicular nodes	2 m/s
The velocity of RSU nodes	5 m/s
Time instant for every $T$ second	60, 120, 180 s
Total simulation time	1000 s

and development. In our proposed idea, we have considered 5 bits of MPLS header label for our research idea. Table 1 illustrates the different MPLS labels used in the transportation environment.

Once the appropriate requested service is fetched from the TGS server, a response message is generated and arranged in the queue for transmission. The scheduling mechanism for the proposed scheme follows a non-preemptive methodology in which the priority packets trigger the queue for accessing the data service. The vehicle classification process crossverifies the connectivity subsystem of which type of stakeholder is requested and the current network status to communicate or relay the response message/service to the neighboring RSU agents in the transportation field. As shown in Table 3, it offers access to and obtains the most recent service updates for various types of requests represented by vehicular nodes.

#### 4. Experimental Setup

A network simulator (NS-3) is used to test the viability of the data security framework. A 3D rectangular waypoint mobility model for RSU and vehicle nodes is used to assess the data security framework's performance. Auxiliary Network Animator (NetAnim) software with a third-party programming language is used to examine, classify, and compute the received data packet packets based on the queuing factors

toward the incoming arrival rates and simulation. Table 4 shows the simulation parameters employed in a three-dimensional transportation simulation.

The data security framework's performance is evaluated in two ways: (1) computation analysis and (2) performance comparison with competing methods. After experimenting with these two features, the data security architecture defines its best-case and worst-case scenarios for use over its vehicular nodes in the transportation environment. In our experiment, we have considered a storage file to which the requested data packets are received. We have used a readline () function to process and provide data service based on the network connectivity level. For example, if there are three vehicular nodes with a network connectivity level of high, then their corresponding node IDs and connectivity levels will be used as pointers to pinpoint the received data packets from the storage file for data service. The information exchanged among aerial and ground nodes are simple bit sequences; hence, the file size is a few kilobytes.

*4.1. Computation Analysis.* The MPLS label classification and queuing factors are computed to identify the demanding service from the vehicular nodes. Based on the data packet requests, the feasibility of the packet-label classifier subsystem is demonstrated under two test scenarios based on incoming arrival rates, namely, adaptive and static. The incoming request

TABLE 5: Usage of adaptive vs. static arrival rates.

Sl. No.	Arrival rates	Descriptions
1	Adaptive	(i) The arrival rate ( $\lambda$ ) varies depending on the stakeholder's request and the network connections (ii) The service rate ( $\mu$ ) is set to a maximum threshold value $X$ (urban or highway) depending on the service demand and environmental conditions (iii) Best-case scenario: RSU nodes can receive a range of 0 to $N$ data packet requests from their stakeholders (iv) Worst-case scenario: a significant resource allocation is required to process the data packet request occasionally
2	Static	(i) The arrival rate ( $\lambda$ ) collects a set number of data packet requests from stakeholders (ii) If the RSU node takes longer to process the data packet request, the service rate ( $\mu$ ) becomes dynamic (iii) Best case: to provide adequate data with its stakeholders in processing the request (iv) Worst case: lack of data priority and contention due to multiple stakeholders' requests sent over a fixed communication channel rate

TABLE 6: Queuing analysis of adaptive arrival rate under  $\mu_1 = 1000/\text{sec}$ .

Vehicular nodes	Queuing factors							Connectivity time (sec)	Vehicle priority
	( $\lambda/\text{sec}$ )	( $\rho$ ) (%)	( $P_0$ ) (%)	( $L_S$ )	( $L_Q$ )	( $W_S$ ) (sec)	( $W_Q$ ) (sec)		
V-1	820	0.820	0.180	4.556	3.736	20.00	16.40	1.22	2
V-2	120	0.120	0.880	0.136	0.016	4.09	0.49	8.35	5
V-3	20	0.020	0.980	0.020	0.001	3.67	0.07	52.43	3
V-4	100	0.100	0.900	0.111	0.011	4.00	0.40	10.00	5
V-5	140	0.140	0.860	0.163	0.023	4.19	0.59	7.10	4
V-6	900	0.900	0.100	9.000	8.100	36.00	32.40	1.11	2
V-7	20	0.020	0.980	0.020	0.001	3.67	0.07	52.43	1
V-8	880	0.880	0.120	7.333	6.453	30.00	26.40	1.14	6
V-9	790	0.790	0.210	3.762	2.972	17.14	13.54	1.27	4
V-10	140	0.140	0.860	0.163	0.023	4.19	0.59	7.10	3
Average	393	0.393	0.607	2.5264	2.1334	12.695	9.095	14.21	

TABLE 7: Queuing analysis of adaptive arrival rate under  $\mu_2 = 1000/\text{sec}$ .

Vehicular nodes	Queuing factors							Connectivity time (sec)	Vehicle priority
	( $\lambda/\text{sec}$ )	( $\rho$ ) (%)	( $P_0$ ) (%)	( $L_S$ )	( $L_Q$ )	( $W_S$ ) (sec)	( $W_Q$ ) (sec)		
V-1	800	0.800	0.200	4.000	3.200	18.00	14.40	1.25	6
V-2	450	0.450	0.550	0.818	0.368	6.55	2.95	2.22	5
V-3	200	0.200	0.800	0.250	0.050	4.50	0.90	5.00	3
V-4	110	0.110	0.890	0.124	0.014	4.04	0.44	9.18	4
V-5	440	0.440	0.560	0.786	0.346	6.43	2.83	2.27	2
V-6	850	0.850	0.150	5.667	4.817	24.00	20.40	1.18	1
V-7	110	0.110	0.890	0.124	0.014	4.04	0.44	9.18	6
V-8	900	0.900	0.100	9.000	8.100	36.00	32.40	1.11	1
V-9	700	0.700	0.300	2.333	1.633	12.00	8.40	1.43	5
V-10	440	0.440	0.560	0.786	0.346	6.43	2.83	2.27	4
Average	500	0.5	0.5	2.3888	1.8888	12.199	8.599	3.51	

packets follow the hybrid approach of dynamic and static arrival rates. To differentiate the arrival rates and their performance towards the queuing factors, we have separately measured them in two parts. The descriptive information about using these two test scenarios within the data security architecture is shown in Table 5.

The numerical dataset acquired in measuring the queuing factors from RSU agents under adaptive arrival rates with two different service rates,  $\mu_1$ , and  $\mu_2$ , is shown in Tables 6 and 7.

The service rate is set to a maximum threshold of  $\mu_1$  and  $\mu_2$  in the best-case scenario, allowing the RSU agents to receive a range of 0 to  $N - 1$  data packet requests from its

TABLE 8: Queuing analysis of static arrival rate under  $\lambda_1 = 100/\text{sec}$ .

Vehicular nodes	$(\lambda/\text{sec})$	$(\rho)$ (%)	$(P_0)$ (%)	Queuing factors				Connectivity time (sec)	Vehicle priority
				$(L_S)$	$(L_Q)$	$(W_S)$ (sec)	$(W_Q)$ (sec)		
V-1	100	0.100	0.900	0.111	0.011	4.00	0.40	10	2
V-2	100	0.100	0.900	0.111	0.011	4.00	0.40	10	5
V-3	100	0.100	0.900	0.111	0.011	4.00	0.40	10	3
V-4	100	0.100	0.900	0.111	0.011	4.00	0.40	10	5
V-5	100	0.100	0.900	0.111	0.011	4.00	0.40	10	4
V-6	100	0.100	0.900	0.111	0.011	4.00	0.40	10	2
V-7	100	0.100	0.900	0.111	0.011	4.00	0.40	10	1
V-8	100	0.100	0.900	0.111	0.011	4.00	0.40	10	6
V-9	100	0.100	0.900	0.111	0.011	4.00	0.40	10	4
V-10	100	0.100	0.900	0.111	0.011	4.00	0.40	10	3
Average	100	0.100	0.900	0.111	0.011	4.00	0.40	10	

TABLE 9: Queuing analysis of static arrival rate under  $\lambda_2 = 200/\text{sec}$ .

Vehicular nodes	$(\lambda/\text{sec})$	$(\rho)$ (%)	$(P_0)$ (%)	Queuing factors				Connectivity time (sec)	Vehicle priority
				$(L_S)$	$(L_Q)$	$(W_S)$ (sec)	$(W_Q)$ (sec)		
V-1	200	0.100	0.900	0.111	0.011	2.00	0.20	10	2
V-2	200	0.100	0.900	0.111	0.011	2.00	0.20	10	5
V-3	200	0.100	0.900	0.111	0.011	2.00	0.20	10	3
V-4	200	0.100	0.900	0.111	0.011	2.00	0.20	10	5
V-5	200	0.100	0.900	0.111	0.011	2.00	0.20	10	4
V-6	200	0.100	0.900	0.111	0.011	2.00	0.20	10	2
V-7	200	0.100	0.900	0.111	0.011	2.00	0.20	10	1
V-8	200	0.100	0.900	0.111	0.011	2.00	0.20	10	6
V-9	200	0.100	0.900	0.111	0.011	2.00	0.20	10	4
V-10	200	0.100	0.900	0.111	0.011	2.00	0.20	10	3
Average	200	0.100	0.900	0.111	0.011	2.00	0.20	10	

TABLE 10: Comparative analysis techniques.

Sl. No.	Title	Descriptions
1	Misbehavior detection and efficient revocation within VANET [38]	A new framework for the certificate revocation process within VANET is introduced. This process can be activated by the misbehavior detection systems (MDSs) running within vehicles and the misbehavior authority (MA) within the infrastructure, which identifies and excludes misbehaving vehicles to guarantee the long-term functionality of the network.
2	A Certificate less Pairing-Free Authentication Scheme for Unmanned Aerial Vehicle Networks [27]	A pairing-free authentication scheme (CLAS) is proposed for Unmanned Aerial Vehicle Networks (UAVNs) based on the certificateless signature technology. It supports batch verification at both the data aggregator (AGT) and commands center (CMC) sides so that the verification efficiency can be improved greatly.

stakeholders every time interval  $T_i$ . When the RSU agents receive the data packet request, we also notice that they compute their vehicle priority checker's average server usage ( $\rho$ ). Once checked, the associated RSU node can determine whether or not it can offer the desired service to the requested stakeholders on time.

Tables 8 and 9 show the numerical dataset gathered from a single RSU agent to measure the queuing factors of data packet requests under two different arrival rates,  $\lambda_1$ , and  $\lambda_2$ , respectively, in contrast to the adaptive arrival rate.

The best-case scenario for this strategy is that the data packet request at the arrival rate is set to a minimum threshold.

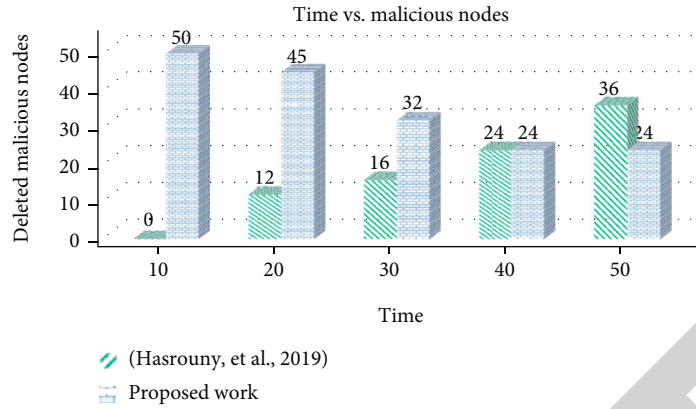


FIGURE 4: Time vs. detected malicious node.

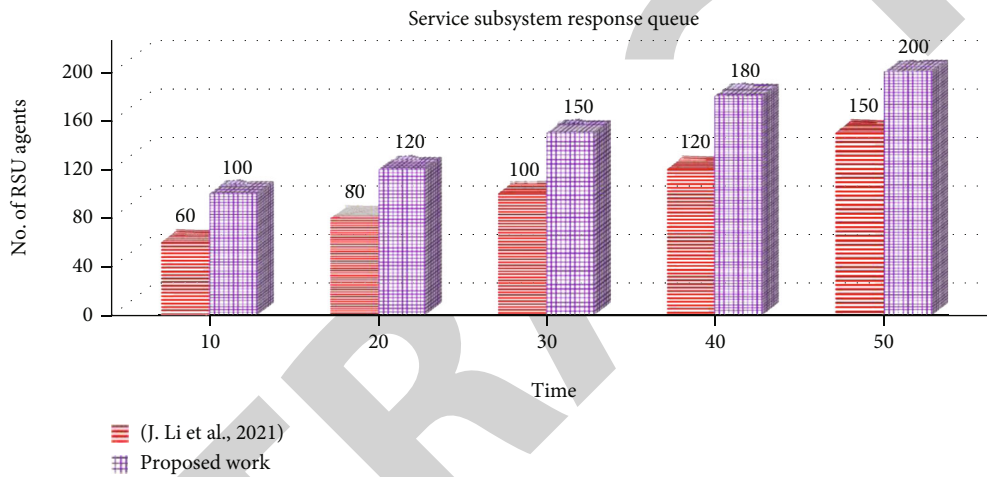


FIGURE 5: Time vs. response queue.

As a result, whether the RSU agent’s network connections are different in processing the desired service, the RSU agents can offer acceptable data to their stakeholders.

4.2. Comparative Analysis. The data security framework has been compared to existing methodologies for two performance indicators, key generation and malicious node detection, at various time instants and the rising number of data packet requests across vehicle nodes. Some of the comparison assessments performed against the proposed model are shown in Table 10.

Figure 4 shows the performance metrics for monitoring the misbehaving nodes in the environment. As time increases, the proposed work identifies the stakeholder behavior according to their idle state and requests unnecessary data queries to the RSU agents. The authentication right is revoked upon these constraints, and the service access link is disconnected.

Figure 5 depicts the service subsystem’s response queue of accepting data service requests from all the stakeholders in the environment. Several RSU agents must process and accumulate the data service requests as time increases. The proposed work requires more RSU agents since the idea of the work is

designed for smart city applications. However, in reality, the deployment of RSU agents in the field will be quite small.

The performance metric “network load” of each vehicular node is calculated against three existing schemes, (1) AIR-RSU framework [1], (2) load balanced routing (LBR), and (3) nearest neighbor routing (NNR) [39]. Each node periodically forwards controls beacon messages to its nearest node to communicate/reach aerial nodes. Figure 6 depicts the network load of individual vehicular nodes at time instants among the existing schemes. Also, it is observed that the network load in LDR and NNR gradually increases as the number of nodes in the transportation environment increases. However, for the AIR-RSU framework and proposed work, the network load in every individual node is equally shared between the vehicular nodes giving an equal chance to communicate and process the information with aerial nodes.

Finally, the level of network density is measured in terms of the percentage of actual connections of a single aerial node or the average of multiple aerial nodes. The network density is defined and given in (source: <https://www.the-vital-edge.com/what-is-network-density>) for the entire network. A single aerial node can establish one or more logical connections depending upon the number of vehicular nodes joining the

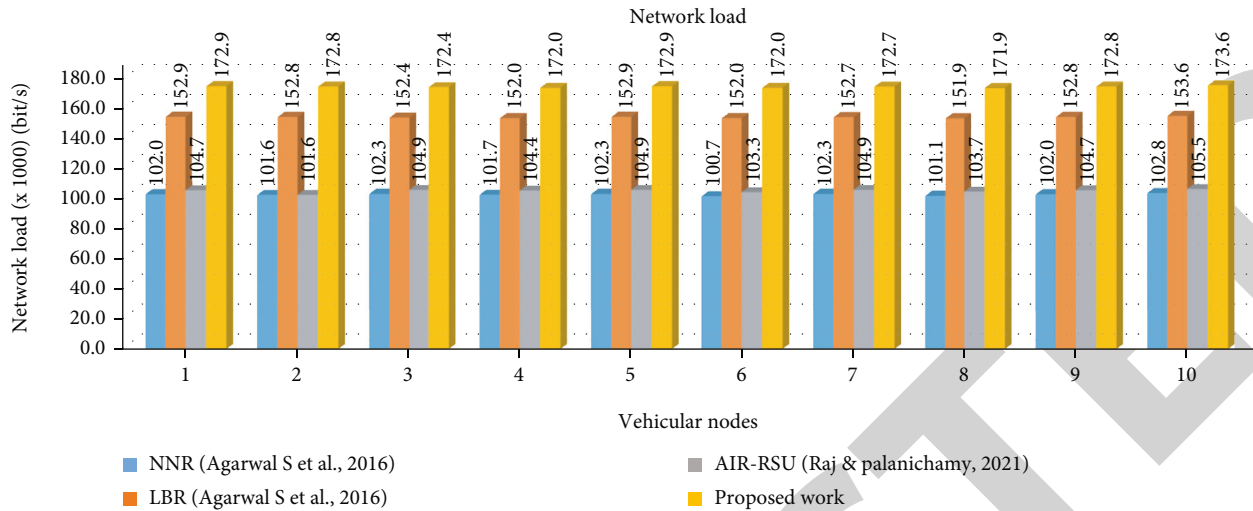


FIGURE 6: Network load of vehicular nodes.

TABLE 11: Network density for single aerial node with range of actual connections.

Nodes	Actual connections (10)	Actual connections (20)	Actual connections (30)	Actual connections (40)	Actual connections (50)
10	0.18	0.36	0.55	0.73	0.91
15	0.08	0.17	0.25	0.33	0.42
20	0.05	0.10	0.14	0.19	0.24
25	0.03	0.06	0.09	0.12	0.15
30	0.02	0.04	0.06	0.09	0.11
35	0.02	0.03	0.05	0.06	0.08
40	0.01	0.02	0.04	0.05	0.06

TABLE 12: Average network density for multiple aerial nodes with range of actual connections.

Nodes	Actual connections (10)	Actual connections (20)	Actual connections (30)	Actual connections (40)	Actual connections (50)
10	0.15	0.31	0.46	0.62	0.77
15	0.09	0.15	0.22	0.30	0.37
20	0.06	0.09	0.13	0.17	0.22
25	0.04	0.06	0.09	0.11	0.14
30	0.03	0.04	0.06	0.08	0.10
35	0.02	0.03	0.05	0.06	0.08
40	0.02	0.02	0.03	0.05	0.06

network within the range. The benefit of providing additional connections for a specific node has a backup connection, multiple hardware communications (i.e., sensors, GPS, tracking camera, and other secondary communications), and infotainment communication. Hence, the more the connection, the higher the network density. In other words, the higher the network density, the better the connectivity.

Tables 11 and 12 represent the network density measure under range of actual connections with a single aerial node and an average of multiple aerial nodes, respectively.

The best case of the proposed application scenario is that as the number of actual connections increases for aerial nodes, the network density among vehicular nodes is almost

entirely connected, and it approaches 1 in a normalized range. However, the worst case of this application scenario is that as the number of vehicular nodes joining the network increases, the network density tends to decrease to a minimum value of 0.01. The overhead of the entire network will increase concerning its bandwidth, latency, and network load as the number of mobile sink nodes and vehicular nodes joining the network increases.

## 5. Conclusion and Future Works

This paper proposes a new topological design for smart city applications, i.e., a Secure Authentication Relay-Based Urban

Network (S-ARUN) specially constructed for registered transportation stakeholders. These registered stakeholders were connected to the S-ARUN topology hold an in-built data security framework consisting of three subsystems: (1) self-authentication subsystem: the requesting stakeholder must authentic itself by sharing its identity to the source responder before transmitting its actual data service request, (2) vehicle classification subsystem: a priority for the data service request will be given based on the type of stakeholder and request needs, and (3) request accumulator subsystem: every source responder will be maintaining a separate queue to accumulate the data service requests to process and transmit the requested data service to the appropriate stakeholder in a short time. The working principle of S-ARUN follows the Kerberos authentication technique where the stakeholders are connected in a well-secured authentic manner.

Results indicate that the best and worst cases of the proposed work are tested under various queuing analysis arrival rates. On the other hand, the priority of the vehicle towards the vehicular nodes is allocated based on their query request type and physical parameters such as distance, signal strength, and velocity. Moreover, the comparison of the malicious node detection and request accumulator procedure with other schemes is analyzed in detail.

For future works, the data security framework will be tested in a real-time environment, where the benefits and drawbacks of the working process will be clearly defined. Also, we can compare the proposed idea with and without a security mechanism for future enhancement. Also, the idea of using without a security mechanism will show great performance value than working with a security mechanism. But the counterpart to using a security mechanism, the malicious nodes can be identified over time. In addition, the data security framework architecture will be evaluated in a heterogeneous vehicular network to experience the incoming arrival rate of data packets towards the RSU networks at the network layer, data-link layer, and physical layers.

## Data Availability

The original data presented in the study are included in the article and queries can be directed to the all authors.

## Conflicts of Interest

The authors declare that they have no conflicts of interest.

## References

- [1] A. S. A. Raj and Y. Palanichamy, "Packet classification based aerial intelligent relay-road side unit (air-rsu) framework for vehicular ad-hoc networks," *Peer-to-Peer Networking and Applications*, vol. 14, no. 3, pp. 1132–1153, 2021.
- [2] H. H. Jeong, Y. C. Shen, J. P. Jeong, and T. T. Oh, "A comprehensive survey on vehicular networking for safe and efficient driving in smart transportation: a focus on systems, protocols, and applications," *Vehicular Communications*, vol. 31, article 100349, 2021.
- [3] R. S. Shukla, N. Tyagi, A. Gupta, and K. K. Dubey, "A new position based routing algorithm for vehicular ad hoc networks," *Telecommunication Systems*, vol. 75, no. 2, pp. 205–220, 2020.
- [4] Z. C. Liu, L. Xiong, T. Peng, D. Y. Peng, and H. Liang, "A realistic distributed conditional privacy-preserving authentication scheme for vehicular ad hoc networks," *IEEE Access*, vol. 6, pp. 26307–26317, 2018.
- [5] 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.
- [6] M. A. Al-Shareeda, M. Anbar, I. H. Hasbullah, and S. Manickam, "Survey of authentication and privacy schemes in vehicular ad hoc networks," *IEEE Sensors Journal*, vol. 21, no. 2, pp. 2422–2433, 2021.
- [7] A. S. A. Raj and Y. Palanichamy, "An aerial intelligent relay-road side unit (AIR-RSU) framework for modern intelligent transportation system," *Peer-to-Peer Networking and Applications*, vol. 13, no. 3, pp. 965–986, 2020.
- [8] S. Lall, A. S. Alfa, and B. T. Maharaj, "The role of queueing theory in the design and analysis of wireless sensor networks: an insight," in *2016 IEEE 14th International Conference on Industrial Informatics (INDIN)*, pp. 1191–1194, Poitiers, France, 2016.
- [9] R. Zaghali, K. Thabatah, and S. Salah, "Towards a smart intersection using traffic load balancing algorithm," in *2017 Computing Conference*, pp. 485–491, London, UK, 2017.
- [10] S. S. Manvi and S. Tangade, "A survey on authentication schemes in VANETs for secured communication," *Vehicular Communications*, vol. 9, pp. 19–30, 2017.
- [11] R. Fotohi, E. Nazemi, and F. Shams Aliee, "An agent-based self-protective method to secure communication between UAVs in unmanned aerial vehicle networks," *Vehicular Communications*, vol. 26, article 100267, 2020.
- [12] S.-J. Horng, S.-F. Tzeng, P.-H. Huang, X. Wang, T. Li, and M. K. Khan, "An efficient certificateless aggregate signature with conditional privacy-preserving for vehicular sensor networks," *Information Sciences*, vol. 317, pp. 48–66, 2015.
- [13] M. Azees, "Reply to comments on dual authentication and key management techniques for secure data transmission in vehicular ad hoc networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 20, no. 9, pp. 3595–3595, 2019.
- [14] H. Tan, D. Choi, P. Kim, S. Pan, and I. Chung, "Comments on dual authentication and key management techniques for secure data transmission in vehicular ad hoc networks," in *IEEE Transactions on Intelligent Transportation Systems*, vol. 19, no. 7, pp. 2149–2151, 2018.
- [15] M. C. Chuang and J. F. Lee, "TEAM: trust-extended authentication mechanism for vehicular ad hoc networks," *IEEE Systems Journal*, vol. 8, no. 3, pp. 749–758, 2014.
- [16] X. Lin and X. Li, "Achieving efficient cooperative message authentication in vehicular ad hoc networks," *IEEE Transactions on Vehicular Technology*, vol. 62, no. 7, pp. 3339–3348, 2013.
- [17] 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.
- [18] X. Zhu, S. Jiang, L. Wang, and H. Li, "Efficient privacy-preserving authentication for vehicular ad hoc networks," *IEEE Transactions on Vehicular Technology*, vol. 63, no. 2, pp. 907–919, 2014.

- [19] J. Cui, L. Wei, J. Zhang, Y. Xu, and H. Zhong, "An efficient message-authentication scheme based on edge computing for vehicular ad hoc networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 20, no. 5, pp. 1621–1632, 2019.
- [20] J. Shao, X. Lin, R. Lu, and C. Zuo, "A threshold anonymous authentication protocol for VANETs," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 3, pp. 1711–1720, 2016.
- [21] F. Azam, S. K. Yadav, N. Priyadarshi, S. Padmanaban, and R. C. Bansal, "A comprehensive review of authentication schemes in vehicular ad-hoc network," *IEEE Access*, vol. 9, pp. 31309–31321, 2021.
- [22] W. Shen, L. Liu, X. Cao, Y. Hao, and Y. Cheng, "Cooperative message authentication in vehicular cyber-physical systems," *IEEE Transactions on Emerging Topics in Computing*, vol. 1, no. 1, pp. 84–97, 2013.
- [23] B. Ying and A. Nayak, "Anonymous and lightweight authentication for secure vehicular networks," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 12, pp. 10626–10636, 2017.
- [24] M. R. Asaar, M. Salmasizadeh, W. Susilo, and A. Majidi, "A secure and efficient authentication technique for vehicular ad-hoc networks," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 6, pp. 5409–5423, 2018.
- [25] P. Vijayakumar, M. Azees, A. Kannan, and L. J. Deborah, "Dual authentication and key management techniques for secure data transmission in vehicular ad hoc networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 17, no. 4, pp. 1015–1028, 2016.
- [26] H. Li, Y. Niu, J. Yi, and H. Li, "Securing offline delivery services by using Kerberos authentication," *IEEE Access*, vol. 6, pp. 40735–40746, 2018.
- [27] J. Li, Y. Wang, Y. Ding, W. Wu, C. Li, and H. Wang, "A certificateless pairing-free authentication scheme for unmanned aerial vehicle networks," *Security and Communication Networks*, vol. 2021, Article ID 9463606, 10 pages, 2021.
- [28] H. Al-Omais, E. A. Sundararajan, R. Alsaqour, N. F. Abdullah, and M. Abdelhaq, "A survey of data dissemination schemes in vehicular named data networking," *Vehicular Communications*, vol. 30, 2021.
- [29] U. Arshad, M. Ali Shah, and N. Javaid, "Futuristic blockchain based scalable and cost-effective 5G vehicular network architecture," *Vehicular Communications*, vol. 31, 2021.
- [30] S. A. Soleymani, S. Goudarzi, M. H. Anisi, M. Zareei, A. H. Abdullah, and N. Kama, "A security and privacy scheme based on node and message authentication and trust in fog-enabled VANET," *Vehicular Communications*, vol. 29, article 100335, 2021.
- [31] Y. Chen, J. Yuan, and Y. Zhang, "An improved password-authenticated key exchange protocol for VANET," *Vehicular Communications*, vol. 27, article 100286, 2021.
- [32] S. A. Eftekhari, M. Nikooghadam, and M. Rafiqhi, "Security-enhanced three-party pairwise secret key agreement protocol for fog-based vehicular ad-hoc communications," *Vehicular Communications*, vol. 28, article 100306, 2021.
- [33] S. O. Ogundoyin and I. A. Kamil, "An efficient authentication scheme with strong privacy preservation for fog-assisted vehicular ad hoc networks based on blockchain and neuro-fuzzy," *Vehicular Communications*, vol. 31, article 100384, 2021.
- [34] M. L. M. Peixoto, A. H. O. Maia, E. Mota et al., "A traffic data clustering framework based on fog computing for VANETs," *Vehicular Communications*, vol. 31, article 100370, 2021.
- [35] K. Rao and N. Ram, "Application of time synchronization process to Kerberos," *Procedia Computer Science*, vol. 85, pp. 249–254, 2016.
- [36] A. P. Shrestha, D. Y. Choi, G. R. Kwon, and S. J. Han, "Kerberos based authentication for inter-domain roaming in wireless heterogeneous network," *Computers and Mathematics with Applications*, vol. 60, no. 2, pp. 245–255, 2010.
- [37] R. Sultana, J. Grover, and M. Tripathi, "Security of SDN-based vehicular ad hoc networks: state-of-the-art and challenges," *Vehicular Communications*, vol. 27, 2021.
- [38] H. Hasrouny, A. E. Samhat, C. Bassil, and A. Laouiti, "Misbehavior detection and efficient revocation within VANET," *Journal of Information Security and Applications*, vol. 46, pp. 193–209, 2019.
- [39] S. Agarwal, A. Das, and N. Das, "An efficient approach for load balancing in vehicular ad-hoc networks," in *In 2016 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*, Bangalore, India, 2016.