Nanotechnology Perceptions
ISSN 1660-6795
www.nano-ntp.com

TR-DSR: A Trusted and Reputation-based Protocol for Securing Data Transmission in the Internet of Vehicle Things (IoVT) against Black Hole Attacks

Rahamathullah Ubaidullah[1], Dr. Karthikeyan Easwaramurthy[2]

[1]Research Scholar, Department of Computer Science, Government Arts College, Udumalpet - 642126, Tamilnadu, India, rah.jmc@gmail.com
[2]Head and Assistant Professor, Department of Computer Science, Government Arts College, Udumalpet - 642126, Tamilnadu, India, Email: e_karthi@yahoo.com

Ensuring the secure dissemination of authenticated data in the Internet of Vehicle Things (IoVT) is vital due to the critical role of Intelligent Transport Systems (ITS). These systems operate in environments characterized by dynamic vehicles, open and shared communication channels, self-organized and distributed networks, and a lack of centralized infrastructure. Such conditions make the IoVT susceptible to various security threats, including both internal and external attacks. Among internal threats, the black hole attack poses a significant challenge by dropping incoming packets intended for forwarding, thereby disrupting normal operations and degrading system performance. To mitigate this issue, this study introduces a Trusted and Reputation-based Dynamic Source Routing (TR-DSR) protocol. The TR-DSR protocol aims to enhance secure data transmission by identifying and eliminating malicious vehicles involved in black hole attacks while ensuring authentication among communicating vehicles. Advanced techniques, including Q-learning and Multi-Agent Systems (MAS), are integrated into TR-DSR to strengthen its security capabilities. The proposed protocol's performance has been evaluated through simulations using various metrics and compared with existing approaches. The results demonstrate the superiority of the TR-DSR protocol, emphasizing its effectiveness in addressing security challenges within the IoVT.

Keywords: Internet of Vehicle Things (IoVT), Intelligence Transport System, Data dissemination, DSR, Security, Black Attack, Authentication, Trust, Q-learning and Multi Agent System.

1. Introduction

Advancements in wireless technology and the Internet of Things (IoT) have significantly influenced the development of the Internet of Vehicle Things (IoVT). Both IoT and IoVT are critical to advancing Intelligent Transport Systems (ITS), offering a sophisticated and enhanced driving experience (Yang, D.-K et al., 2000). These technologies have emerged as promising solutions in the automotive industry, prioritizing driver comfort and safety. In IoVT, mobile nodes are represented as connected vehicles, comprising stationary or moving vehicles linked via wireless networks (Wang, X et al., 2016). The network structure can operate under infrastructure-based or non-infrastructure modes. The infrastructure mode typically involves Road Side Units (RSUs) (MORAIS, N. B. S. D, 2022), while non-infrastructure mode relies on vehicle-to-vehicle communication.

Although IoVT offers numerous benefits, securing connected vehicles is a significant challenge due to the absence of embedded security features. In countries like India, manufacturers often prioritize cost reduction over enhancing vehicle security systems (Zear, A et al., 2016, Chen, R et al., 2022). Consequently, maintaining robust security in IoVT remains a persistent concern. Routing protocols are fundamental to enabling communication among vehicles, as they facilitate data dissemination (Jawad, S et al., 2021, Shon, T. 2021). Their primary purpose is to establish routes from source to destination. Protocols such as RPL, AODV, DSR, TORA, and DSDV are commonly used to determine optimal routes between vehicles in the IoVT environment (Shah, Z et al., 2021). These routes may involve single-path or multipath configurations. This study focuses on the Dynamic Source Routing (DSR) protocol, which supports multipath routing between vehicles but lacks built-in security measures, making it vulnerable to various attacks. Among these, the black hole attack is particularly prominent within IoVT environments (Batra, N et al., 2024, Liu, S et al., 2022).

IoVT security relies on several key requirements, including authentication, data confidentiality, authorization, integrity, non-reputation, and service availability (William Stallings, 2003, Sabri, Y et al., 2021). Among these, authentication serves as the foundation by verifying the identities of communicating vehicles, enabling the enforcement of other security requirements (Karim, A., 2022). However, the dynamic and open nature of IoT-based IoVT environments makes achieving authentication particularly challenging. Vehicles often communicate without adequate security protocols, resulting in potential security breaches. Therefore, ensuring secure vehicle communication is critical to achieving a safe and reliable IoVT ecosystem (Taslimasa, H et al., 2023, Sadhu, P. K et al., 2022).

The presence of a black hole attack severely disrupts the functionality and reliability of the Internet of Vehicle Things (IoVT). In such an attack, a malicious vehicle or node falsely claims to have the shortest path to all destinations, intercepting data packets and subsequently dropping them instead of forwarding them to the intended recipients. This malicious behavior leads to several adverse effects on the IoVT environment. Communication is disrupted, preventing vehicles from receiving critical information such as traffic updates or safety alerts, and resulting in significant data loss. Network congestion may increase as legitimate nodes attempt retransmissions to recover lost packets, further straining the system. Performance metrics such as packet delivery ratio, throughput, and latency

degrade, reducing the overall efficiency of the network. Safety is also compromised, as the timely exchange of information critical to collision avoidance or emergency response is obstructed, increasing the risk of accidents.

Additionally, the attack erodes trust within the network, causing vehicles to become wary of relying on communication from other nodes, weakening IoVT's collaborative framework. The repeated retransmissions and rerouting efforts required to overcome packet loss also lead to increased energy consumption, especially for resource-constrained devices. As IoVT networks scale, these issues become even more pronounced, undermining the system's ability to handle growing vehicle populations. Mitigating the impact of black hole attacks necessitates robust security measures such as trust-based routing protocols, intrusion detection systems, and effective authentication mechanisms to identify and isolate malicious nodes, ensuring the network's resilience and integrity.

The structure of this paper is organized as follows: Section 2 provides the background of the proposed work, including details on the Multi-Agent System. Section 3 outlines the adversary model. Section 4 discusses the importance of authentication in Intelligent Transport Systems. Section 5 reviews related works. Section 6 presents the proposed solution. Section 7 details the results and discussion, and the final section concludes the study.

1.1 Contribution of the Proposed Work:

- Development of TR-DSR Protocol: The study introduces a novel Trusted and Reputation-based Dynamic Source Routing (TR-DSR) protocol designed to enhance secure data dissemination in the Internet of Vehicle Things (IoVT) by addressing internal security threats, particularly black hole attacks.

- Integration of Advanced Techniques: The proposed TR-DSR protocol incorporates Q-learning and Multi-Agent Systems (MAS) to improve its ability to detect and eliminate malicious nodes, thereby strengthening the overall security of the IoVT environment.

- Focus on Authentication: The protocol ensures authentication among communicating vehicles, laying a strong foundation for secure interactions within the IoVT network.

2. Background: Multi-Agent System (MAS)

The proposed trust model is designed using the principles of a Multi-Agent System (MAS). The subsequent section explores the role of MAS in the Internet of Vehicle Things (IoVT) environment and examines the motivations behind its adoption by researchers, as highlighted by Van der Hoek et al. (2008) and Dorri et al. (2018). MAS has garnered significant attention in the computing field due to its numerous advantages: 1) facilitating interaction among individuals that can be analyzed and modeled, 2) catering to application-specific needs, and 3) enabling the division of complex modeling and computational tasks into manageable subcomponents or layers. According to Balaji et al. (2010), MAS is defined as "a group of autonomous entities, referred to as agents, working collaboratively within a shared environment to achieve specific goals." Uhrmacher et al. (2018) describe an agent as

"an autonomous computational system situated in an environment, capable of taking actions to fulfill its designed objectives." Agents are equipped to navigate their environment, gather information, communicate, and interact with other agents. However, since agents often operate with limited resources, they collaborate within the MAS framework to efficiently complete assigned tasks. Agents possess key attributes such as mobility, autonomy, intelligence, and communication abilities (Julian et al., 2019).

MAS is characterized by three core capabilities: social ability, reactivity, and proactiveness (Blas et al., 2020). Social ability refers to the capacity of an agent to cooperate with others to achieve shared goals. Reactivity is the agent's ability to adapt and respond to environmental changes. Proactiveness reflects an agent's dynamic, goal-oriented behavior to meet its objectives. These features make MAS an ideal choice for diverse applications, including recommender systems, data mining, mobile ad hoc networks, e-health, military operations, and more. Its flexibility and efficiency in solving complex problems underscore its relevance across various domains.

2.1 Mapping of MAS with Intelligence Transport System

When mapping the Multi-Agent System (MAS) to the Internet of Vehicle Things (IoVT) environment, each agent in the MAS is represented as a vehicle within the IoVT ecosystem. In this context, vehicles are not just physical entities but intelligent agents capable of interacting with one another to exchange crucial information. These interactions enable vehicles to collaboratively gather and share real-time data about various aspects of the driving environment. For instance, vehicles can communicate to obtain updates on traffic congestion, road accidents, optimal routes to reach a destination, and weather conditions along the travel path. Additionally, they can share information about nearby amenities such as fuel stations, charging points for electric vehicles, and rest areas, enhancing the overall driving experience.

This mapping leverages the inherent features of MAS, such as autonomy, intelligence, and communication capabilities, to create a dynamic and self-organizing network of connected vehicles. Each vehicle, as an agent, plays an active role in the ecosystem, not only consuming data but also contributing information to help other agents. This collaborative approach ensures efficient navigation, safety, and resource optimization within the IoVT framework. The interactions between agents are facilitated through wireless communication technologies, creating a robust and adaptive network capable of responding to real-time changes in the environment

The following figure illustrates how MAS principles are applied to the IoVT environment, showcasing the relationships and interactions between vehicles (agents) and highlighting how data flows seamlessly to support intelligent transport systems.

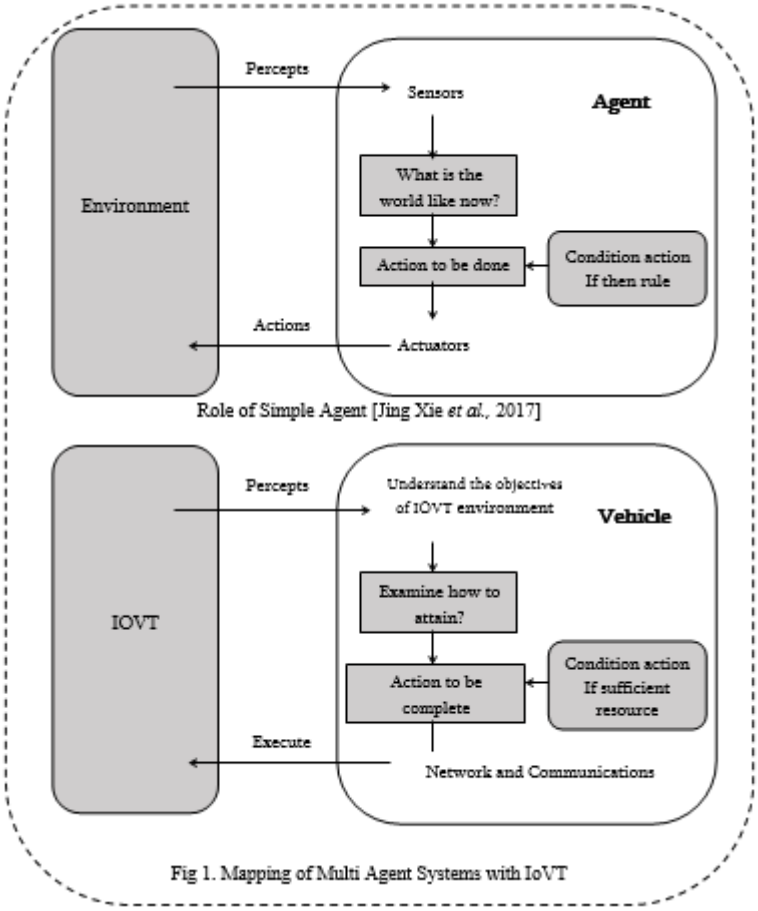

Fig 1. Mapping of Multi Agent Systems with IoVT

2.2 The reasons for opt of MAS for IoT based Intelligence Transport System

The characteristics and capabilities of MAS closely align with those of the IoVT environment, making it a suitable framework for the proposed work. For example, the cooperative behavior among agents in MAS mirrors the collaboration among vehicles in the IoVT ecosystem. Another key similarity is scalability. In MAS, agents can be dynamically added based on situational requirements. Similarly, in the IoVT environment, an indefinite number of vehicles can join the network, moving freely within the system and reflecting its inherently growing and dynamic nature.

Additionally, MAS features such as adaptability to open and dynamic environments, efficient task allocation, user preference handling, and task representation make it highly compatible with the IoVT framework. Most importantly, MAS significantly enhances network performance across various metrics, including reliability, robustness, maintainability, computational efficiency, flexibility, reusability, and responsiveness, as supported by previous studies (Yu et al., 2013; Chavhan et al., 2022; Rahman et al., 2022).

3. Adversary model: Black hole attack

In this section, we discuss the working nature of DSR routing protocol and impact of black hole attack in it.

3.1 Working nature of DSR

The following section explains the working principle of the Dynamic Source Routing (DSR) protocol (Johnson et al., 2001), which is classified as an on-demand routing protocol because it is activated only when needed. It operates based on source routing, meaning that all routing information is explicitly included in the packet header. As a result, intermediate nodes do not need to store routing information. The protocol involves two main phases: route discovery and route maintenance. Additionally, DSR supports both unidirectional and asymmetric links.In the IoVT environment, each vehicle maintains a route cache, which stores all available routing information. This helps reduce the propagation of route requests and accelerates the route discovery process. When a vehicle wants to send a packet to another vehicle, it first checks its route cache to see if the necessary routing information is available. If not, it initiates the route discovery process. The route request process begins by sending Route Request (RREQ) packets to neighboring vehicles. During this process, the initiating vehicle can simultaneously send and receive packets from other vehicles.

The destination vehicle, however, does not initiate the route request process. The RREQ packet contains the sender's address, the destination address, and a unique request ID assigned by the sender. The combination of the initiator's address and the request ID helps avoid the duplication of RREQ packets. Upon receiving a RREQ, the vehicle may either be an intermediate vehicle or the destination vehicle. If the vehicle is intermediate, it performs the following actions: If it finds its own address in the received RREQ, it discards the packet. If not, it appends its own address to the routing information in the RREQ and forwards it to its neighboring vehicles. If the receiving vehicle is the destination vehicle, it sends a Route Reply (RPLY) to the source vehicle using the address specified in its route cache. Once the source vehicle receives the RPLY, it sends the actual data packets to the destination vehicle via the established route.

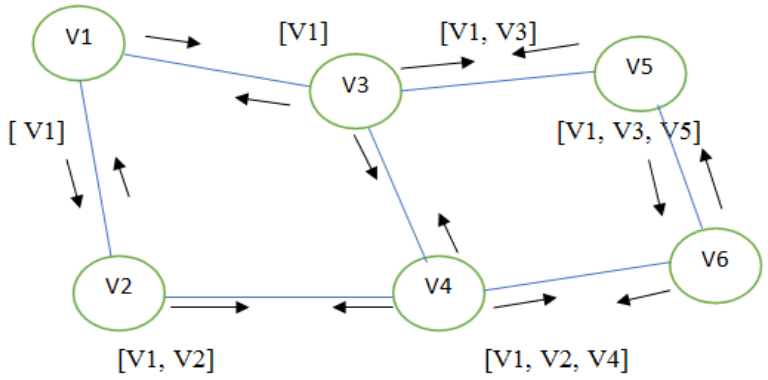

Fig. 2. Route Discovery Process

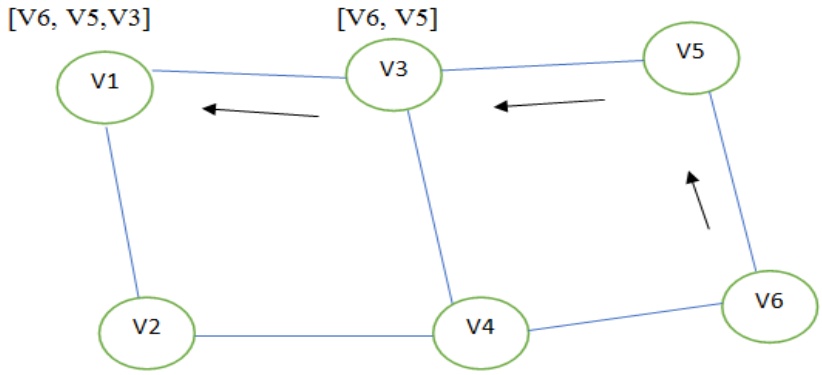

Fig. 3. Route Reply Process

The route discovery process of the DSR protocol operates as follows: In the given network, there are six vehicles: V1, V2, V3, V4, V5, and V6. The source vehicle is V1, and the destination vehicle is V6, with the remaining vehicles functioning as intermediate nodes. When vehicle V1 wants to transmit information to destination vehicle V6, it first checks its own route cache to determine if a route to V6 already exists. If a valid route is found, V1 will use it to send the information. If no route is available, V1 will initiate the route discovery process by broadcasting a Route Request (RREQ) packet.

Upon receiving the RREQ packet, intermediate vehicles such as V2 and V3 will append their own addresses to the routing information and forward the RREQ to other intermediate vehicles. This process continues until the destination vehicle, V6, receives the RREQ packet and recognizes that it is the intended recipient. Upon receiving the RREQ, V6 will send a Route Reply (RPLY) back to the source vehicle, V1, providing the route information needed to establish the communication path. Once the source vehicle V1 receives the RPLY, it can use the newly discovered route to transmit the data to destination vehicle V6.

3.2 Impact of black attack over DSR routing protocol

This section discusses the impact of black hole attack over DSR routing protocol. The following picture depicts the normal routing discovery process without black hole attack.

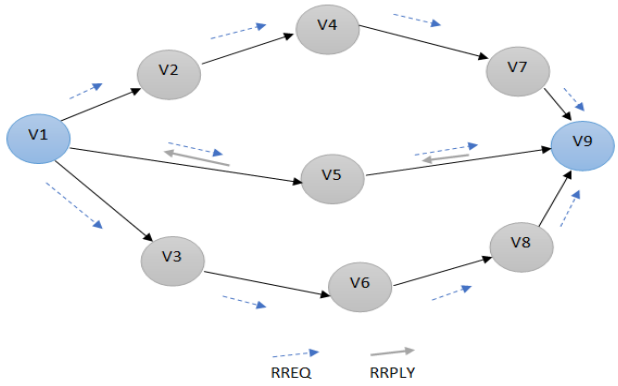

Fig. 4 Route discovery process of DSR without black hole attack

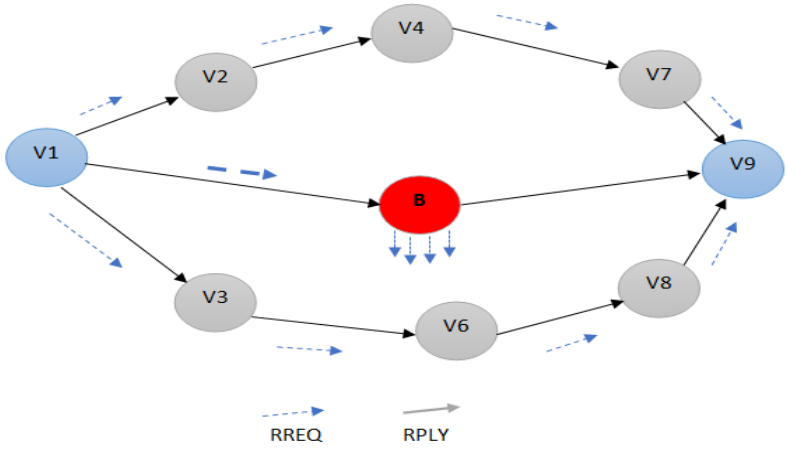

Fig 5. Impact of Black hole attack over DSR routing protocol

In the above IOVT environment which is shown in the fig. consists of nine nodes/vehicles denoted as V1, V2, V3, V4, V5, V6 and V7. Assume node V3 wants to transmit any traffic related information to the destination node V5. To do that, it will initiate route discovery process by sending RREQ packets. During the route discovery process, it comes to know there are three paths from source to the destination. The first path is V3-V4-V1-V2-V5. The second path is V3-V6-V7-V5 and the third path is V3-V4-V5.

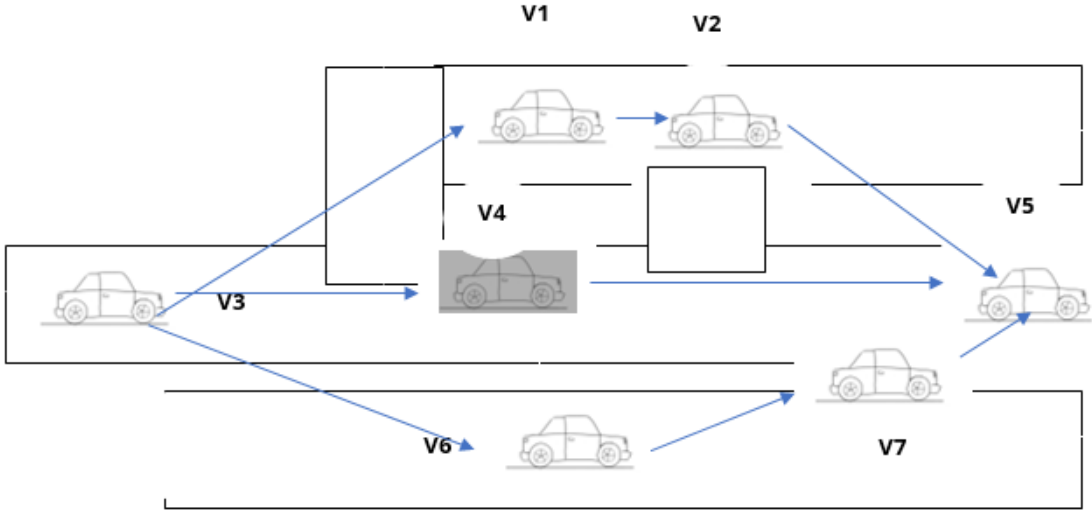

Fig 6.Demonstration of Black hole attack in IOVT over DSR

Among the three paths, the path V3-V4-V5 is also one of the path hence the route request will also proceed via that path also. Over the period of time vehicle V4 may behave as a black hole vehicle which is shown in the fig. so, all the data packets which is transferred via vehicle V4 will be dropped. Besides, the black hole vehicle also advertise itself that has the shortest route to the destination vehicle V5 by the way it tries to getting attention from other nodes and drop the packets which is transferred via this vehicle. By the way the black hole

attack can be executed in DSR routing protocol.

4. Need of Authentication for IoT based Intelligence Transport System

IOVT environment compromises of set of vehicles, road side units and other wireless enabled technologies to support the communication. All these elements working together and ensure the road safety. These vehicles are exchanging messages by data dissemination in the form of notifications such as presence of obstacles in the road, notifying oil bunks, notifying accident spots, nature of weather conditions and traffic jams in a certain area of the road. In this scenario, most of the vehicles are going to communicate with unknown vehicles. Therefore, there is a blindness in communication happens such blindness will lead to security violations. To address the issue, every vehicle must ensure the identity of communicating vehicle. This process is called authentication. In network security the authentication is defined as "the ability of a communicating node to ensure the identity of the communicated node" (William stalling, 2003). Typically, authentication can be achieved in two ways such as pre-authentication and post-authentication. In pre-authentication, all the vehicles are authenticated before participating in the IOVT environment. The second one is post-authentication, here over the period of time, every vehicle in the environment will be assessed and ensure the authentication (Y.Xiao et al., 2007). In this research work, we are focusing on post-authentication mechanism.

5. Review of literature

The following section discuss the some of the notable works in securing data dissemination over Vehicular Ad hoc Network.

The proposed work (Prakash et al., 2023) focuses on enhancing the security of Internet of Vehicle Things (IoVT) communications by identifying malicious nodes and detecting forged messages in Vehicular Ad-hoc Networks (VANETs). The authors introduced a Lightweight Blockchain-based Security Protocol (BSP-IOVT) to improve VANET security by effectively detecting and mitigating fake messages and malevolent nodes. The primary objectives of the proposed work (Hang et al., 2023) are to design a vehicle security early warning terminal based on the Internet of Things (IoT) and to enhance automobile safety while reducing asphyxiation incidents. The system utilizes carbon monoxide, oxygen, temperature, and pyrogenic infrared detection modules. Additionally, a wireless communication module sends vehicle location information to a mobile phone. This IoT-based early warning terminal detects anomalies, activates warnings, and sends location data to the cloud and phone.

Enhancing security in the Internet of Vehicles (IoV) can be effectively achieved using blockchain technology(Shreya et al., 2024). By establishing a trust model for data sharing among connected vehicles, blockchain technology ensures a secure and efficient exchange of information. This proposal outlines the development of a trust model to facilitate secure and reliable data sharing within the IoV ecosystem, leveraging blockchain's inherent security features to protect against unauthorized access and data breaches. The main objective of this system(Harish et al., 2023) is to resolve the security demands of Intelligent Transport

Systems (ITS) and address risk factors without compromising on the functionality of IoT-ITS. In this paper, cognitive science is utilized to design a security framework, enabling real-time data analysis. The proposed secured IoT-ITS framework leverages cognitive science to effectively meet security requirements and mitigate risk factors.

The main objective is to propose(Jin et al., 2022) an improved multiserver-based authentication and key agreement protocol. In this work, Password and smart card used to hide private keys and Formal and informal security proofs provided. In this paper, (Tu, S et al., 2023), proposed the Vehicle-Based Secure Blockchain Consensus (VBSBC) algorithm to enhance secure communication between vehicles and improve the efficiency of data storage, processing, and sharing in the Internet of Vehicles (IoV). The VBSBC algorithm is employed to bolster authentication processes, key distribution, and request handling during vehicle movement. The major goals include enhancing IoV security through the VBSBC algorithm using blockchain technology, which improves authentication, key processing, attack detection, and overall system reliability.

Amel Meddeb Makhlouf et al., 2019 proposed a protocol called secure and efficient DSR routing protocol. The main aim is to eliminate the malicious vehicles over DSR routing protocol. The security could be achieved by applying hash function and certificates while sending RREQ and RREP packets. Similarly, Sultana, J et al., 2017 proposed secure DSR routing protocol for mobile ad hoc networks. IshaDhyani et al., 2017 proposed a reliable tactic trust model to eliminate black hole attack over DSR routing protocol. The work makes use of vehicle's data forwarding behaviour and dropping behaviour as metrics to evaluate the trustworthiness by the they eliminated the black hole attack.Badreddine Cherkaoui et al., 2017 proposed a cluster-based security mechanism to detect black hole attack. This method makes use of packet forwarding behaviour of vehicles to calculate the trustworthiness.

5.1 Research Gap

From the literature we observed that most of the techniques that is implemented for ensuring IoVT security is based on cryptographic techniques and other complex algorithms. Typically, IoVT environment is highly dynamic and it always posses real time information and that information are minimum. To process such information on demand, applying complex algorithms will be costly and leads to overhead in terms of its processing time, memory and computational. Therefore, an alternate solution is needed to assess the real time information. Trust and reputation-based security model will be the promising solution. Hence, in this work we are focusing on trust and reputation-based security model.

6. Proposed work:

Trusted and Reputation based DSR routing protocol for IoT based Intelligence Transport System

The following section discusses the proposed trust and reputation based DSR routing protocol. Initially, it starts with some preliminaries and initial deployment of IoVT environment.

6.1 Initial condition and assumptions

The IoVT environment consists of autonomous vehicles equipped with processing, communication, and storage capabilities. In addition, each vehicle is equipped with an agent. As previously discussed, an agent is a computing system that interacts with other agents in the IoVT environment. Every vehicle has two types of agents: the Vehicle Trust Evaluating (VTE) agent and the Routing Agent (RA). The VTE agent is responsible for calculating the trust value of communicating devices and ensuring the authenticated dissemination of data by identifying and eliminating black hole attacks. The RA agent is responsible for establishing a trusted route from the source to the destination. Initially, the trust values of all vehicles are set to 1.

The overall trust value ranges from 0 to 1, where 0 represents the minimum trust and 1 represents the maximum trust. Each vehicle can communicate with other vehicles to share information related to environmental conditions while dynamically roaming. Additionally, there are two fixed infrastructures: one is the Road Side Unit (RSU), which facilitates communication with other vehicles and RSUs, and the other is the base station, which enables communication technologies like 4G, 5G, WiFi, Zigbee, WiMax, and others via the internet. Initially, all vehicles or nodes are considered trustworthy. However, due to the open and dynamic nature of the network, vehicles may begin to exhibit malicious behaviors over time, such as dropping essential information, flooding the network with dummy packets, or spreading false or misleading information. In this research, we focus on black hole attacks, where a vehicle simply discards or drops incoming packets. As part of our approach, we designate some vehicles as black hole vehicles. Centralized authorities, such as Road Side Units, also store information about vehicles, tracking their movements from home to work or from home to malls, within the same city or neighborhood, at the same time of day.

Each vehicle in the IoVT maintains a routing table that stores all trust-related information. The structure of the routing table is shown in Table 1.

Table1. Routing table

D	Seq.no	AHC	RL	AT

D-Destination, Seq.no- Sequence number, AHC- Advertised Next Hop, RL – Routing List, AT- Aggregated Trust

The proposed trust and reputation model can piggyback with DSR routing protocol.

6.2 The proposed model: Trusted and Reputed DSR

As mentioned earlier, all vehicles are considered trustworthy at the time of initial network deployment. However, due to the open, shared, and dynamic nature of the IoVT environment, each vehicle must assess the trustworthiness of other participating vehicles over time.

The proposed trust model is consisting of the following key responsibilities:

1. Aggregated Trust Calculation by the Vehicle Trust Evaluation (VTE) Agent: The VTE agent is responsible for calculating the aggregated trust value of each vehicle in the

network. This calculation is based on the behavior and interactions of the vehicles, allowing the system to continuously evaluate and update trust levels to ensure reliable communication.

2. Ensuring Authentication by Identifying Black Hole Vehicles: The trust model also focuses on ensuring authentication by detecting and eliminating malicious black hole vehicles. These vehicles, which drop or discard incoming packets, are identified based on their trustworthiness, preventing them from negatively impacting the network's performance and security.

3. Trusted Route Formation by the Routing Agent (RA): The RA agent is tasked with forming trusted routes between source and destination vehicles. By relying on the trust values calculated by the VTE agent, the RA ensures that only reliable and secure routes are used for communication, further enhancing the security and efficiency of the IoVT environment.

6.2.1 Aggregated Trust Evaluation

The IoVT environment consists of N vehicles (V1, V2, V3, … VN) and Road Side Units (RSU1, RSU2, RSU3, … RSUR). When a vehicle, Vi, receives an alarm or any traffic-related, accident-related, or temperature-related messages from another vehicle, Vj, it first assesses the correctness and validity of the received messages. This is done by calculating the aggregated trust of the sending vehicle, which is managed by the Vehicle Trust Evaluation (VTE) agent. The aggregated trust is determined based on two factors: direct trust and reputation trust.

Direct trust is calculated using two components: previous interactions and situational awareness trust. The previous interactions are based on the number of successful data and control packet deliveries between the vehicles. Malicious vehicles, however, tend to focus less on data packets and more on control packets, such as Route Reply (RPLY) and Route Error (RERR) messages, to attract attention. These malicious vehicles claim to have the shortest route to the destination when they receive Route Request (RREQ) packets or detect link breakages during transmission. Once they gain the attention of other vehicles, they redirect data packets to themselves, receiving and discarding them.

To calculate the direct trust of vehicle Vj in relation to vehicle Vi, the model considers both previous interactions and situational awareness trust. Situational awareness trust is becoming increasingly important in the automotive industry and is defined as the ability to perceive, comprehend, and project information to enable informed decision-making in a dynamic environment. This type of trust helps drivers better understand their surroundings and predict potential changes in the environment, allowing them to respond more effectively (Miller et al., 2014). Given its importance, situational awareness trust is also considered in the calculation of direct trust. The following equation 1 is used to compute the direct trust of vehicle Vj in relation to vehicle Vi over a period of time, t.

$$D_{vivj}(t) = \sum_{t=1}^{N} (\alpha_i P_{vivj} + \alpha_i S_{vivj}) \qquad (1)$$

Where $i, j, t = 1,2,3 \ldots N, i \neq j, \sum \alpha_i = 1$ and D_{vivj}represents the direct trust value of vehicle

vj with respect to vehicle vi over time period t, P_{vivj} denotes the previous interactions with vehicle vj with respect to vehicle vi over time t and S_{vivj} denotes the situational awareness of the vehicle vj with respect to vehicle vi.

The situational awareness trust of vehicle Vj with respect to vehicle Vi is calculated using the following equation. This trust value is determined by assessing whether the vehicle (or driver) is responding based on an understanding of the surrounding environment and its ability to predict future events. If the vehicle is genuine, it will respond to others' queries without expecting any benefit, contributing positively to the network's operation. On the other hand, a malicious vehicle will not respond to queries and will primarily aim to disrupt normal routing operations. Based on this distinction, situational awareness trust is calculated using the equation 2 below.

$$\begin{gathered} \text{if respond of Vj}, \leq \text{ threshold time t1}, S_{vivj} = 1.0 \\ \text{if respond of Vj}, \geq \text{ the threshold time t2}, S_{vivj} = 0.0 \qquad (2) \\ \text{otherwise}, S_{vivj} = 0.5 \end{gathered}$$

Next, the vehicle will calculate the previous interaction based on the data and control packets. The following equation 3 depicts the data packet forwarding ratio (DPF_{vivj}) of vehicle vj with respect to vehicle vi.

$$DPF_{vivj} = \sum_{t=1}^{N} \left(\frac{NDPF_{vivj}}{NDPR_{vivj}} X100 \right) \qquad (3)$$

Where $i, j, t = 1,2,3 \ldots N, i \neq j$, $NDPF_{vivj}$ denotes number of data packets forwarded by vehicle vj with respect to vehicle vi and $NDPR_{vivj}$ denotes actual number of data packets received by vehicle vj. From the equation 3 based on the percentage of data packet forwarding ratio, a trust value will be assigned based on the below equation (4).

$$\begin{gathered} if\ DPF_{vivj} \leq threshold\ value\ Th1, DPF_{vivj}T = 0.0 \\ if\ DPF_{vivj} \geq threshold\ value\ Th2, DPF_{vivj}T = 1.0 \qquad (4) \\ Otherwise, DPF_{vivj}T = 0.5 \end{gathered}$$

From the above equation (Equation 4), the data forwarding ratio trust of vehicle Vj with respect to vehicle Vi is calculated. As previously mentioned, black hole nodes typically do not focus on forwarding data packets, so we assign maximum trust to nodes that forward data packets and assign null trust to those that do not forward packets. Black hole nodes fall under the category of nodes with null trust. For vehicles that intermittently fail to forward packets, we assign a moderate trust value of 0.5. This partial trust is assigned because, in the dynamic nature of the IOVT environment, legitimate vehicles can occasionally turn into black hole vehicles due to various factors.

The following equation (Equation 3) illustrates the control packet forwarding ratio of vehicle Vj with respect to vehicle Vi. In the DSR routing protocol, four types of control packets are used: RREQ, RPLY, RERR, and SALVAGE. While the likelihood of a black hole vehicle using an RREQ packet is low and thus not the primary focus, we concentrate on the other three packets: RPLY, RERR, and SALVAGE. The reason for this is that black hole vehicles often use these control packets to attract attention from neighboring nodes, especially during the route discovery and route maintenance phases. Therefore, the equation below is used to calculate the control packet forwarding ratio of vehicle Vj with respect to vehicle Vi.

$$CPF_{vivj} = \sum_{t=1}^{N} \left(\frac{NRPLYF_{vivj}}{NRPLYR_{vivj}} + \frac{NRERRF_{vivj}}{NRERRR_{vivj}} + \frac{NSALF_{vivj}}{NSALR_{vivj}} \right) X\ 100 \qquad (5)$$

Where $i, j, t = 1,2,3 \ldots N, i \neq j$, $CDPF_{vivj}$ denotes number of control packets forwarded by vehicle vj with respect to vehicle vi. $NRPLYF_{vivj}$ denotes number of route reply packets forwarded, $NRPLYR_{vivj}$ denotes number of route reply packets received, $NRERRF_{vivj}$ denotes number of route error packets forwarded, $NRERRR_{vivj}$ denotes number of route error packets received, $NSALF_{vivj}$ denotes number of salvage packets forwarded, $NSALR_{vivj}$ denotes number of salvage packets received.

From the equation 5, based on the percentage of control packet forwarding ratio, a trust value will be assigned based on the below equation (6).

$$\begin{aligned} if\ CPF_{vivj} \leq\ threshold\ value\ Th1, CPF_{vivj}T &= 1.0 \\ if\ CPF_{vivj} \geq\ threshold\ value\ Th2, CPF_{vivj}T &= 0.0 \\ Otherwise, CPF_{vivj}T &= 0.5 \end{aligned} \qquad (6)$$

From the above equation, the control forwarding ratio trust of vehicle Vj with respect to vehicle Vi is calculated. As previously mentioned, black hole nodes tend to focus on control packets rather than data packets. Therefore, we assign maximum trust to nodes that actively forward control packets, while nodes that do not forward control packets receive null trust. Additionally, we assign a moderate trust value of 0.5 to vehicles that occasionally forward control packets. This partial trust is assigned because legitimate vehicles also use control packets, but the probability of a legitimate vehicle using these packets is relatively low compared to black hole vehicles, which frequently manipulate control packets to disrupt the network.

Based on the equation 4 and equation 6, past interaction is calculated based on the below equation.

$$P_{vivj}(t) = \sum_{t=1}^{N} \left(DPF_{vivj}T + CPF_{vivj}T \right) \qquad (7)$$

By substituting Equation 2 and Equation 7 into Equation 1, the direct trust value is calculated. Next, vehicle Vi will calculate the reputation trust of vehicle Vj. The purpose of calculating this trust is to assess the reputation of vehicles within the IOVT environment over a given period. This trust is determined based on three factors: direct trust, recommendations from other vehicles, and recommendations from road side units (RSUs). The first factor is direct trust, which is the trust that vehicle Vi places in vehicle Vj based on its own observations and interactions. For example, the direct trust value that vehicle Vi has for vehicle Vj is calculated based on their previous interactions. The second factor is the recommendation from other vehicles, such as vehicle Vk, which provides insight into the trustworthiness of vehicle Vj from its perspective. This recommendation is based on the past interactions and experiences between vehicle Vj and vehicle Vk. The third factor is the recommendation from RSU, such as RSUi, which adds another layer of trust by considering data from a more centralized and stable infrastructure.

The following equation (Equation 8) is used to calculate the reputation trust of vehicle Vj with respect to vehicle Vi over time, considering these three factors.

$$Rep_{vivj}(t) = \alpha_i D_{vivj}(t) + \sum_{t=1}^{NR} \alpha_i \; D_{vivk}(t) + \; \alpha_i D_{RSUivj}(t) \quad (8)$$

Where, $i, j, t, k = 1,2,3 \ldots N, i \neq j$, $\sum_{i=1}^{i=N} \alpha_i = 1$ and NR represents the number of recommended vehicles in the IOVT environment.

Finally, Vehicle Trust Evaluation (VTE) Agent will calculate the aggregated trust based on the direct trust and reputation trust which is shown in the equation 9.

$$AT_{vivj}(t) = \alpha_1 D_{vivj}(t) + \alpha_2 \, Rep_{vivj}(t) \quad (9)$$

Where $\alpha_1 + \alpha_2 = 1$

Based on the aggregated trust value, vehicle vi will make decision whether to accept the data dissemination from vehicle vj.

6.2.2 Ensuring authentication by Identification of Black hole vehicles

The decision will be taken based on the aggregated trust value. The following algorithm is used to make a decision about vehicle vj.

Algorithmic Description

Algorithm: Identifying Black Hole Vehicles Based on Aggregated Trust (AT)

Input: Aggregated Trust (AT) for each vehicle

Output: Identification of Black Hole vehicles and updating the trust table

Begin

// Step 1: Check if Aggregated Trust (AT) is calculated for all vehicles

if (Aggregated Trust is calculated) then

// Step 2: Evaluate the trust of each vehicle (vj) from the perspective of vehicle (vi)

```
for each Vehicle vi evaluates every other vehicle vj do
        // Step 3: Read the Aggregated Trust (AT) value for vehicle vj
    Read AT

    // Step 4: Check if the Aggregated Trust (AT) is less than or equal to threshold value
    if AT <= Threshold_value then

        // Step 5: Mark vehicle as untrusted or black hole, and notify neighbouring vehicles
        // Broadcast the information about black hole vehicle to the neighbouring vehicles
        Broadcast information about Black Hole vehicle to Neighbouring Vehicles

        // Step 6: Remove the vehicle entry (vj) from the trust table
        Delete entry of vj from AT table
            else
                // Step 7: Vehicle is trusted, allow it to participate in the routing process
        Allow vehicle vj in the routing process

    end if
  end for
 end if
End
```

By the way authentication in data dissemination is achieved in IOVT environment.

6.2.3 Trusted Route Formation by the Routing Agent (RA)

Trusted route establishment only involved with trusted vehicles. Routing Agent (RA) takes responsible for forming trusted route. It consists of the following phases,

- Route discovery
- Route Maintenance

Route Discovery

Typically in standard DSR, route discovery process is accomplished by Route Request (RREQ) and Route Reply (RPLY) packets. The proposed TR-DSR take this advantage and append its evaluated AT value with original RREQ packets of standard DSR the result is

Trusted RREQ packet. The TRREQ packet format of TR-DSR is given below.

Table.2 Trusted Route Request (RREQ) packet of TR-DSR

4 Bytes	4 Bytes	2 Bytes	2 Bytes
Sour_Add	Dest_add	V_id	AT

In the above table Sour_Addr denotes the source address, Dest_Add denotes the destination address, V_id denotes the Vehicle identity and AT denotes the aggregated trust.

Algorithm of Route Discovery process

The following table illustrates the route discovery process of proposed TR-DSR.

Algorithm 5.3: Trusted Route Formation

Input: Authenticated vehicles and Aggregated Trust (AT) of each vehicle

Output: Trusted Route from source to destination

Begin

// Step 1: When the route discovery process starts

if (source vehicle) then

// Step 2: Check if a trusted route is available in the source vehicle's route cache

Check source's route cache

// Step 3: If a trusted route from source to destination is available

if (trusted route available) then

// Step 4: Forward the data packets to destination

Forward data packets

else

// Step 5: Create RREQ packet (Sour_Addr, Dest_Addr, U_id, AT)

Create RREQ packet with Source Address, Destination Address, Unique ID, and Aggregated Trust

// Step 6: Broadcast RREQ packets to neighboring vehicles and set a timer for reply

Broadcast RREQ to neighboring vehicles

Set timer to wait for a reply

```
    end if

  end if

  // Step 7: If intermediate vehicles receive RREQ
  if (intermediate vehicle) then
    // Step 8: Receive RREQ packet
    Receive RREQ

    // Step 9: If already received this RREQ
    if (RREQ already received) then
      // Step 10: Drop the RREQ packet
      Drop RREQ

    else
      // Step 11: Calculate Cumulative Aggregated Trust (CAT) value
      // Add the source vehicle's AT with the current vehicle's AT and update in Decision Table (DT)
      Calculate CAT = Source_vehicle_AT + Current_vehicle_AT
      Update Decision Table (DT) with the new CAT value

      // Step 12: Repeat the process (go back to Step 8)
      Go to Step 8

    end if
  end if

  // Step 13: If destination vehicle receives RREQ
  if (destination vehicle) then
```

```
// Step 14: If the destination vehicle receives the first RREQ packet
if (first RREQ received) then

    // Step 15: Calculate the Cumulative Aggregated Trust (CAT) value
    // Add the source vehicle's DT with the current vehicle's DT
    Calculate CAT = Source_vehicle_DT + Current_vehicle_DT

    // Step 16: Check if CAT > threshold
    if (CAT > threshold) then

        // Step 17: Create RPLY packet
        Create RPLY packet

        // Step 18: Unicast RPLY packet to the source vehicle via intermediate vehicles
        Unicast RPLY to source vehicle via intermediate vehicles

        // Step 19: Add the route along with the CAT value to the destination vehicle's route cache
        Add route and CAT to route cache

        // Step 20: Forward the RPLY packet
        Forward RPLY

        // Step 21: Repeat the process until reaching the source vehicle
        Go to Step 28

    end if
  end if
end if

// Step 22: If source vehicle receives RPLY
```

```
if (source vehicle) then

    // Step 23: Check RPLY
    if (CAT > threshold) then
        // Step 24: Forward the data packets to the destination
        Forward data packets
    else
        // Step 25: Discard the packet
        Discard data packet
    end if
end if

End
```

6.2.4 Route Maintenance

Due to the mobility of vehicles, link failure occurs often it will affect the overall performance of the network. It can be overcome by route maintenance process. The proposed TR-DSR follows the route maintenance of standard DSR.

7. Results and Discussion

The proposed model is implemented in NS3, and the following simulation parameters are used in this work. The model is compared with the approach by Balaji et al. (2020) and the traditional DSR routing protocol. All experiments are conducted in the presence of black hole nodes. A total of 100 vehicles/mobile nodes are used in the simulation, with the percentage of black hole nodes increasing randomly.

Table 3. Simulation Parameters

Simulation Parameters	
Simulator	NS3
Duration	1000sec
Routing Protocols	DSR, Proposed Protocol, Bhalaji et al., 2020
Number of vehicles	100
Number of blackhole nodes	10%, 20%.....80%
Traffic type	Constant Bit Rate (CBR)
Propagation model	Nakagami Model
Mobility model	Random Waypoint
MAC type	802.11
Mode of channel	Wireless
Data payload	512 bytes/packet
Simulation area	1000mx1000m
Nodes' speed	5-10-15-20-25 (m/s)
Data rate	10.4Mbps

Threshold th1	0.4
Threshold th2	0.7
Threshold time tt1	10S
Threshold time tt2	5S

The following experiments have done and the results are discussed below,

1. Detection ratio of blackhole nodes
2. Packet loss ratio
3. Packet delivery ratio
4. End to end delay

7.1 Detection Ratio.

The detection ratio of black hole nodes is defined as the proportion of black hole nodes detected from the total number of nodes. In this experiment, the detection ratio of black hole nodes is analyzed. The simulation runs over a specified time interval, with black hole nodes randomly selected from the overall nodes. The final trust level is calculated based on Equation 8. Since the proposed trust model is integrated with the DSR routing protocol, we first compare the results with DSR and then with the approach by Balaji et al. (2020). From the results, we observe that the detection ratio of the proposed trust model is higher compared to the other two models. This is because the proposed model evaluates aggregated trust using various metrics such as previous interactions, situational awareness trust, and reputation trust. As a result, the model invests significant effort into evaluating trustworthiness, leading to a higher detection ratio. In contrast, the DSR protocol lacks an inherent detection mechanism, resulting in a lower detection ratio. Furthermore, the lower detection accuracy observed in the model proposed by Balaji et al. (2020) can be attributed to its less robust trust evaluation mechanism. The weaker trust assessment methodology in their model results in suboptimal detection capabilities, leading to reduced accuracy in identifying black hole nodes.

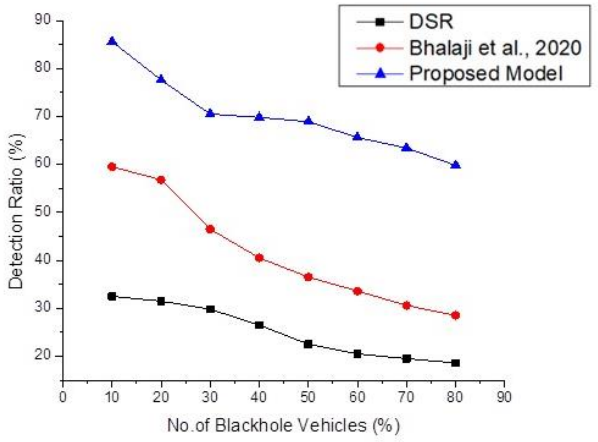

Fig. 7 Detection Ratio Vs Blackhole Nodes

7.2 Packet loss ratio

It is defined as number of packets not delivered to destination node which is sent by the source node over the period of time. The packet loss ratio is low in the proposed trust model due to the comprehensive and robust trust evaluation mechanism integrated with the DSR routing protocol. This mechanism, which incorporates metrics such as previous interactions, situational awareness trust, and reputation trust, ensures that only authenticated and reliable vehicles are included in the routing process. By accurately identifying and excluding black hole nodes, which often drop or maliciously alter packets, the trust model significantly reduces the chances of packet loss.In contrast, the traditional DSR protocol lacks an inherent detection mechanism for malicious nodes, such as black hole nodes. As a result, malicious vehicles that discard or misdirect packets are not effectively filtered out, leading to a higher packet loss ratio. Similarly, the model proposed by Balaji et al. (2020) also exhibits a higher packet loss ratio due to its weaker trust evaluation mechanism, which is less effective in identifying and mitigating malicious behavior in the network.By ensuring that only trustworthy nodes are used for routing, the proposed trust model minimizes the chances of data being dropped or misdirected, ultimately resulting in a lower packet loss ratio compared to the DSR and Balaji et al. models. This enhanced trust evaluation process directly contributes to improved overall network performance, reliability, and robustness.

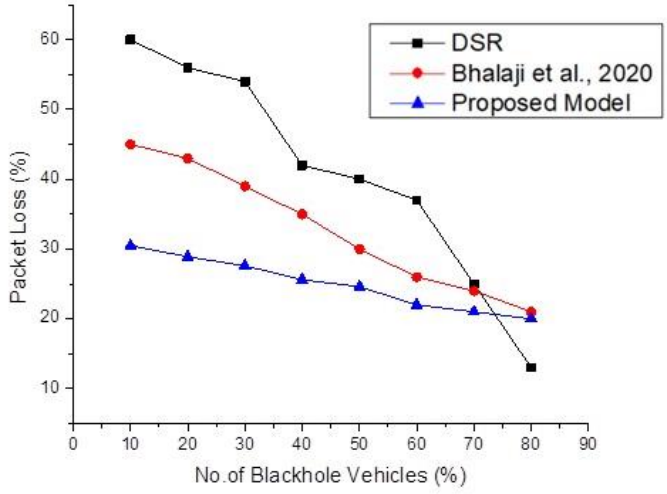

Fig 8. Packet Loss Ratio Vs. Blackhole Nodes

7.3 Packet delivery ratio

Packet delivery ratio is defined by the percentage of delivered data to the destination node from the source node over the period of time. The packet delivery ratio is high in the proposed trust model due to the effective filtering of malicious or untrustworthy nodes, which ensures that only reliable vehicles participate in the data forwarding process. In this model, the trustworthiness of vehicles is evaluated through a combination of metrics, including previous interactions, situational awareness trust, and reputation trust. By

calculating an aggregated trust value for each vehicle and excluding those with low trust (such as black hole nodes), the model ensures that only vehicles with a verified history of proper behavior are involved in the packet forwarding process. In comparison, the traditional DSR protocol does not have any built-in mechanism to assess node trustworthiness, making it vulnerable to black hole nodes that may discard or misdirect packets. As a result, this leads to a lower packet delivery ratio in DSR, as packets may be lost or misrouted by malicious nodes. Similarly, the model proposed by Balaji et al. (2020) also suffers from a lower packet delivery ratio because its trust evaluation methodology is less robust, leading to insufficient identification of malicious nodes. By incorporating a more rigorous and dynamic trust evaluation approach, the proposed model minimizes the likelihood of malicious nodes affecting the routing process, thereby ensuring that more packets are successfully delivered to their intended destinations. This is why the packet delivery ratio is higher in the proposed model, as it effectively reduces packet loss by ensuring that only trustworthy nodes participate in the routing and forwarding process.

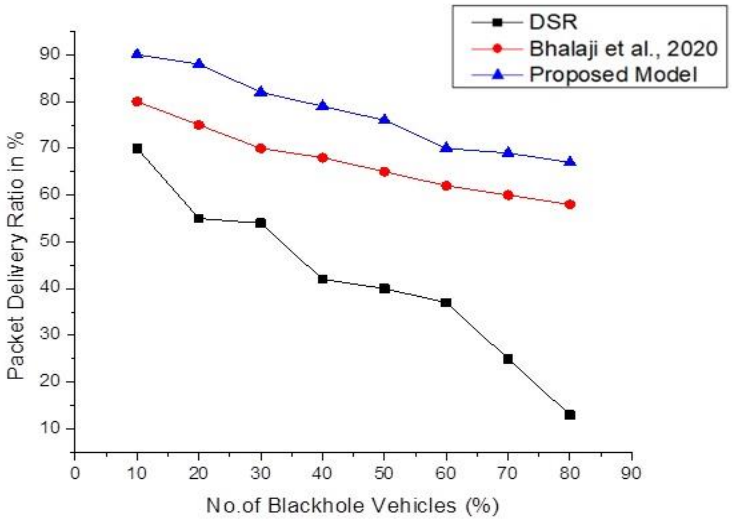

Fig 9.Packet delivery ratio Vs. Blackhole Nodes

7.4 End to end delay

The low end-to-end delay in the proposed trust model is a result of several key factors. First, the efficient detection of malicious nodes through aggregated trust evaluation allows for the early identification and exclusion of black hole nodes, preventing delays caused by these malicious vehicles. In contrast, traditional DSR and the model by Balaji et al. (2020) lack effective detection mechanisms, leading to delays in route maintenance and retransmissions. Additionally, the proposed model's optimized route selection, based on trustworthiness factors like previous interactions and situational awareness, enables the source vehicle to choose only reliable vehicles, avoiding delays caused by route failures. The model also reduces the impact of route discovery and maintenance, as fewer trusted vehicles need to be involved in recalculating routes, minimizing the need for retransmissions and

route error packets. Moreover, by excluding black hole nodes early, the model ensures fewer data packet losses, which directly contributes to reduced end-to-end delay. Lastly, the model guarantees more stable and reliable routing paths by using only trusted nodes, reducing the frequency of route changes and ensuring faster packet delivery. In contrast, traditional protocols are more prone to delays due to unstable or malicious nodes.

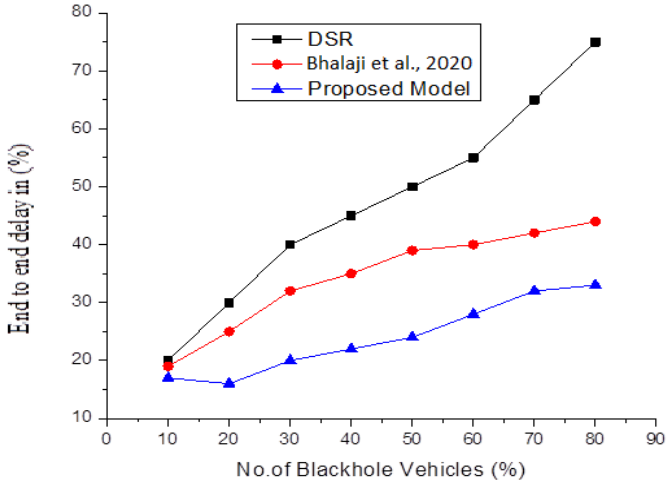

Fig 10. End to end delay Vs. Black hole nodes

8. Conclusion

Modern transportation systems are increasingly incorporating advanced technologies, and the Internet of Vehicles (IoVT) is one such innovation that aims to enhance driver comfort and safety. IoVT has garnered significant attention due to its remarkable features, and it is now being adopted by vehicle manufacturers worldwide. However, the lack of robust security mechanisms inherent in IoVT, coupled with its unique characteristics, makes it vulnerable to various security threats. One such threat is the black hole attack, which poses a significant challenge in IoVT environments. This article explores the detection and isolation of black hole attacks within the context of the DSR routing protocol. The proposed trust model is integrated with the DSR protocol, using aggregated trust to identify and eliminate black hole nodes from the network. The aggregated trust of a vehicle is determined by both direct trust and reputation trust. With this trust model, a secure and reliable route is formed, ensuring that only trusted vehicles are involved in communication. Since the trust evaluation process does not rely on complex algorithms, it is well-suited for lightweight IoT devices. Ultimately, by detecting and eliminating black hole attacks, secure data dissemination is achieved, and vehicle authentication within the IoVT environment is ensured. Future research will focus on applying this model to other routing protocols within IoVT.

References

1. Amel Meddeb Makhlouf and Mohsen Guizani (2019) , SE-DSR: secure and efficient DSR routing protocol for vehicular communications, International Journal of Information Security.
2. Badreddine Cherkaoui, Abderrahim Beni-hssane and Mohammed Erritali (2017), A Clustering Algorithm for Detecting and Handling Black Hole Attack in Vehicular Ad Hoc Networks. Advances in Intelligent, Systems and Computing, 481-491.
3. Balaji, P. G., & Srinivasan, D. (2010). An introduction to multi-agent systems. Innovations in multi-agent systems and applications-1, 1-27.
4. Batra, N., & Goyal, S. (2024). Security aspects in IoT. 251–265. https://doi.org/10.1201/9781003307488-7
5. Bhalaji, N., K. S. Hariharasudan, and K. Aashika (2020), "A trust based mechanism to combat blackhole attack in RPL protocol." ICICCT 2019–System Reliability, Quality Control, Safety, Maintenance and Management: Applications to Electrical, Electronics and Computer Science and Engineering. Springer Singapore, 2020.
6. Blas, H. S. S., Mendes, A. S., Encinas, F. G., Silva, L. A., & González, G. V. (2020). A multi-agent system for data fusion techniques applied to the internet of things enabling physical rehabilitation monitoring. Applied Sciences, 11(1), 331.
7. Chavhan, S., Gupta, D., Gochhayat, S. P., N, C. B., Khanna, A., Shankar, K., & Rodrigues, J. J. (2022). Edge computing ai-iot integrated energy-efficient intelligent transportation system for smart cities. ACM Transactions on Internet Technology, 22(4), 1-18.
8. Chen, R., & Muthu, B. (2022). Internet of vehicle things communication based on big data analytics integrated internet of things. International Journal of Internet Protocol Technology, 15(3/4), 203–213. https://doi.org/10.1504/ijipt.2022.10051096
9. Dorri, A., Kanhere, S. S., & Jurdak, R. (2018). Multi-agent systems: A survey. Ieee Access, 6, 28573-28593.
10. Hang, Peng., Qin, Wang., Xuebin, Zhang. (2023). A Vehicle Security Early Warning Terminal Based on Internet of Things. doi: 10.1145/3641343.3641363
11. Harish, Karthikeyan., G, Usha. (2023). A secured IoT-based intelligent transport system (IoT-ITS) framework based on cognitive science. Soft Computing, doi: 10.1007/s00500-023-08410-7
12. Isha Dhyani, I., Goel, N., Sharma, G., Mallick, B (2017) A Reliable Tacticfor Detecting Black Hole Attack in Vehicular Ad Hoc Networks,Advances in Computer and Computational Sciences, pp. 333–343.
13. Jawad, S., Munsif, H., Azam, A., Ilahi, A. H., & Zafar, S. (2021). Internet of Things-based Vehicle Tracking and Monitoring System. https://doi.org/10.1109/icosst53930.2021.9683883
14. Jin, Wang., Libing, Wu., Huaqun, Wang., Kim-Kwang, Raymond, Choo., Lianhai, Wang., Debiao, He. (2022). A Secure and Efficient Multiserver Authentication and Key Agreement Protocol for Internet of Vehicles. IEEE Internet of Things Journal, doi: 10.1109/JIOT.2022.3188731
15. Johnson, D. B., Maltz, D. A., & Broch, J. (2001). DSR: The dynamic source routing protocol for multi-hop wireless ad hoc networks. Ad hoc networking, 5(1), 139-172.
16. Julian, Vicente, and Vicente Botti. "Multi-agent systems." Applied Sciences 9.7 (2019): 1402.
17. Karim, A. (2022). Development of secure Internet of Vehicle Things (IoVT) for smart transportation system. Computers and Electrical Engineering, 102, 108101.
18. Liu, S. (2022). Communication Security in IoT. Transactions on Computer Systems and Networks, 79–115. https://doi.org/10.1007/978-981-19-1585-7_5
19. Miller, D., Sun, A., and Wendy, J (2014), "Situation Awareness with Dierent Levels of Automation," in Systems, Man and Cybernetics (SMC), IEEE International Conference on, October 2014, 688-693
20. MORAIS, N. B. S. D. (2022). Internet of Things-Based Smart Transportation System for Smart Cities. Advanced Technologies and Societal Change, 39–50. https://doi.org/10.1007/978-981-19-0770-8_4
21. Prakash, Krishna, Shinde., Rajesh, Keshav, Deshmukh., Priya, Pise. (2023). Lightweight Blockchain-based Secuirity Protocol for Internet of Vehicle Things. doi: 10.1109/gcitc60406.2023.10426193
22. Rahman, M. A., Rahim, M. A., Rahman, M. M., Moustafa, N., Razzak, I., Ahmad, T., & Patwary, M. N. (2022). A secure and intelligent framework for vehicle health monitoring exploiting big-data analytics. IEEE Transactions on Intelligent Transportation Systems, 23(10), 19727-19742.
23. Sabri, Y., Siham, A., & Maizate, A. (2021). Internet of things (IoT) based smart vehicle security and safety system. International Journal of Advanced Computer Science and Applications, 12(4).
24. Sadhu, P. K., Yanambaka, V. P., & Abdelgawad, A. (2022). Internet of things: Security and solutions

survey. Sensors, 22(19), 7433.
25. Shah, Z., Levula, A., Khurshid, K., Ahmed, J., Ullah, I., & Singh, S. (2021). Routing protocols for mobile Internet of things (IoT): A survey on challenges and solutions. Electronics, 10(19), 2320.
26. Shon, T. (2021). In-vehicle Networking/Autonomous vehicle security for internet of Things/Vehicles. Electronics, 10(6), 637.
27. Shreya, Yadav., Karan, Singh., Sergey, Bezzateev. (2024). Enhancing Security using Trusted Blockchain Method for Internet of Vehicle. doi: 10.1109/autocom60220.2024.10486132
28. Sultana, J., and Ahmed, T. (2017) Securing DSR protocol in mobileadhoc network with elliptic curve cryptography. In: InternationalConference on Electrical, Computer and Communication Engineering(ECCE), pp. 539–543,systems, IEEE Access, Vol.1, pp.35–50.
29. Taslimasa, H., Dadkhah, S., Neto, E. C. P., Xiong, P., Ray, S., & Ghorbani, A. A. (2023). Security issues in Internet of Vehicles (IoV): A comprehensive survey. Internet of Things, 22, 100809.
30. Tu, S., Yu, H., Badshah, A., Waqas, M., Halim, Z., & Ahmad, I. (2023). Secure Internet of Vehicles (IoV) with decentralized consensus blockchain mechanism. IEEE Transactions on Vehicular Technology, 72(9), 11227-11236.
31. Uhrmacher, A. M., & Weyns, D. (Eds.). (2018). Multi-Agent systems: Simulation and applications. CRC press.
32. Van der Hoek, W., & Wooldridge, M. (2008). Multi-agent systems. Foundations of Artificial Intelligence, 3, 887-928.
33. Wang, X., & Ding, T. (2016, April 20). Intelligent public transport system.
34. Yang, D.-K., Wu, J., & Zhang, Q. (2000). Intelligent transport system and its informatics model. Journal of Beijing University of Aeronautics and Astronautics, 26(3), 270. https://bhxb.buaa.edu.cn/EN/abstract/abstract11312.shtml
35. Yu, H., Shen, Z., Leung, C., Miao, C., & Lesser, V. R. (2013). A survey of multi-agent trust management systems. IEEE Access, 1, 35-50.
36. Zear, A., Singh, P. K., & Singh, Y. (2016). Intelligent Transport System: A Progressive Review. Indian Journal of Science and Technology, 9(32), 1–8. https://doi.org/10.17485/IJST/2016/V9I32/100713