IJARSCT

International Journal of Advanced Research in Science, Communication and Technology

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

ISSN: 2581-9429

Volume 5, Issue 2, December 2025

Impact Factor: 7.67

Mitigating DoS Attacks in VANETs Using an Innovative Security Method

Ajit Kumar[1], Dr. Harsh Lohiya[2], Mr. Ankit Navgeet Joshi[3]

[1]Research Scholar, Department of CSE

[2]Associate Professor, Department of CSE

[3]Assistant Professor, Department of CSE

Sri Satya Sai University of Technology & Medical Sciences, Sehore, Madhya Pradesh, India

Abstract: *The high mobility of Vehicular Ad Hoc Networks (VANETs) makes secure routing a critical challenge. Their highly dynamic topology leads to frequent changes and susceptibility to network disruptions caused by obstacles such as buildings, tunnels, and bridges. These intermittent connections often result in packet loss, degrading overall network performance. Identifying the root cause of packet loss is difficult, as it may stem from both network instability and various security threats. As a subset of Mobile Ad Hoc Networks (MANETs), VANETs are vulnerable to attacks including denial of service (DoS), black hole, gray hole, and ghost attacks. Although numerous security mechanisms have been proposed for MANET routing, VANETs require more robust solutions due to their unique communication modes—vehicle-to-infrastructure (V2I) and vehicle-to-vehicle (V2V). There is a growing need to secure the interaction between these communication types. This paper presents a security approach designed to detect, analyze, and mitigate existing threats to ensure reliable and secure routing in VANET environments.*

Keywords: Authentication, Confidentiality, Attack,VANET, Replay.

I. INTRODUCTION

Vehicular Ad Hoc Networks (VANETs) are designed to improve safety and efficiency within modern transportation systems. They consist of mobile nodes—vehicles and roadside units (RSUs)—equipped with sensors, processing capabilities, and wireless communication modules. Through vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication, a wide range of applications can be supported. Many research efforts highlight that frequent beaconing of vehicle position, status, and environmental alerts will play a crucial role in enabling safety-related services.

However, VANETs are highly vulnerable to security attacks that can compromise system performance and user privacy. Attackers may inject false beacons, manipulate transmitted information, or track vehicle messages to infer sensitive data about drivers. Therefore, implementing strong security and privacy-preserving mechanisms is essential for the reliable deployment of VANETs.

Key security issues in VANET include:

- **Data Authentication:** Since vehicles frequently change lanes and positions, validating the authenticity of safety messages and their origin becomes challenging. Flooding attacks with fake messages can overwhelm network bandwidth, making robust entity authentication necessary.
- **Data Integrity:** Information transmitted over open wireless channels may be intercepted and modified. Mechanisms must be in place to ensure that data received by vehicles remains unchanged.
- **Data Availability:** Obstacles and malicious attacks can disrupt message forwarding, preventing critical alerts from reaching vehicles. Systems must be capable of detecting and resolving such interruptions.
- **Data Confidentiality:** Sensitive data should remain inaccessible to unauthorized nodes, yet the shared wireless medium exposes communication to potential breaches.

DOI: 10.48175/568

- **Non-repudiation:** Vehicles, drivers, or passengers may deny sending messages by altering their identities. Reliable identification mechanisms are essential to prevent such disputes.

VANETs commonly face attacks such as wormhole, blackhole, grayhole, Sybil, DoS, DDoS, spoofing, fabrication, and signal jamming. This paper focuses on a security solution that protects routing information specifically against Denial-of-Service (DoS) attacks, as detailed in the following sections.

Denial of Service (DoS) Attack

The most dangerous attack in the network is Denial of Service (DOS) attack. In DOS attack (Figure 1) dummy or fake nodes are created to transmits fake messages like "path ahead is closed. It stops the communication between vehicle-to-vehicle and vehicle-to-infrastructure. This type of attack is done to reduce the efficiency and performance of the system [48]. In the scenario given below the malicious node transmit the wrong information to RSU (roadside unit) that path is not available ahead so that RSU gives or transmit the wrong information to the other nodes which are behind the attacker node.

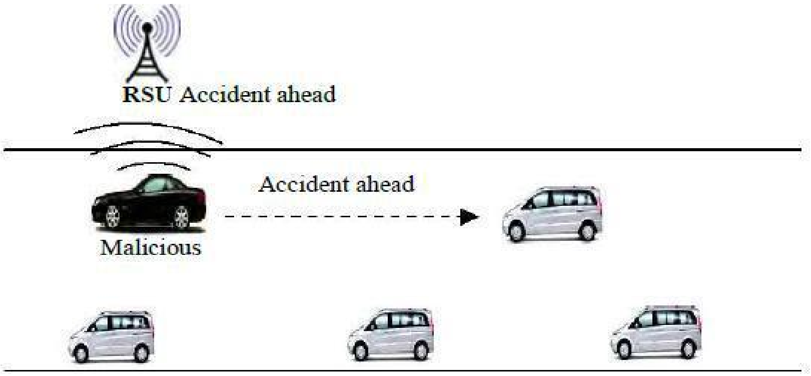

Figure 1: Denial of Service Attack

In case of Dos attack, intruder intercepts the channel and brings down the available network resources by following:

• Resource consumption: Intruder can consume the available bandwidth by injecting fake messages thus resulting in congestion over network and degrading the end user's experience.

• Signal Jamming: An Intruder can jam the transmission using interference.

• Packet Drop: Intruder can also drop all or selected packets to interrupt the routing.

Wang Suwan and He Yuan "A Trust System for Detecting Selective Forwarding Attacks in VANETs," In this paper, they are working on the selective forwarding attack in which malicious nodes acts as a normal node by making the trust based system

1) Mutual monitoring is used for finding the attacks between nodes by using the local and global information.

2) Detection of attacker node based upon abnormal or bad driving patterns of malicious nodes.

Since both in-band and out-band data is used. VANET is a high natural portability and takes information, to share the data among different vehicles. Selective forwarding attack, are the attack in which masquerade nodes acts as normal nodes which drop the data packets, damage the real form of data and damages the legitimacy of genuine VANETs applications. It is very difficult to obtain the selective forwarding attack because the attacker node always acts as a normal node and try to clash with each other whenever they want to change the integrity of data and so that damage occur in the VANET system.

II. LITERATURE SURVEY

Amrita Chakraborty et al., in "Swarm Intelligence: A Review of Algorithms," present an overview of insect- and animal-inspired algorithms. The paper analyzes the functioning of these algorithms, outlines the biological inspirations behind them, and highlights specific application areas. As an essential branch of artificial intelligence, swarm intelligence is discussed in terms of its fundamental concepts, technical aspects, and future research potential [23].

Ahmad Shaheen et al., in “Comparison and Analysis Study between AODV and DSR Routing Protocols in VANET with IEEE 802.11b,” evaluate the performance of AODV and DSR protocols in VANET under two different scenarios. Each protocol is assessed independently through various tasks, and their performance metrics are compared. Since VANETs are a specialized form of MANETs, MANET routing protocols can be adapted for VANETs, although modifications are often required due to differing network characteristics [24].

Tareq Emad Ali et al., in “Review and Performance Comparison of VANET Protocols: AODV, DSR, OLSR, DYMO, DSDV & ZRP,” provide a comprehensive study of ad hoc routing protocols used in vehicular networks. Due to the high mobility of vehicles, path breaks frequently occur, affecting the stability and performance of routing protocols. The paper compares these protocols using metrics such as packet delivery ratio, delay, and throughput, emphasizing the role of vehicular networks in enabling dynamic data exchange among moving vehicles [25].

L. Bariah et al. examine the latest security mechanisms proposed for VANETs. Their investigation covers a variety of threats—including repudiation, wormhole, spamming, replay, jamming, DoS, DDoS, and blackhole attacks—along with corresponding issues and potential solutions. The study categorizes threats based on V2V and V2I communication and compares simulation tools such as NCTUns, NS-2, Qualnet, GrooveNet, and TraNS [5].

A. Singh et al. propose an algorithm known as EAPDA to detect DoS attacks in VANETs. The method uses time slots, threshold values, and communication gaps to identify intruder nodes, ultimately isolating compromised nodes from the network. Simulation results demonstrate improved throughput and a reduction in false alarms [6].

R. Saranya et al. conduct a survey on DDoS and wormhole attacks and analyze existing mitigation techniques. Their findings indicate that the FireCol method effectively reduces attack intensity, while traffic matrices are useful for monitoring P2P-based applications. Additionally, Bloom filters can safeguard routing information. The survey includes a comparative assessment of these solutions [7].

III. PROPOSED WORK

All routing information is logged as per the events occurred over network. If there is any packet drop at any specific route and its cause is unknown, its drop count is incremented automatically and after reaching a Threshold value, current path is isolated from network, if node is drooping the packet, without any valid reason.

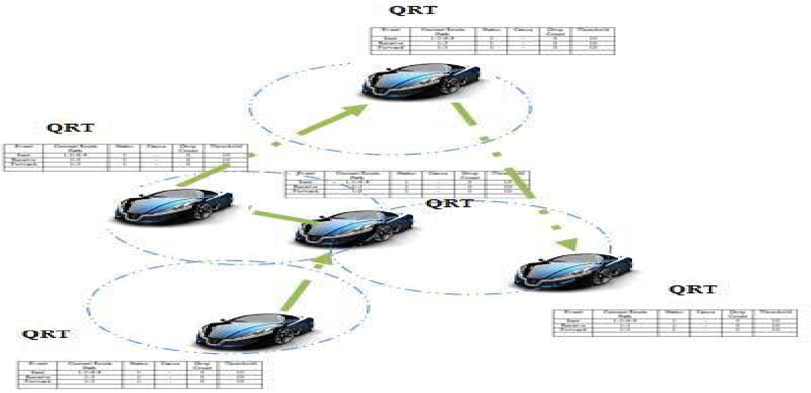

Figure 2: QRT for routing

During route maintenance phase, using QRT, identified routes and nodes are ignored and cannot be considered for routing purpose.

TABLE-I QRT FOR ROUTING INFORMATION ANALYSIS

Event(s)	Current Route Path	Status	Cause	Drop Count	Threshold
Sent	1-3-6-9	1	-	0	10
Receive	1-3	1	-	0	10
Forward	1-3	1	-	0	10

DOI: 10.48175/568

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 2, December 2025
Impact Factor: 7.67

TABLE – II QRT FOR DOS DETECTION

Event	Current Route Path	Status	Cause	Drop Count	Thres hold
Sent	1-3-6-9-12-18	1	-	6	10
Receive	1-3	0	Unknown Drop	39	10
Forward	6-9	0	Drop, if path not found	19	10

Table II above shows that there is a huge packet drop at route path 1-3 and its reason is known whereas for route 6-9, packets are dropped due to invalid path information. So QRT assumes that route 1-3 has been compromised and there is a need to isolate this from network.

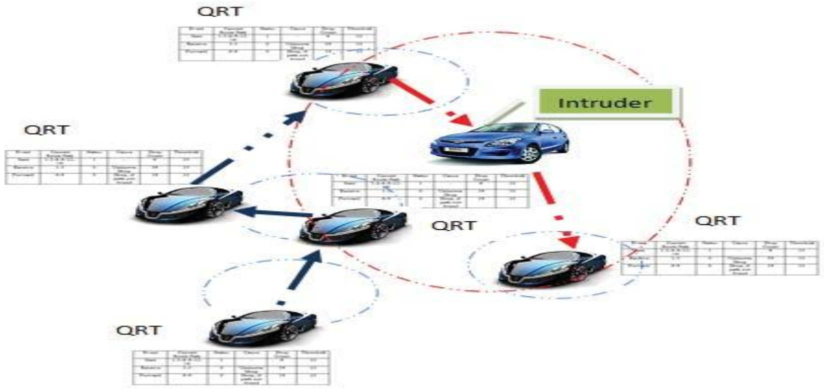

Figure 3:. QRT response for DoS attack

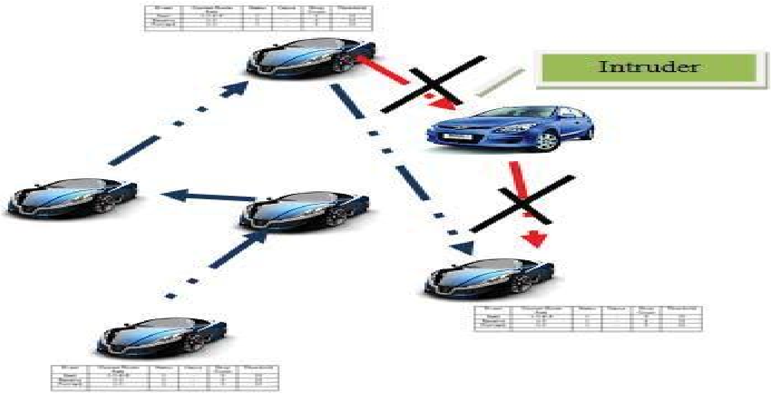

Figure 4: Route building by isolating the malicious node using QRT

Algorithm to build QRT:

```
Event Used:
S:= Packet Sent; D:= Packet Drop;
R:= Packet Received; F:= Packet Forward;
DCount: Packet Drop Count; Cr:= Get_Info(Current Route)
Cr->analyze (Event,Status,Cause,Count,Threshold)
If (Event==S || R || F)
{       If (Cause(D)!Valid)
{
Cr->DCount++; Log_QRT (Cr);
}
```

DOI: 10.48175/568

```
If (Status==0 && Count > Th && Cause!=N)
{           Dump(Cr->CRP); Log_QRT (Cr);
}
       }
```

Route Maintenance:

```
Route Maintenance ()
{       If exists (node->ID, QRT)
{       FindRoute(node->ID) //  malicious nodes
DeleteRoute(node->ID)  //  Delete  entry  malicious  nodes from existing routes
AvoidRoute(node->ID) // Avoid malicious nodes for route selection
} else { Addroute(node->ID)
}
       }
```

IV. RESULT ANALYSIS

To investigate the effectiveness of the proposed scheme in defending against VANET's DoS attacks, the simulation on a topology was carried out using Network Simulator version (NS 2.35)

Table 1: Simulation Configuration

Parameters	Configuration Value(s)
Routing Protocol	Dynamic Source Routing
Wireless Terrain	1200x1200
Node's Density	30
Velocity	100ms
MAC Protocol	MAC 802.11p
Traffic Type	CBR
Ifq length	50
Propagation Model	Nakagami
Sampling Interval	0.05 ms
Simulation Time	10 seconds
Simulation Scenarios	a. NDoS: Uncompromised Network b. WDoS: With DoS (Compromised Network) c. QRT: DoS: Quick Response Tables for DoS attack

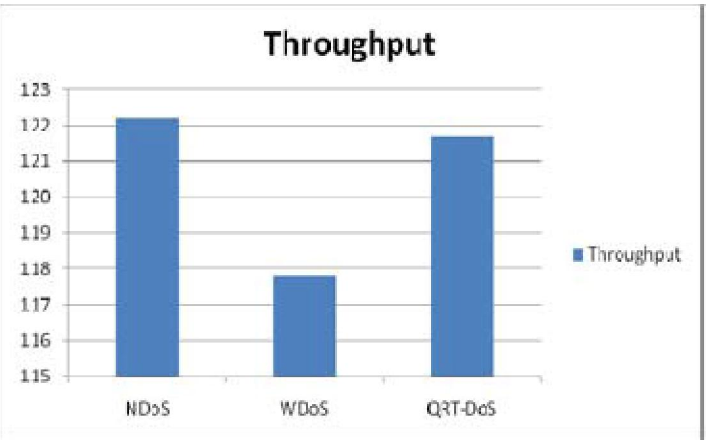

Figure 4.1: Throughput

Figure 4.1 above shows the impact of DoS attack (WDoS) over Throughput of DSR protocol. It can be observed that without using QRT, Throughput is very less and QRT enhanced the Throughput efficiently.

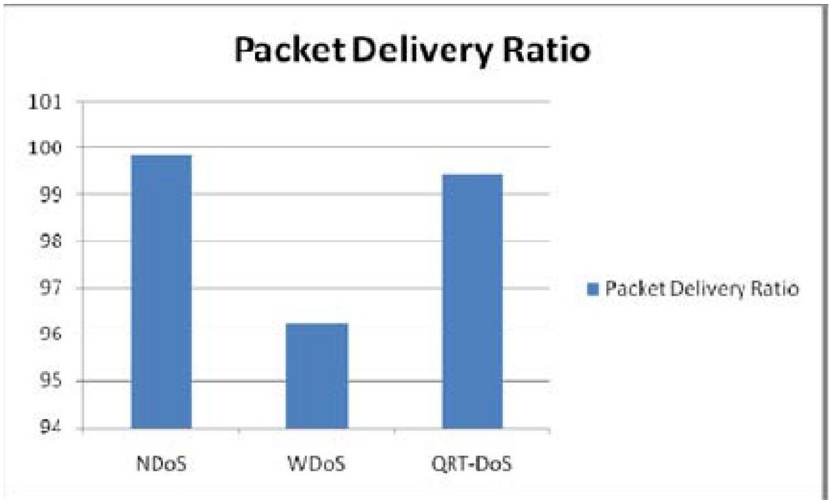

Figure 4.2: Packet Delivery Ratio

Figure 4.2 above shows the impact of DoS attack (WDoS) over PDR. It can be observed that without using QRT, PDR is very less and QRT enhanced the PDR.

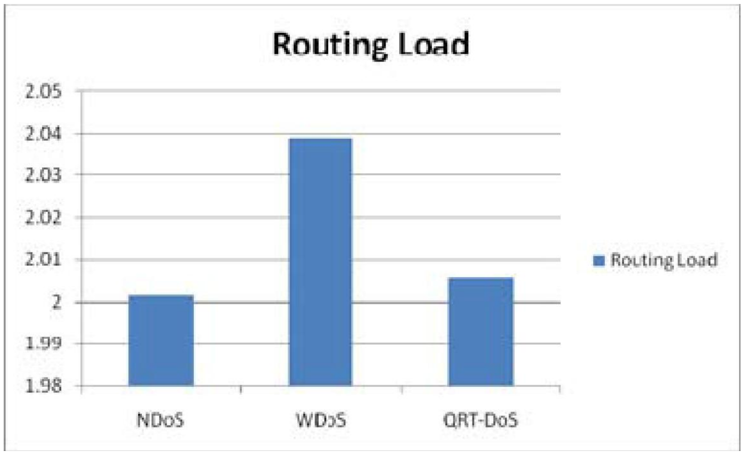

Figure 4.3: Routing Load

Figure 4.3 above shows the impact of DoS attack (WDoS) over routing load. It can be observed that without using QRT, routing load is very high and QRT reduced the routing load.

Figure 4.4 shows the imapct of DoS attack (WDoS) over Delay. It can be observed that without using QRT, routing load is very high and QRT reduced the routing load. Figure 4 shows the impact of DoS atatck (WDoS) over delay. It can be observed that without using QRT, delay is very high and QRT reduced the delay upto a siginificant level.

DOI: 10.48175/568

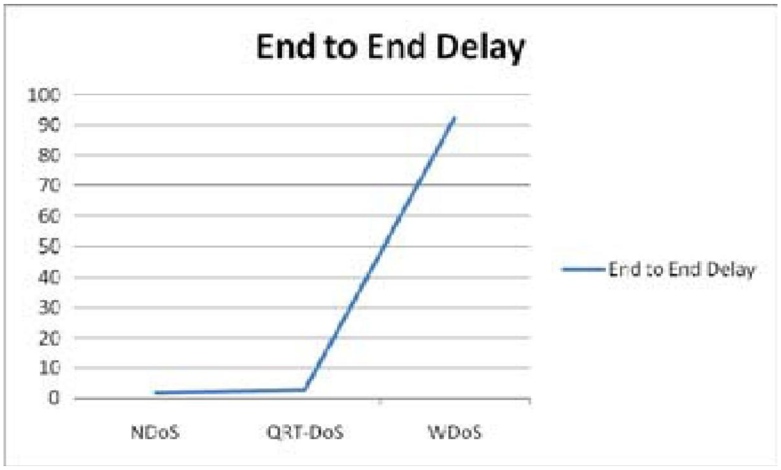

Figure 4.4: End to End Delay

V. CONCLUSION

We propose a scheme to protect VANETs from DoS attacks using Quick Response Tables (QRT). The QRT mechanism monitors frequent updates in routing information and compares them against a reference table. When a node exhibits malicious behavior, its status is recorded in the QRT for future reference. This information is then shared with all nodes, enabling them to use the log during route maintenance to prevent malicious nodes from re-entering the routing process.

The security analysis shows that packet drops occurring in the early stages are treated as normal loss; however, with the help of QRT logs, large-scale packet drops can be easily identified at later stages, allowing timely isolation of the intruding node from the routing table. QRT maintains detailed event references along the routing path, and once a log entry is created for a specific node, neighboring nodes begin to ignore it. As a result, QRT effectively safeguards the entire network from DoS attacks.

Simulation results demonstrate that DoS attacks increase routing load and reduce throughput and packet delivery ratio (PDR). With QRT, these attacks are efficiently detected, and network performance is gradually restored. The proposed approach enhances throughput and PDR while reducing routing load and delay. This scheme can be further extended to mitigate DDoS attacks in VANETs using additional protocols.

REFERENCES

[1] B. Gupta, V. Prajapati, N. Nedjah, P. Vijayakumar, A. A. A. El-Latif, and X. Chang, “Machine learning and smart card based two-factor authentication scheme for preserving anonymity in Telecare Medical Information System (TMIS),” Neural Comput. Appl., pp. 1–26, 2021. [Online]. Available: https://link.springer.com/article/10.1007/s00521-021-06152-x#citeas

[2] C. Wang, R. Huang, J. Shen, J. Liu, P. Vijayakumar, and N. Kumar, “A novel lightweight authentication protocol for emergency vehicle avoidance in VANETs,” IEEE Internet Things J., vol. 8, no. 18, pp. 14248–14257, Sep. 2021.

[3] M. A. R. Baee, L. Simpson, X. Boyen, E. Foo, and J. Pieprzyk, “Authentication strategies in vehicular communications: A taxonomy and framework,” EURASIP J. Wireless Commun. Netw., vol. 2021, no. 1, pp. 1–50, 2021.

[4] M. A. Rezazadeh Baee, L. Simpson, X. Boyen, E. Foo, and J. Pieprzyk, “ALI: Anonymous lightweight inter-vehicle broadcast authentication with encryption,” IEEE Trans. Dependable Secure Comput., early access, 2022, doi: 10.1109/TDSC.2022.3164436.

[5] L. Bariah, Dina Shehada, Ehab Salahat and Chan Yeob Yeun, "Recent Advances in VANET Security: A Survey", Vehicular Technology Conference (IEEE-VTC Fall), pp.1-7, 2015.

[6] A. Singh, Priya Sharma, "A novel mechanism for detecting DoS attack in VANET using Enhanced Attacked Packet Detection Algorithm (EAPDA)", 2nd International Conference on Recent Advances in Engineering & Computational Sciences (RAECS), pp.1-5, 2015.

[7] R.Saranya, Dr.S.Senthamarai Kannan,N.Prathap, "A survey for restricting the DDOS traffic flooding and worm attacks in internet", International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT), pp.251-256, 2015.

[8] S. Wang and Y. He, "A Trust System for Detecting Selective Forwarding Attacks in VANETs," Springer International Publishing Switzerland, 2016, vol.4, pp. 377–386.

[9] M. Kaur and M. Mahajan, "Protection Against DDOS Using Secure Code Propagation In The VANETs," An International Journal of Engineering Sciences, 2016, vol. 17, no. 1, pp. 573–577.

[10] K. Lim, "Secure and Authenticated Message Dissemination in Vehicular ad hoc Networks and an Incentive-Based Architecture for Vehicular Cloud," 2016, vol. 19, pp. 1-104.

[11] A. Info, "Design and Analysis of Secure VANET Framework preventing Black Hole and Gray Hole Attack," International Journal of Innovative Computer Science & Engineering **,** 2016**,** vol. 3, no. 4, pp. 9-13.

[12] M. N. Mejri, Nadjib Achir, Mohamed Ham, "A New Security Games Based Reaction Algorithm against DOS Attacks in VANETs", 13th IEEE Annual Consumer Communications & Networking Conference (CCNC), pp.837 – 840, 2016.

[13] G. Kumaresan, T. Adiline Macriga, "Group Key Authentication scheme for Vanet INtrusion detection (GKAVIN)", Wireless Networks, Springer, pp 1–11, 2016.

[14] Farhan Jamil, Anam Javaid Tariq Umer, Mubashir Husain Rehmani "A comprehensive survey of network coding in vehicular ad-hoc networks", Wireless Networks, Springer, pp 1–20, 2016.

[15] M. J. Faghihniya, Seyed Mojtab Hosseini Maryam Tahmasebi, "Security upgrade against RREQ flooding attack by using balance index on vehicular ad hoc network", Wireless Networks, Springer, pp.1–12, 2016.

[16] S. Ibrahim, Mohamed Hamdy, Eman Shaaban, "A Proposed Security Service Set for VA NET SOA", Seventh International Conference on Intelligent Computing and Information Systems (IEEE-ICICIS), pp. 649 – 653, 2015.

[17] X. Li, T. Liu, M. S. Obaidat, F. Wu, P. Vijayakumar, and N. Kumar, "A lightweight privacy-preserving authentication protocol for VANETs," IEEE Syst. J., vol. 14, no. 3, pp. 3547–3557, Sep. 2020.

[18] M. A. Khan, A. Ghani, M. S. Obaidat, P. Vijayakumar, K. Mansoor, and S. A. Chaudhry, "A robust anonymous authentication scheme using biometrics for digital rights management system," in Proc. Int. Conf. Commun., Comput., Cybersecurity, Inform., 2021, pp. 1–5.

[19] B. Gupta, V. Prajapati, N. Nedjah, P. Vijayakumar, A. A. A. El-Latif, and X. Chang, "Machine learning and smart card based two-factor authentication scheme for preserving anonymity in Telecare Medical Information System (TMIS)," Neural Comput. Appl, pp. 1–26, 2021. [Online]. Available: https://link.springer.com/article/10.1007/ s00521-021-06152-x#citeas

[20] C. Wang, R. Huang, J. Shen, J. Liu, P. Vijayakumar, and N. Kumar, "A novel lightweight authentication protocol for emergency vehicle avoidance in VANETs," IEEE Internet Things J., vol. 8, no. 18, pp. 14248–14257, Sep. 2021.

[21] M. A. R. Baee, L. Simpson, X. Boyen, E. Foo, and J. Pieprzyk, "Authentication strategies in vehicular communications: A taxonomy and framework," EURASIP J. Wireless Commun. Netw., vol. 2021, no. 1, pp. 1–50, 2021.

[22] M. A. Rezazadeh Baee, L. Simpson, X. Boyen, E. Foo, and J. Pieprzyk, "ALI: Anonymous lightweight inter-vehicle broadcast authentication with encryption," IEEE Trans. Dependable Secure Comput., early access, 2022, doi: 10.1109/TDSC.2022.3164436.

[23] A. Chakraborty and A. K. Kar, "Swarm Intelligence : A Review of Algorithms," Springer International Publishing AG, 2017, vol. 10, pp. 475–494

[24] A. Shaheen, "Comparison and Analysis Study between AODV and DSR Routing Protocols in VANET with IEEE," Journal of Ubiquitous Systems & Pervasive Networks, 2016, vol. 7, no. 12, pp. 7-12.

DOI: 10.48175/568

[25] T. E. Ali and L. A. Khalil, “Review and Performance Comparison of VANET Protocols: AODV, DSR, OLSR, DYMO, DSDV & ZRP,” Al-Sadeq International Conference on Multidisciplinary in IT and Communication Science and Applications (AICMITCSA), 2016, vol. 5, pp. 1-6.