Journal of Intelligent Systems and Internet of Things
Vol. 16, No. 01, PP. 102-117, 2025
DOI: https://doi.org/10.54216/JISIoT.160109

Multi-Dimensional Trust based Data Dissemination mechanism (MDTD) for Ensuring Authentication by Eliminating Blackhole Attack in VANET

C. Balakumar[1,*], S. Vydehi[2]

[1]Research Scholar, Department of Computer Science, Dr.SNS Rajalakshmi College of Arts and Science (Autonomous), Coimbatore, India

[2]Associate Professor & Head, Department of Information Technology, Dr.SNS Rajalakshmi College of Arts and Science (Autonomous), Coimbatore, India

Emails: balakumarc.cbk@gmail.com; vydehi.s@gamil.com

Abstract

Vehicular Ad Hoc Networks also known as VANET, and it is a special type of ad hoc networks since it is deployed on demand. Here the nodes are representing as vehicles, and they are communicating with each other to ensure the reliable and secure safety driving. Since it is open environment, ensuring secure routing is always a challenging task. Routing is one of the essential things in ad hoc networks because it is carrying road safety information always. However, most of the time, it is affected by attacks. Black hole is one of the attacks where the malicious nodes that is black hole vehicles advertise itself that having the shortest path to the destination by the way it tries to disturb the entire environment. In this paper, multi-dimensional trust-based data dissemination mechanism is proposed. The main objective is to ensure authentication by eliminating black hole attack. The proposed method makes use of multiple trusts such as direct, indirect, integrity, intimacy, and mobility over Dynamic Source Routing (DSR) protocol by the way authentication can be achieved. Simulation results shows that the proposed model works efficiently compare with existing models.

Received: November 25, 2024 Revised: January 02, 2025 Accepted: January 29, 2025

Keywords: Vehicular Ad Hoc Networks; Security; Routing, Trust; Data Dissemination; Authentication; Dynamic Source Routing

1. Introduction

Vehicular ad hoc networks are the special type of Mobile Ad hoc Networks where the nodes are represented as Vehicles. The aim of the VANET is to providing communicating between nearby vehicles as well as roadside units [1-2] to share traffic and safety related information. Hence, it leads to Intelligence Transport System (ITS). The communication in VANET always carried between vehicle to vehicle that is V2V or between roadside infrastructure-based units and vehicles, which is V2I. Every vehicle in the VANET is equipped with an On-Board Unit (OBU), which is capable of doing computing and communication. The distinct nature of VANET leads to various applications such are navigational support, dissemination of safety related information, infotainment, gaming, warning, comfort, music sharing, maintenance, financial related support such as process for fuel, parking, tolls and etc. Vehicular Ad Hoc Networks (VANETs) are a specialized form of Mobile Ad Hoc Networks (MANETs) that enable communication between vehicles and roadside infrastructure. VANETs have gained significant attention due to their potential to enhance road safety, traffic efficiency, and provide various intelligent transportation system (ITS) applications. However, ensuring the security and privacy of the communication within VANETs is crucial to their successful deployment [1].The following figure 1 shown the general architecture of VANET.

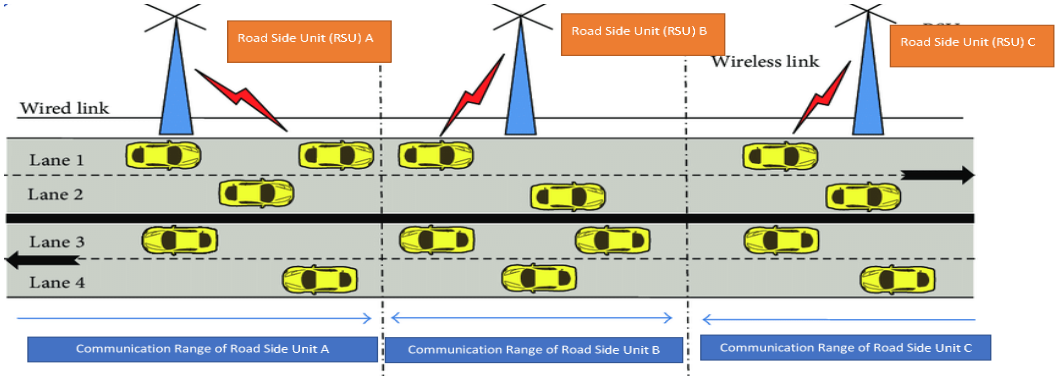

Figure 1. The Architecture of VANET.

The distinct nature of VANET offers various applications at the same time it leads to various research challenges such as standards, routing protocols, fundamental limits and opportunities, connectivity, cross layer, cooperative communication, mobility, Validation, and security privacy [4]. Vehicular Ad Hoc Networks (VANETs) have gained significant attention in recent years, but several research challenges persist that need to be addressed for the widespread deployment and adoption of scalable, reliable, robust, and secure VANET architectures, protocols, technologies, and services [5]. Among the challenges security and privacy is one of the considerable issues. In general, success of any application depends how it is secured from adversaries hence securing VANET environment is also becoming a challenging task because of its unique nature mainly the open, distributed, and dynamic environment. The security of VANET can be achieved once the following security requirements to be addressed such as integrity, authentication, confidentiality, non-repudiation, availability, authentication, real time constraint and real time protection [6]. Among the requirements authentication is important because it is providing initial level of security. Once the authentication is ensured, rest of the security requirements can be achieved easily. This paper is mainly focusing on authentication in message dissemination that is every vehicle should ensure the authentication that means ensure the identity before it is going to disseminating message to other vehicle.

Security of VANET threated by various attacks. In VANET, the attacks can be classified into two category such as insider attack and outsider attack. As the name implies, the insider attack can be launched within the network. These types of attacks are also known as active attack. Whereas outside attack also known passive attack, can be launched from outside of the network. It is hard for an outside attacker to execute an attack however, they can collect driver's information without their knowledge and that can be used in future. [7]. There are so many attackers are there among one of the notable attack is Black hole attack.In this type of attack, an attacker advertise itself that having the shortest path to the destination by the way it is getting attention from outside environment and try to affect the whole environment. The working principle of black hole attack is presented in the following figure2.A Blackhole vehicle is a malicious vehicle that falsely replies for route requests without having an active route to the particular destination and exploits the routing protocol to advertise itself as having shortest path to a destination vehicle [8]. In general, this type attack will execute between vehicle-to-vehicle (V2V). The given figure 2 shows the demonstration of Blackhole attack.

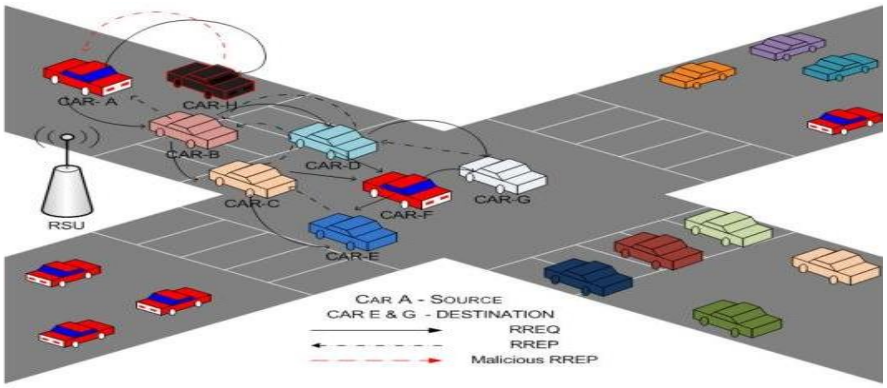

Figure 2. Demonstrate of Black hole attack.

In the above figure Car “A” wants to send data packets to the destination cars namely “E” and “G” so it starts the route discovery process. Therefore, if car “H” is a black hole vehicle then it will claim itself that it has shortest and active routes to the destination by the way it receives RREQ packets. It will then send reply to car “A” before any other nodes. Now, car “A” will think that this is the shortest route and therefore route discovery is complete so that car “A” will neglect all other replies and will start seeding data packets to car “H”. In this way, all the routing related information will be lost consumed or lost.

Motivation of the Research Work

The emergent reliance on VANETs for Intelligent Transportation Systems (ITS) is obvious because of their essential role in optimizing and revolutionizing modern transport system. To promote ITS, VANETs support continuous communication among vehicles that are involving in VANET and the roadside units that might be a physical infrastructure, pedestrians, developing a safer, more efficient transport system. This cumulative requirement is driven by the possible for real-time data exchange, enabling applications such as emergency services, road safety, traffic management and collaborative driving. The addition of VANETs is determined by the quest of cleverer and more approachable transportation solutions, design a noteworthy change near intelligent and interconnected mobility systems. The research commenced by addressing the fundamental question of how to attain secure and efficient data dissemination in VANETs. However, accomplishing this objective proves to be intricate within the context of the uncertain and dynamic environment characteristic of VANETs. Ensuring secure and efficient data dissemination in VANETs is crucial for the success of various services, including collaborative driving, emergency services, traffic management, road safety, and vehicle assistance, such as locating nearby fuel stations and rest areas. Therefore, a timely and reliable exchange of information is essential to guarantee the provision of the services. Consequently, achieving success in Intelligent Transport Systems (ITS) is contingent upon ensuring road safety and enhancing transportation facilities' efficiency.

Outline of the problem

Due to the unpredictable, dynamic topology, and resource-constrained nature of vehicles, various security challenges and issues arise in the data dissemination of VANETs. Verifying the authenticity of information related to road safety and other pertinent details becomes a challenging task in such a dynamic environment. This challenge stems from the fact that every vehicle communicates with others without prior recommendations or considerations. This lack of foresight in communications results in numerous security violations, typically manifesting as attacks that harm the VANET environment and cast doubt on its overall performance. Among these attacks, the Blackhole attack stands out for its high impact on VANET data dissemination compared to other security threats. The repercussions include data loss, disruption of normal communication, compromised safety applications, inefficiencies, traffic congestions, erosion of trust, and adverse effects on emergency services.

To address these issues, various security mechanisms, including cryptographic solutions [1-3], intrusion detection solutions [4-5], key management [6-9], blockchain technologies [10-12], and more, have been proposed by different authors. While these techniques are effective, applying them to resource-constrained vehicles poses challenges. The discussed techniques often demand high computational, storage, and processing capabilities, leading to potential security violations in such constrained environments [13]. In response to these challenges, this proposed work introduces trust management, which does not involve complex algorithms, offering a potential solution to the security issues associated with resource-constrained vehicles [13]. Furthermore, numerous researchers have leveraged trust management for secure data dissemination; however, there is a noticeable absence of comprehensive solutions that guarantee improved performance metrics while ensuring authentication.

Contribution

The research work aims to achieve authentication by identifying and mitigating blackhole attacks through the implementation of trust management, all while taking into account multiple evaluation metrics. The establishment of the trusted route relies on the Decision Trust, which is maintained by the trusted vehicles.

2. Review of Literature

There are numerous amounts of existing work is made with respect to authentication and routing in VANET. Here some of the significant works are presented. Ming Chin Chuang et al., [9] presented a Trust Extended Authentication Mechanism for Vehicular Ad hoc Networks (VANET). The main aim of the work is ensured authentication among the communicating vehicles by using cryptographic techniques along with XOR operations and Hash functions. Felix Gomez Marmaol et al., [10], present a Trust and Reputation infrastructure-based proposal for VANET. The

separate the malicious nodes from the VANET environment by make use of behavioral trust and reputation management.

Dijiang Huang et al., [11], present situation Aware Trust Architecture for Vehicular networks. The main objective of the work is to address several trust related issues that is based on identity based cryptographic to integrate several factors such are entitytrust, data trust, security policy enforcement andsocial network trust. The overall objective is to control the data access by ensuring authentication. Zhang et al., [12] proposed a vehicular authentication protocol called as APPA, which is based on the identity-based cryptography, aggregated signature and one-time signature. The main motivation is to ensure authentication among the communicating vehicles.

Mutual authentication in self-organized VANET is presented by candido Caballero Gil et al., [13]. They make use of cryptographic protocol including a zero-knowledge proof and certification graph. In addition, they also used to secrete key cryptography and public key cryptography to avoid the misbehaving nodes in the VANET environment. Detection of black hole attack is presented by malathi et al., [14] by modify the existing DSR routing protocol. The modification has been done in two ways, one is detection of black hole nodes before forwarding any routing related information and during routing related information is forwarding.

Parul et al., [15] proposed a detection and prevention of black hole attack in VANET. In this proposed method, every source node stores all route replies in their look up table and this tablestores the sequences of all route reply. In order to arrange these replies in ascending order PUSH and POP operations are used. By using the sequence number, priority is calculated and RREP having doubtless very highdestination sequence number. Nodes that are having high sequence number that can be prevented and detected from the network by the way black hole nodes can be deleted from the network. Ajay.N.Udadhaya et al, [17] proposed a prevention of Blackhole in VANET based on two approaches. In first approach, they make use of maximize the sequence number and in the second approach they make use of neighbour awareness count.

Reliable tactical for detection of blackhole is proposed by Isha Dhyaniet al.[16]. The make use of reliable mechanism called trust factor technique is used in order to eliminate the black hole attack. The field of VANETs involves various data dissemination techniques for sharing information in highway and urban environments. These techniques aim to ensure good quality of services, reliable rebroadcast, and message assurance when reaching the destination [18].This work is the modification of AOMDV. Sisily Sibichen et.al describing a hybrid security approach for a network, where RSA key exchange is used for initial secure communication and then symmetric key cryptography is employed for ongoing communication within a neighborhood of nodes [19]. S Majeed et al, discussing the mitigation of blackhole attacks in the context of the Ad-hoc On-Demand Distance Vector (AODV) routing protocol. A blackhole attack is a type of malicious activity where a node in the network selectively drops packets, causing disruption and degradation in communication [20]. Ram Shringar Raw et al, summarizing a Vehicular Ad Hoc Networks (VANETs) with a particular emphasis on safety, Intelligent Transport Systems (ITS), VANET architecture, technical aspects, and security considerations for attacks and its solutions[21].

Karagiannis et al proposed the methods collectively contribute to enhancing the security and reliability of VANETs. Localization is crucial for various applications in VANETs, such as navigation and collision avoidance, and ensuring the accuracy of location information is essential. Meanwhile, detecting Sybil attacks is important for maintaining the integrity of the network by preventing malicious nodes from impersonating multiple identities and disrupting communication. The described metrics and methods contribute to achieving these objectives in a VANET environment [22].

Sangeetha Kannan et al presents the integration of a trust management technique into the AODV routing protocol (TSAODV) enhances the security of VANETs by mitigating specific types of attacks. Trust values play a crucial role in assessing the reliability of nodes and the routing decisions are made in consideration of these trust values, contributing to a more secure and trustworthy network environment [23]. Sathish M et.al, described strategy employs a combination of techniques, including fake RREQ broadcasts, the creation of a black hole list, and the use of digital signatures and trust values, to reduce the impact of single and collaborative black hole attacks in VANETs. However, the simulation results suggest that the introduced security measures come at the cost of additional delay in the network. This trade-off should be carefully considered in the context of the specific VANET

application and its requirements for both security and real-time communication [24].Chaker et al discussed, crucial to recognize the challenges associated with collaborative attacks in VANETs. Collaborative attacks can be more sophisticated and harder to detect because multiple malicious nodes cooperate to achieve their malicious objectives. Addressing such challenges may require more advanced techniques, possibly involving machine learning, anomaly detection, or distributed consensus algorithms to identify coordinated malicious behavior [25].

P. S Hiremath and Anuradha T analysed, communication system involves periodic updates, fuzzy inference for next hop neighbor selection, and a comparison with an adaptive method. The choice of fuzzy logic and an adaptive method reflects an interest in leveraging intelligent decision-making mechanisms for efficient and reliable communication in VANETs. The comparison results will likely provide insights into the strengths and weaknesses of each approach [26].Fiade et al, emphasizes the impact of black hole and flooding attacks on a modified AODV protocol designed for battery energy efficiency in VANETs. The results suggest improved performance in terms of throughput, packet loss rate, remaining battery energy, and end-to-end delays compared to the standard AODV protocol [27]. From the review of literature, we concluded that most of the paper addresses either the authentication or preventing black hole attack or ensuring reliable routing security. To overcome that, we provide an integrated solution for authenticated data dissemination by eliminating black hole attack be proposed.

3. Multi-Dimensional Trust-Based Data Dissemination (MDTD)

The main objective of this research is to eliminate the blackhole attack that affects the data dissemination process in VANET. Additionally, the goal is to establish a trusted route by leveraging the most trustworthy vehicles. Initially, all vehicles in the VANET environment are considered trustworthy. However, over time, some transform into blackhole vehicles and engage in malicious activities by dropping all incoming packets intended for forwarding to other vehicles. The causes of the blackhole attack are discussed in the introduction section. To mitigate these issues, the MDTD mechanism has been introduced. This mechanism involves core components of vehicle activities. The proposed method has been integrated into the Dynamic Source Routing protocol to counteract black hole attacks and establish a reliable route within the Vehicular Ad hoc Network. Trust, also referred to as Decision Trust (DT), is computed considering multiple aspects, including direct observation, indirect observation assessed through recommendations from others, intimacy trust determined by a positive count of interactions, integrity trust evaluated based on confidence, and mobility trust calculated using battery or energy levels and distance. The establishment of the trusted route relies on the Decision Trust, which is maintained by the trusted vehicles [28-32].

The MDTD protocol comprises the following phases:

Preprocessing and Decision Trust parameter setting phase
Decision Trust (DT) evaluation phase
DT propagation and Identifying Black holevehicles phase
Trusted Route establishment phase

Phase 1: Preprocessing and Decision Trust (DT) parameter setting phase

Initially, each vehicle in the network possesses well-defined resources and is considered trustworthy. However, in this study, the presence of black hole vehicles increases gradually. Every vehicle in the network maintains a table called Decision Trust (DT) to store trust information about other vehicles. The structure of DT is depicted in Table 1. All Decision Trust values fall within the range of 0 to 1, where 0 signifies minimum trust, and 1 indicates maximum trust. Each vehicle has the capability to calculate the trust values of others but not its own. It is assumed that the initial energy level of all vehicles is 100%. Unauthorized trust modification by a vehicle to its decision table is strictly prohibited.

Table 1: Structure of DT table maintained by each vehicle

TT table of vehicle		
NID_i (j)	DT_i(j)	TUT_{ij}

Where NID represents the identity of the evaluated vehicle; DT represents the Decision Trust of neighboring vehicle ‘i’ with respect to vehicle ‘j’and TUT represents the trust update time of vehicle ‘i’ with respect to vehicle ‘j’ . The

Decision Trust is assessed based on various aspects, and Table 2 illustrates the trust parameters used in evaluating Decision Trust.

Table 2: Decision Trust evaluation parameters

Vehicle's Comportment	Trust between vehicle i and j at time t	Meaning
Direct trust	T_{ij}^{D} (t)	Direct observation of vehicle *'j'* with respect to vehicle *'i'* at time *'t'*.
Indirect trust	T_{kj}^{ID} (t)	Recommendations of vehicle *'j'* with respect to vehicle *'k'* at time *'t'*.
Intimacy trust	T_{ij}^{IM} (t)	Positive number of interactions of vehicle *'j'* with respect to vehicle *'i'* at time *'t'* .
Integrity trust	T_{ij}^{IG} (t)	Confidence of vehicle *'j'* with respect to vehicle *'i'* at time *'t'*
Mobility trust	T_{ij}^{M} (t)	Mobility trust is calculated based on the battery life and distance

Phase 2: Decision Trust evaluation phase

Over a period, performance of the network may degrade due to black hole vehicles so every vehicle in the network is in situation to execute the MDTD routing protocol [33-37]. As stated earlier, Decision Trust (DT) is calculated based on multi aspects such as direct trust, indirect trust, intimacy trust, integrity trust and social trust. Vehicle 'i' evaluate direct observation of vehicle 'j' at time ti based on packet forwarding ratio. It can be represented as, $At\ time\ t_i$,

$$T_{ij}^{D}(t) = \frac{NCF_j - NCD_j}{NCP_j} + \frac{NDF_j - NDD_j}{NDP_j} \quad T_{ij}^{D}(t) \in [0, 1] \qquad (1)$$

In the eq.1, T_{ij}^{D}(t) denotes direct trust of vehicle 'j' evaluated by vehicle 'i' at time 't' , similarly, NCF_j denotes the number of control packet forwarding ratio of vehicle 'j', NCD_j denotes the number control packet dropping ratio of vehicle 'j',NDF_j denotes number of data packet forwarding ratio of vehicle 'j' andNDD_j denotes number of data packet dropping ratio of vehicle 'j'. Next vehicle 'i' calculate the indirect observation of vehicle 'j' based on the equation 2.

$$T_{ij}^{ID}(t) = T_{ij}^{D}(t) * \sum T_{kj}^{D}(t) \qquad T_{ij}^{ID}(t) \in [0, 1] \qquad (2)$$

In the above equation 2, T_{ij}^{ID}(t) denotes the indirect observation of vehicle *'j'* with respect to vehicle *'i'*, T_{ij}^{D}(t) denotes direct trust of vehicle *'j'* evaluated by vehicle *'i'* and T_{kj}^{D}(t) denotes direct trust of vehicle *'j'* evaluated by neighbor vehicles *'k'*. Next vehicle *'i'* calculate intimacy trust of vehicle *'j'* based on the number of positive interactions and overall interactions. The equation 3 depicts the intimacy trust calculation.

$$T_{ij}^{IM}(\mathrm{t}) = \frac{NPI_j}{OI_j} \quad T_{ij}^{IM}(\mathrm{t}) \in [0,1] \qquad (3)$$

T_{ij}^{IM}(t) denotes the intimacy trust of vehicle 'j' with respect to vehicle 'j', NPI_j denotes the number of positive interactions and OI_j denotes the overall interaction. Next, vehicle 'i' calculate the integrity trust of vehicle 'j' based on confidence level and it is calculated based on reputation of vehicle 'j'. If vehicle 'j' successfully forwarded the packet given by vehicle 'i', it increments good reputation counter by 1. Otherwise it increments the bad reputation counter by one.

$$if\ good\ \ reputation\ counter \geq threshold_1, inegrity = 1$$

$if good\ \ reputatio\ \ n\ counter = threshold_1, inegrity = 0.5$
$if bad\ \ reputation\ counter > threshold_1, inegrity = 0$
$T_{ij}^{IG}(t)$ € [0,1] (4)

Next vehicle 'i' calculates the mobility trust of vehicle 'j'. It is calculated based on the two factors such as energy level and distance between vehicle 'i' and vehicle 'j'. The energy level or battery life is calculated based on the equation 5,

$$E_{ij} = IE_j - [\ \omega_1\ \left[(N-1) * SENT_{Packets_j}\right] + \omega_2\ \left[(N-1) * REC_{Packets_j}\right] + \ \omega_3\ \left[(N-1) * OVR_{Packets_j}\right] \quad (5)$$

E_{ij} represents the present energy of vehicle 'j' with respect to vehicle i, IE_jrepresents the initial energy of vehicle 'j', N represents the number of neighbor vehicle, $SENT_{Packets_j}$ represents the consumed energy while route discovery and route maintenance processes, $REC_{Packets_j}$ represents the consumed energy while route reply process and $OVR_{Packets_j}$ represents consumed energy while monitoring neighbors behaviors. The percentage of present energy is calculated by equation 6.

$$\%E_{ij} = \left(\frac{E_{ij}}{IE_j}\right) * 100\ \ \%\ E_{ij} \in [0,1] \quad (6)$$

Based on the % of Energy (E), Energy Level (EL) is calculated and is classified into four categories that represented in the following equation (7),

$$if\ \%\ of\ energy \geq 80, Energy\ level = 1$$
$$if\ \%\ of\ energy \geq 80 \&\&\ \%\ of\ energy \geq 50, Energy\ level = 0.7 \quad (7)$$
$$if\ \%\ of\ energy < 50 \&\&\ \%energy > 20, Energy\ level = 0.4$$
$$if\ \%\ of\ energy \leq 20, Energy\ level = 0$$

Distance is calculated based on the closeness level. If average closeness of vehicle 'j' with respect to vehicle 'i' is high, distance is also high. Otherwise is low. It can be represented in the equation 8.

$$if\ average\ closeness > threshold_2, distance = 1$$
$$if\ average\ closeness = threshold_2, distance = 0.5 \quad (8)$$
$$if\ average\ closeness < threshold_2, distance = 0$$

Based on the equation 7 and equation 8, mobility trust is calculated based on the equation 9.

$$T_{ij}^{M}(t) = \frac{EL_j + DIS_{ij}}{2}\ T_{ij}^{M}(t)\ \in [0,1] \quad (9)$$

In the above equation 9,T_{ij}^{M}(t) denotes the mobility trust, EL_j denotes the energy level and DIS_{ij} denotes the distance between vehicle 'i' and vehicle 'j'. Finally vehicle 'i' evaluate the vehicle j's decision trust based on direct, indirect, intimacy, integrity and mobility trusts which is shown in the equation 10.

$$DT_{ij} = T_{ij}^{D}(t) + T_{ij}^{ID}(t) + T_{ij}^{IM}(t) + T_{ij}^{IM}(t) + T_{ij}^{M}(t)\ DT_{ij} \in [0,1] \quad (10)$$

In the above equation DT_{ij} denotes the decision trust of vehicle 'j' with respect to vehicle 'j' at time 't'. Then based on the above process, every vehicle in the network will calculate the DT values of their neighboring vehicles.

Phase 3: DT propagation and Identifying Black hole vehicles phase

Once the decision trust (DT) is calculated, based on the DT evaluating vehicle i take decision on vehicle j based on the threshold table, which is shown in the table. If DT_{ij} is greater than or equal to threshold value, those vehicles become trusted vehicles hence they will involve in route discover process. Otherwise, they are untrusted vehicles means black hole vehicles. Information about the black hole every vehicle to its neighboring vehicles broadcasts

vehicles. Upon receiving, neighbor vehicles delete the entries of untrusted vehicles in its route cache. By the way authentication of vehicles can be ensured.

Table 3: Decision Table

Level	DT	Decision
1	$DT_{ij} \geq Threshold\_3$	Authenticated Vehicle
2	$DT_{ij} < Threshold\_3$	Untrusted vehicle or Black hole vehicle

Phase 4: Trusted Route establishment phase

Trusted route establishment only involved with trusted vehicles. The trusted vehicles filtered in the previous phase itself. Here the trusted route form phase consists of the following:

- Route discovery
- Route Maintenance

Route Discovery

Route Request (RREQ) and Route Reply (RPLY) packets accomplish Typicallyin standard DSR, route discovery process. MDTD take this advantage and append its evaluated DT value with original RREQ packets of standard DSR the result is Trusted RREQ packet [38-40] The TRREQ packet format of MDTD is given below.

Table 4: Trusted Route Request (RREQ) packet of MDTD

4 Bytes	4 Bytes	2 Bytes	2 Bytes
Sour_Add	Dest_add	U_id	DT

In the above table, Sour_Addr denotes the source address; Dest_Add denotes the destination address, U_id.

Algorithm of Route Discovery process

The following table illustrates the route discovery process of proposed MDTD.
Algorithm Trusted Route formation
Input: Authenticated vehicles and DT of them
Output: Trusted Route from source to destination
Begin
1. //When route discovery process
2. if source vehicle then
3. Check its own route cache
4. if trusted route from source to destination is available then
5. forward the data packets
6. else
7. Create RREQ packet //(Sour_Addr, Dest_addr,U_id, DT)
8. Broadcast RREQ packets to its neighboring vehicles and set a timer to wait for a reply.
9. If intermediate vehicles then
10. Receive RREQ
11. if already received RREQ
12. Drop the RREQ
13. else
14. Calculate ADT value by adding source's vehicleDT with current vehicle'sDT value and update in the Decision Table (DT).
15. Go to line 8. Repeat the process until reach the destination
16. End if

17. If destination vehicle then
18. If receives first RREQ packet
19. Calculate ADT value by adding source's vehicle DT with current vehicle's DT value
20. Check if ADT> threshold
21. Create RPLY packet
22. Unicast RPLY to source vehicle via intermediate vehicles
23. Add the route along with ADT value in its route cache
24. Forward the RPLY
25. Go to line 28. Repeat the process until reach the source vehicle
26. If source vehicle then
27. Check RPLY. If ADT> threshold, then
28. Forward the data packet
29. Else
30. Discard the packet

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 [41]. The proposed MDTD follows the route maintenance of standard DSR.

4. Simulation Results and Discussion

The proposed MDTD is implemented and tested in Network Simulator (NS3). Vehicles can be represented as number of nodes. The number of mobile vehicles involved in the simulation is 100. Those vehicles are placed randomly in 1000m x 1000m flat area. The total simulation run time is 600s. The DT value of each vehicle calculated at regular interval of 200s over 600s. We have run the simulation for three times for each interval. We have chosen the source and destination vehicle in random fashion with random way point mobility model. The maximum speed of mobile vehicle is set to 30m/s and minimum is set to1 m/s. the vehicle pause is 0. The IEEE 802.11b is used as the medium access control protocol. UDP-CBR (Constant Bit Rate) is used as a traffic generator. The packet size is 64 byte with the data rate of 3072bps. To analyze the impact of black hole vehicle in the network, we have chosen randomly in increasing percentage. The proposed routing protocol is compared with standard DSR routing protocol and TDSR (Mohnapriya et al., 2013) routing protocol. To analyze the performance we used the following performance metrics such as packet delivery ratio, routing packet overhead, average latency, probability of detection and energy consumption. For each metric, we increase the number of black hole vehicles.

Packet delivery ratio versus percentage of black hole vehicles

The figure depicts the packet delivery ratio versus black hole vehicles in percentage.

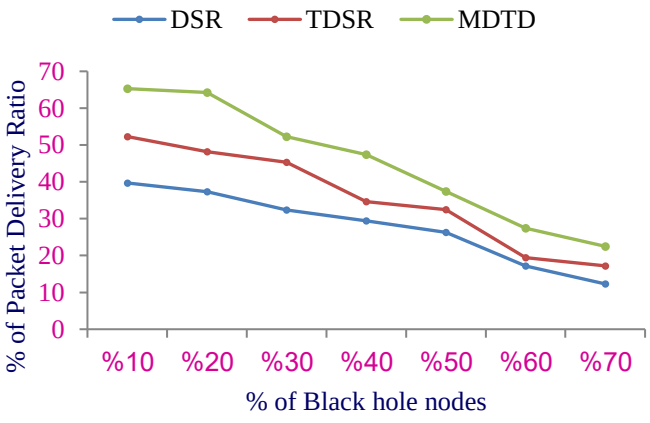

Figure 3. Packet delivery ratio

From the fig 3. We observed that packet delivery ratio of MDTD remains high compared with DSR and TDSR though the number black hole vehicles has increased. The reason is black hole vehicles are identified and isolated from the network based on the DT values before they involve in route discovery process. So route establishment is only involved with authenticated and trusted vehicles therefore packet delivery ratio has increased though black hole vehicles has increased. On the other hand, in TDSR packet delivery ratio is 9.5 low compared with MDTD. The reason is evaluating trustworthiness focused on only packet forwarding ratio.Henceprobability of black hole vehicles remains high therefore, packet delivery ratio is low. Nevertheless, in MDTD trust evaluation is based on multi factors so maximum effort has given to evaluate the trustworthiness. In standard DSR, as there is no detection mechanism of black hole vehicles by default, packets are dropped therefore, packet delivery ratio degrades significantly whenever black hole vehicle increases.

Detection ratio versus percentage of black hole vehicles

The following figure. Represent the detection ratio of TDSR and MDTD.

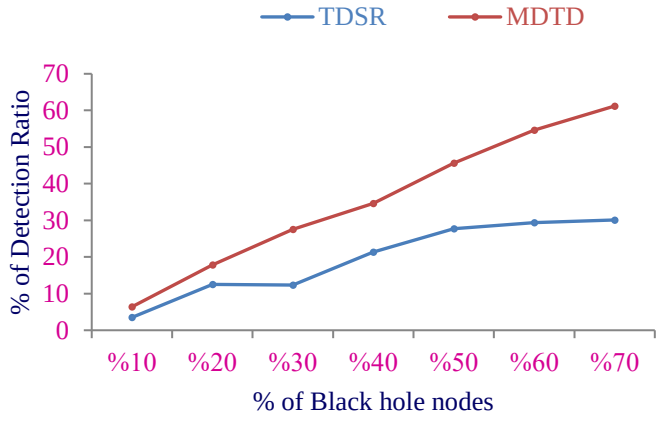

Figure 4. Detection ratio

From the above figure 4, we observed that detection ratio of black hole vehicles in MDTD is 15.84% higher than TDSR. The reason is, in MDTD we identified the black hole vehicles based on multi attributes such as direct, indirect, intimacy, integrity and mobility. Because of these reason detection ratio has increased significantly compared with MDTD. In standard DSR by default, there is no detection mechanism so we did not take into account.

End to end delay versus percentage of black hole vehicles

The following figure 5 depicts the end-to-end delay versus percentage of black hole vehicles. The figure shows end to end delay of DSR is high. As the presence of black hole vehicles, packets are dropping constantly. Therefore, DSR requires retransmission of more packets and it leads to increasing end-to-end delay. Both TDSR and MDTD make use of trust concepts so they eliminated the misbehaving vehicles from dropping the packets. Howeverweakness in trust evaluation of TDSR leads possibility of black hole vehicles. Consequently, packets may drop it causes increasing end-to-end delay. Whereas in MDTD, black hole vehicles are dropped before they involve in route discovery process hence decreasing end-to-end delay.MDTD has 7.11% reduction in end-to-end delay compared with TDSR.

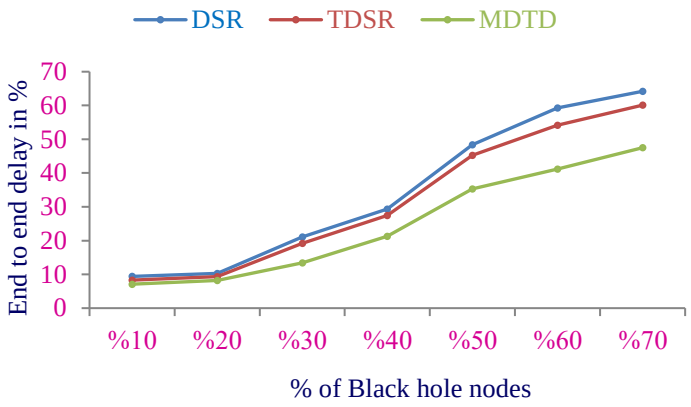

Figure 5. End to end delay

Routing packet overhead versus percentage of black hole vehicles

The figure 6 depicts the routing packet overhead versus percentage of black hole vehicles. From the figure we observed, routing overhead of DSR is less compared with other two protocols. The reason is, in DSR there is no special information in RREQ and RPLY packets like in TDSR and MDTD. In addition, broadcasting of RREQ and RPLY packets are very less. Because of these reasons, routing overhead is low. On the other hand routing overhead is slightly high in MDTD compare with TDSR because broadcasting of DT values before the route discovery process. But in TDSR, there is no such process. However only 1.6% of routing overhead of MDTD increase compared with TDSR.

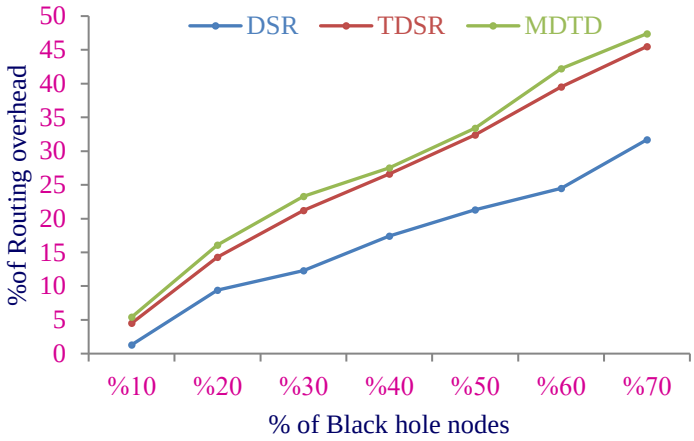

Figure 6. Routing packet overhead

The following table illustrates the performance comparison of various routing protocols.

Table 5: Performance comparison of various routing protocols

S. No.	Parameters	Routing Algorithms		
		DSR	TDSR	MDTD
1	Packet delivery ratio in %	27.8	35.64	45.22
2	End to end delay in ms	34.57	31.97	24.85
3	Detection ratio in %	0	19.54	35.38
4	Routing overhead in %	16.84	26.28	27.9

Discussion and interpretation

The proposed MDTD maintains a consistently high PDR even as the percentage of black hole vehicles increases. This is attributed to MDTD's proactive approach of identifying and isolating black hole vehicles based on Directional Trust (DT) values before engaging in the route discovery process. TDSR exhibits a lower PDR compared to MDTD. The focus on evaluating trustworthiness primarily through packet forwarding ratio contributes to a higher probability of black hole vehicles in the network, leading to a lower PDR. Standard DSR experiences a significant degradation in PDR as the number of black hole vehicles increases due to the absence of a default detection mechanism. This vulnerability results in dropped packets, negatively influencing the overall PDR. MDTD's detection ratio of black hole vehicles is 15.84% higher than TDSR. The multi-attribute approach in MDTD, considering attributes such as direct, indirect, intimacy, integrity, and mobility, contributes to the significantly improved detection ratio compared to TDSR. Standard DSR, lacking a detection mechanism, is not considered in the detection ratio analysis. This highlights a critical limitation in DSR's ability to identify and mitigate black hole attacks. DSR experiences high end-to-end delay due to constant packet drops caused by the presence of black hole vehicles.

The need for retransmission of more packets contributes to an increase in end-to-end delay. TDSR and MDTD, leveraging trust concepts, manage to eliminate misbehaving vehicles, mitigating packet drops. However, TDSR's weakness in trust evaluation leads to a possibility of black hole vehicles, causing increased end-to-end delay. In contrast, MDTD's proactive approach of dropping black hole vehicles before route discovery contributes to a decrease in end-to-end delay. DSR has lower routing packet overhead compared to TDSR and MDTD. The absence of special information in Route Request (RREQ) and Route Reply (RPLY) packets, along with minimal broadcasting, contributes to this lower overhead. MDTD exhibits slightly higher routing overhead compared to TDSR due to the broadcasting of DT values before the route discovery process. However, this increase is modest, with only a 1.6% rise compared to TDSR.

In summary, MDTD emerges as a robust routing protocol, demonstrating superior performance in packet delivery ratio, detection ratio, and end-to-end delay compared to TDSR and DSR. While DSR exhibits, low routing overhead, MDTD's slightly higher overhead is offset by its comprehensive security mechanisms. The findings highlight the effectiveness of MDTD in mitigating the impact of black hole attacks in vehicular networks.

5. Conclusion

This article introduces a multi-dimensional trust-based data dissemination mechanism designed to enhance authentication and eliminate blackhole attacks in VANET. The proposed method ensures that data dissemination occurs exclusively among authenticated vehicles, effectively removing blackhole vehicles from the network through a multi-factor trust evaluation mechanism encompassing direct, indirect, mobility, integrity, and intimacy trusts. Consequently, the proposed method is highly effective in detecting and mitigating blackhole attacks. Notably, this approach is particularly suitable for vehicles with limited processing capability, as it does not rely on cryptographic methods. By limiting data dissemination to trusted (authenticated) vehicles, the overall security of the VANET environment is bolstered. Since TDSR exhibits limitations in trust evaluation, future work could focus on improving the trustworthiness assessment mechanisms. Exploring additional factors beyond packet forwarding ratio and incorporating a multi-faceted trust model may contribute to more robust detection and mitigation of black hole attacks. While MDTD demonstrates effective detection and isolation of black hole vehicles, further research could be directed towards optimizing the end-to-end delay. Investigating techniques to minimize delays associated with the proactive dropping of black hole vehicles before route discovery may enhance overall network efficiency. Machine learning algorithms can be integrated into the trust management systems to enhance the accuracy and efficiency of black hole detection. Developing models that can adapt to evolving attack strategies and patterns could strengthen the overall security posture of the vehicular network.

References

[1] G. Jyoti, M. S. Gaur, and S. Auerbach, *Security of Self-organizing Networks MANET, WSN, WMN, VANET*, CRC Press, 2010.

[2] Y. Wang and F. Li, *Vehicular Ad Hoc Networks*, Springer-Verlag, London, 2009.

[3] C. Wei, Y. Jianding, and L. Xiangjun, "The design of electronic license plate recognition terminal system based on nRF24LE1," in *Proc. 2012 Fifth Int. Symp. Computational Intelligence and Design (ISCID)*, 2012, pp. 127–129.

[4] W. Liang, Z. Li, H. Zhang, S. Wang, and R. Bie, "Vehicular Ad Hoc Networks: Architectures, Research Issues, Methodologies, Challenges, and Trends," *Int. J. Distributed Sensor Networks*, vol. 2015, Article ID 745303, 11 pages.

[5] S. Zeadally, R. Hunt, Y.-S. Chen, A. Irwin, and A. Hassan, *Vehicular Ad Hoc Networks (VANETS): Status, Results, and Challenges*, Springer Science, 2010.

[6] Z. Stampoulis and Z. Chai, "A Survey of Security in Vehicular Networks," Project CPSC 534, 2007.

[7] T. Zhou, R. R. Choudhury, P. Ning, and K. Chakrabarty, "Privacy-preserving detection of sybil attacks in vehicular ad hoc networks," in *Proc. 4th Annual Int. Conf. Mobile and Ubiquitous Systems: Networking and Services. MobiQuitous*, 2007, pp. 1–8.

[8] H. Hasrounya, A. E. Samhat, C. Bassil, and A. Laouitia, "VANet security challenges and solutions: A survey," *Vehicular Communications*, vol. 7, pp. 7–20, 2017.

[9] M.-C. Chuang and J.-F. Lee, "TEAM: Trust-Extended Authentication Mechanism for Vehicular Ad Hoc Networks," *IEEE Syst. J.*, DOI: 10.1109/JSYST.2012.2231792.

[10] F. Gómez-Mármol and G. Martínez Pérez, "TRIP, a trust and reputation infrastructure-based proposal for vehicular ad hoc networks," *J. Netw. Comput. Appl.*, vol. 35, pp. 934–941, 2012.

[11] D. Huang, X. Hong, and M. Gerla, "Situation-Aware Trust Architecture for Vehicular Networks," *IEEE Commun. Mag.*, vol. 48, no. 11, pp. 128–135, Nov. 2010.

[12] X. Lai, J. Zhou, and H. Li, "APPA: Aggregate Privacy-Preserving Authentication in Vehicular Ad Hoc Networks," *LNCS 7001*, pp. 293–308, 2011.

[13] C. Caballero-Gil, P. Caballero-Gil, and J. Molina-Gil, "Mutual authentication in self-organized VANETs," *Comput. Stand. Interfaces*, vol. 36, no. 4, pp. 25–30, 2013.

[14] A. Malathi and N. Sreenath, "Black Hole Attack Prevention and Detection in VANET using Modified DSR Protocol," *Int. J. Comput. Appl.*, vol. 168, no. 7, pp. 1–8, Jun. 2017.

[15] P. Tyagi and D. Dembla, "Performance analysis and implementation of proposed mechanism for detection and prevention of security attacks in routing protocols of vehicular ad-hoc network (VANET)," *Egypt. Informat. J.*, vol. 18, no. 2, pp. 133–139, Jul. 2017.

[16] I. Dhyani, N. Goel, G. Sharma, and B. Mallick, "Black hole Attack Prevention in VANET," *Int. J. Futur. Revol. Comput. Sci. Commun. Eng.*, vol. 3, no. 10, pp. 1–6, 2017.

[17] M.-Y. Su, "Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems," *Comput. Commun*, vol. 34, no. 1, pp. 107–117, Jan. 2011.

[18] E. Karthikeyan et al., "A review analysis on emergency data dissemination techniques in vehicular adhoc networks," *Int. J. Sci. Technol. Res.*, vol. 8, pp. 1209–1215, 2019.

[19] S. Sibichen et al., "An Efficient AODV Protocol and Encryption Mechanism for Security Issues in Adhoc Networks," in *Proc. Int. Conf. Microelectronics, Commun. and Renewable Energy (ICMiCR-2013)*, IEEE, 2013.

[20] S. Majeed and M. Abdala, "Blackhole Attack effect Elimination in VANET Networks using IDA-AODV, RAODV and AntNet Algorithm," *J. Telecommun.*, vol. 36, no. 1, pp. 15–19, Feb. 2017.

[21] R. S. Raw, M. Kumar, and N. Singh, "Security challenges, issues and their solutions for vanet," Sept. 2013.

[22] G. Karagiannis, O. Altintas, et al., "Vehicular networking: A survey and tutorial on requirements, architectures, challenges, standards and solutions," *IEEE Commun. Surv. Tutor*, vol. 13, no. 3, pp. 1–22, 2011.

[23] S. Kannan et al., "Secure Data Transmission in MANETs using AODV," *Int. J. Comput. Commun. Eng. Res.*, vol. 2, no. 2, pp. 1–9, 2014.

[24] S. M. Arumugam, N. Neelavathy Pari, H. V. S., "Detection of Single and Collaborative Black Hole Attack in MANET," in *Proc. Int. Conf. Wireless Commun, Signal Process. and Networking (WiSPNET)*, IEEE, pp. 2040–2044, 2016.

[25] A. K. Chaker, A. Lakasy, and N. Lagraa, "Detection of Intelligent Malicious and Selfish Nodes in VANET using Threshold Adaptive Control," in *Proc. 5th Int. Conf. Electronic Devices, Syst. and Appl. (ICEDSA)*, IEEE, 2016.

[26] P. S. Hiremath and A. T., "Adaptive Method for Detection and Prevention of Cooperative Black Hole Attack in MANETs," *Int. J. Electr. Electron. Data Commun*, vol. 3, no. 4, pp. 1–7, 2015.

[27] A. Fiade, A. Y. Triadi, A. Sulhi, S. U. Masruroh, V. Handayani, and H. B. Suseno, "Performance Analysis of Black Hole Attack and Flooding Attack AODV Routing Protocol on VANET," in *Proc. 2020 8th Int. Conf. Cyber and IT Service Manag. (CITSM)*, IEEE, 2020.

[28] R. Dhanaraj, R. K. Rajesh Kumar, S. K. Hafizul Islam, and V. Rajasekar, "A cryptographic paradigm to detect and mitigate blackhole attack in VANET environments," *Wireless Netw*, vol. 28, no. 7, pp. 3127–3142, 2022.

[29] B. Alaya and L. Sellami, "Clustering method and symmetric/asymmetric cryptography scheme adapted to securing urban VANET networks," *J. Inf. Secur. Appl.*, vol. 58, pp. 102779, 2021.

[30] T. Nandy et al., "A secure, privacy-preserving, and lightweight Authentication scheme for VANETs," *IEEE Sensors J.*, vol. 21, no. 18, pp. 20998–21011, 2021.

[31] B. Karthiga et al., "Intelligent intrusion detection system for VANET using machine learning and deep learning approaches," *Wireless Commun. and Mobile Comput*, vol. 2022, pp. 1–11, 2022.

[32] H. Bangui, M. Ge, and B. Buhnova, "A hybrid machine learning model for intrusion detection in VANET," *Computing*, vol. 104, no. 3, pp. 503–531, 2022.

[33] F. Ghaleb et al., "Misbehavior-aware on-demand collaborative intrusion detection system using distributed ensemble learning for VANET," *Electronics*, vol. 9, no. 9, pp. 1411, 2020.

[34] Z. Ma et al., "An efficient decentralized key management mechanism for VANET with blockchain," *IEEE Trans. Vehicular Technol.*, vol. 69, no. 6, pp. 5836–5849, 2020.

[35] L. Wei et al., "Proven secure tree-based authenticated key agreement for securing V2V and V2I communications in VANETs," *IEEE Trans. Mobile Comput.*, vol. 21, no. 9, pp. 3280–3297, 2021.

[36] A. Kumar et al., "Distribution Key Scheme for Secure Group Management in VANET Using Polynomial Interpolation," *Int. Symp. Security and Privacy in Social Networks and Big Data*, Singapore: Springer Singapore, 2021.

[37] N. Ravi et al., "Securing VANET using blockchain technology," *J. Phys.: Conf. Ser.*, vol. 1979, no. 1, 2021.

[38] Y. Inedjaren et al., "Blockchain-based distributed management system for trust in VANET," *Vehicular Commun.*, vol. 30, pp. 100350, 2021.

[39] Z. Ma et al., "An efficient decentralized key management mechanism for VANET with blockchain," *IEEE Trans. Vehicular Technol.*, vol. 69, no. 6, pp. 5836–5849, 2020.

[40] K. Prathapchandran and T. Janani, "A trust aware security mechanism to detect sinkhole attack in RPL-based IoT environment using random forest–RFTRUST," *Comput. Netw*, vol. 198, 2021, Art. 108413.

AUTHOR PROFILE

Balakumar Chellamuthu received his MCA from Kongu Engineering College, in 2013 & M. E(CSE) from Anna University, Chennai in 2015. He is pursuing the Ph.D degree at Dr.SNS Rajalakshmi College of Arts and Science (Autonomous) Coimbatore. He published more then 10 articles in PG level. His research interests include Vechicular Adhoc Networks,Network Security, Wireless Sensor Networks. Email: balakumar.cbk@gmail.com

Dr. Vydehi Shanmugavadivelu received her Post Graduation from University of Madras in 2000, M. Phil. from Bharathidasan University, Tiruchirappalli in 2008. She also completed her Ph. D in Computer Science from Periyar University in 2018. She is presently working as Associate Professor and Head in Department of Information Technology Dr.SNS Rajalakshmi College of Arts and Science (Autonomous) Coimbatore. She has more then 20 year teaching and research experience. Her research interests on Design Thinking, Deep Learning, Machine Learning, Networks,Artificial Inelligence.