Prevent Vehicle Ad hoc Networks from Denial of Service Attack using Novel Approach

Sonam Kumari [1], Dr. Harsh Lohiya[2], Dr Rajendra Singh Kushwah

[1]*Research Scholar, Department of CSE, SSSUTMS, Sehore, Madhya Pradesh, India,*
[2]*Associate Professor, Department of CSE, SSSUTMS, Sehore, Madhya Pradesh, India*
[3] *Professor, Department of CSE, SSSUTMS, Sehore, Madhya Pradesh, India*

ABSTRACT

Due to the mobility of VANET's, secure routing is a major issue. Due to its dynamic nature, changes are constant and can also be subject to network outages due to obstacles such as buildings, tunnels and bridges. Intermittent connections can cause packet loss, which can result in poor network performance. Determining the cause of packet loss with VANETs can be quite difficult as it can occur due to security threats. VANET is a wireless ad hoc network in mobile ad hoc networks (MANETs) that is subject to many attacks such as denial of service (DoS), black holes, gray holes, and ghost attacks. Researchers have developed various security mechanisms for secure routing through MANETs. Communication infrastructure (V2I) to initiate communication through which vehicles can communicate with each other (V2V) or through. A solution needs to be created to prevent the connection between these two types of communication. This paper describes a security approach that identifies and mitigates existing security threats.

Keyword: *Authentication, Confidentiality, Attack, VANET, Replay.*

1. INTRODUCTION

Vehicular ad hoc networks (VANETs) aim at enhancing safety and efficiency in transportation systems. They com- prise network nodes, that is, vehicles and road-side infrastructure units (RSUs), equipped with on-board sensory, processing, and wireless communication modules. Vehicle-to-vehicle (V2V) and vehicle-to infrastructure (V2I) communication can enable a range of applications. Among these, primarily safety will be enabled, as numerous research and development initiatives indicate, by vehicles frequently beaconing their position, along with warnings on their condition or environment. Nonetheless, VANETs can be vulnerable to attacks and jeopardize users' privacy. For example, an attacker could inject beacons with false information, or collect vehicles' messages, track their locations, and infer sensitive user data. To thwart such attacks, security and privacy-enhancing mechanisms are necessary or, in fact, a prerequisite for deployment.
Following are the security issues for VANET:
• Data Authentication: Applications can broadcast the safety messages over VANET and it is quite complex to identify the authentic message and its source as the vehicles can change the lane frequently. Fake message flooding can consume the entire bandwidth of the network. So there should be a provision to identify/authenticate the entities i.e. vehicle and driver etc.
• Data Integrity: Transmitted data over an open channel may be intercepted and altered. So there must be a mechanism to ensure the data integrity at the receiver's end.
• Data Availability: Due to obstacles and attacks, alerts cannot be forwarded to vehicles, so there should be a way to identify/rectify the actual cause of interruption.
• Data Confidentiality: Transmitted data should not be accessible to unauthorized vehicles but use of shared channel acts as a security hole for confidential data.
• Non-repudiation: Entities can alter their identities and deny the message transmission. There must be a method to recognize the objects involved in transmission but vehicle and driver and the passengers, all are different entities and can easily deny the transactions.
Common attacks for VANET are Worm/Black/Gray hole, Sybil attack, DoS, DDoS, Spoofing, fabrication and signal jamming etc. In this paper, security solution protects the routing information through Dos attack which is explained below:

1.1 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.

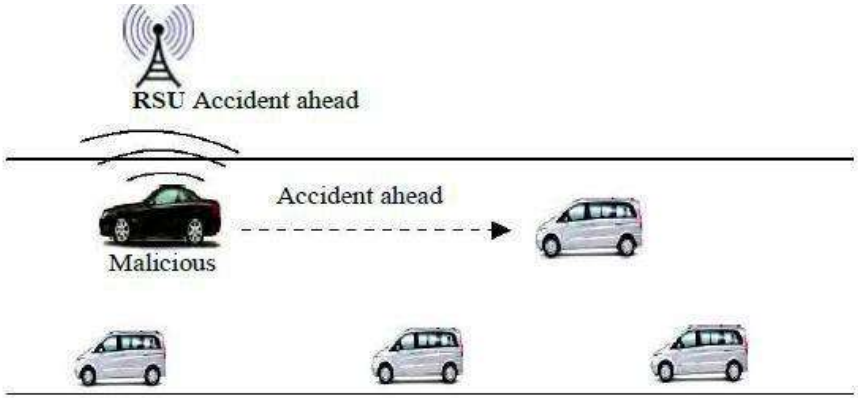

Figure 1: Denial of Service Attack

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.

2. LITERATURE SURVEY

Amrita Chakraborty et al. "Swarm Intelligence: A Review of Algorithms," This paper describes the study of insect and animal based algorithms. This is the analysis of way in which these algorithms operate. The specified areas for these protocols have been introduced after the analysis of inspiration. Specific areas where these algorithms can be applicable have been highlighted. Swarm intelligence is an integral part of the artificial intelligence. This study is providing the basic concept of the technical aspects and the future scope of algorithms [23].

Ahmad Shaheen et al. "Comparison and Analysis Study between AODV and DSR Routing Protocols in VANET with IEEE 802.11b," In this paper, the AODV and DSR are performed in a VANET over two distinct situations. Both protocols are performed individually by different tasks and then evaluated the performances of both protocols. As we know that MANET is a class of VANET. The protocols which are used in MANET can be used in VANET but not directly with some modification [24].

Tareq Emad Ali et al. "Review and Performance Comparison of VANET Protocols: AODV, DSR, OLSR, DYMO, DSDV & ZRP," This paper is providing the brief study of ad- hoc protocols for routing that are being used in a Vehicular ad-hoc network. The vehicular network is providing communication among the vehicles that are moving on roads. The protocols that are being used for communication are being affected by the high speed of vehicles which is leading to the path breaks. The main motive of a vehicular network is the assembly of data system in vehicles which are moving on the roads. In this paper routing protocols has been compared on the basis of a delivery ratio of packets, delay, throughput etc [25].

L. Bariah et al. investigated the recently developed security provisions for VANET. Investigation covers various threats (Repudiation, Wormhole, Spamming, Replay, Jamming, DoS, DDoS and Black Hole etc.), issues and remedies. Study shows that threats can be categorized on the basis of V2V and V2I. It also compares the various simulation tools i.e. NCTUns, NS-2, Qualnet, GrooveNet and TraNs etc. [5]

A. Singh et al. developed an algorithm to identify the DoS attack over VANET, called EAPDA. It uses time slots and Threshold values. Communication gap is used to identify the intruder nodes. Finally, entire network is isolated from detected threat. Simulation results show that it enhances the Throughput of the network and does not produce False alarms[6].

R. Saranya et al. conducted a survey of the DDoS and Wormhole attack and compared various existing prevention schemes. Study shows that FireCol method can reduce the intensity of the attack over network whereas Traffic Matrices can be used to monitor the traffic for P2P based applications. Use of Bloom filters can protect the routing information. Survey also includes the comparison of these methods[7].

3. 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.

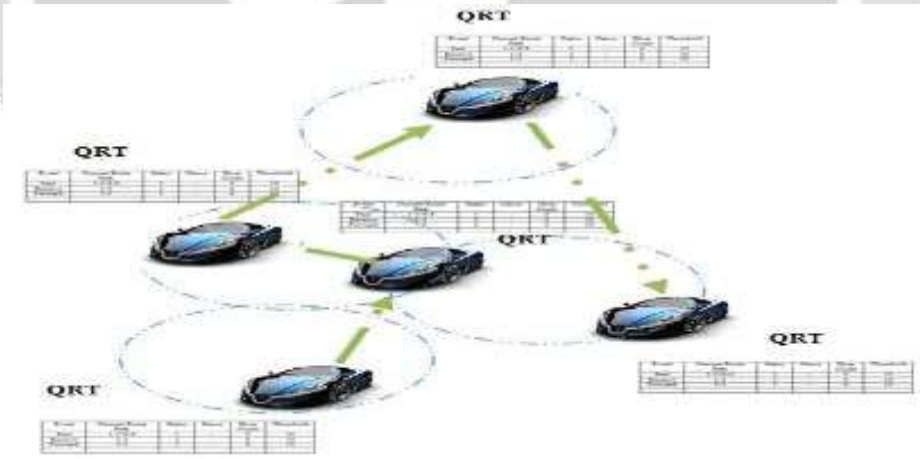

Figure 2: QRT for routing

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

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.

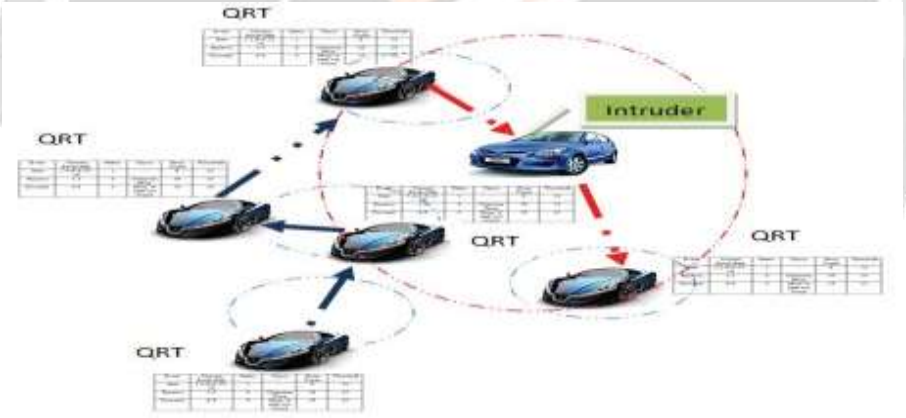

Figure 3:. QRT response for DoS attack

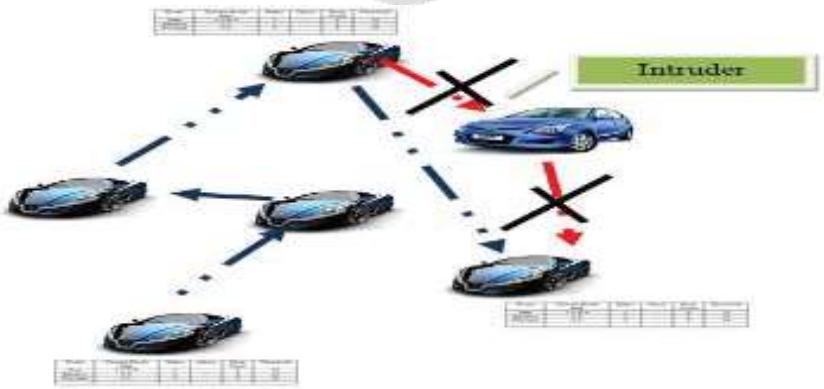

Figure 4: Route building by isolating the malicious node using QRT

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);
}
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)
}
        }
```

5. 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

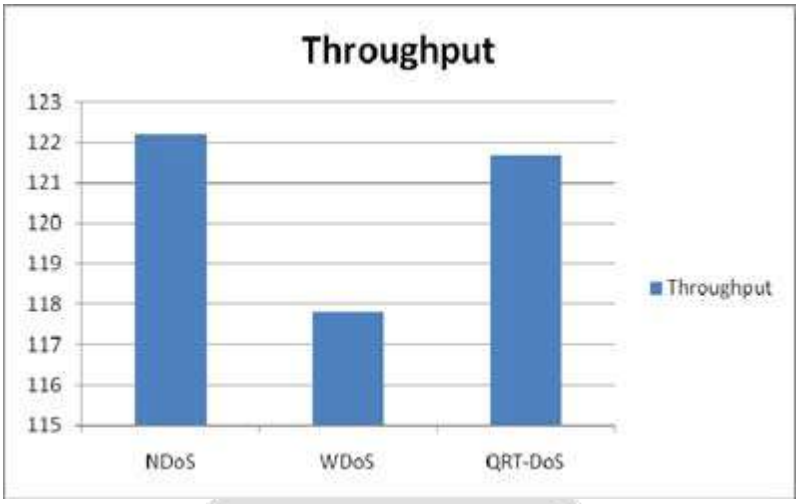

Figure 4.1: Throughput

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.

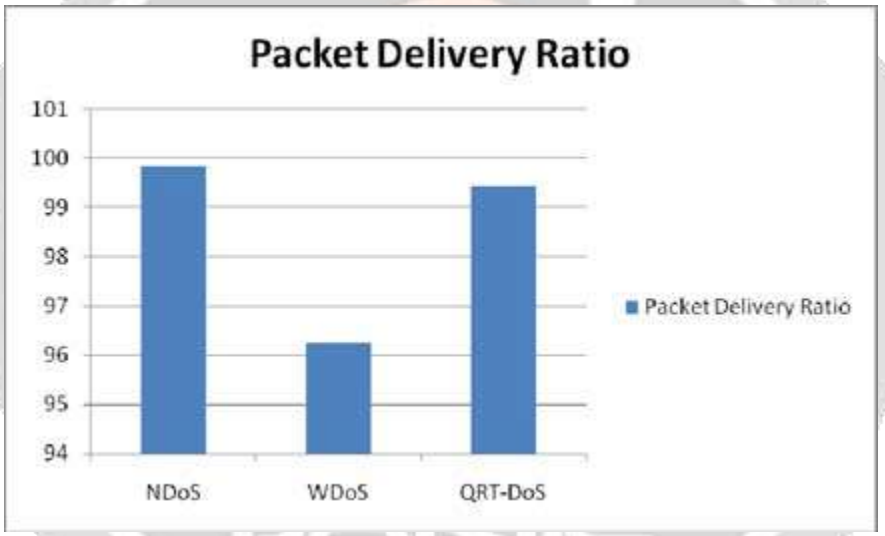

Figure 4.2: Packet Delivery Ratio

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.

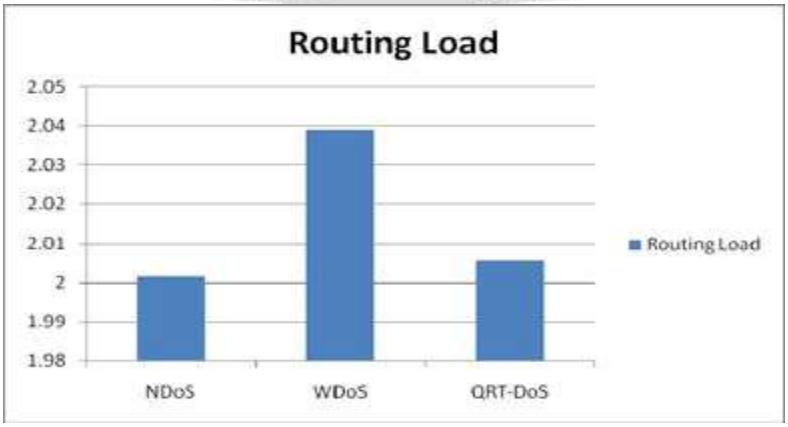

Figure 4.3: Routing Load

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.

Figure 4.4: End to End Delay

5. CONCLUSION

We have proposed a scheme was proposed to secure the VANET from DoS, using Quick Response Tables (QRT) which can analyze the frequent updates in routing information and uses a reference table. If any node acts as an intruder, then its status is saved in QRT table for future use. Finally, all nodes are informed about this Log and it is further used for route maintenance to avoid the entries of malicious nodes. Security analysis shows that packet drop at earlier stages is considered as normal packet drop but at a later stage, on the basis of QRT Logs, large scale packet drop can be identified easily, thus resulting in the isolation of intruder from routing table. QRT maintains a reference of each event at current routing path and once a Log for a specific node is created, identified node is ignored by neighbors and finally, QRT prevents the entire network from DoS attack. Simulation results show the intensity of DoS attack over VANET, as it is increasing Routing Load and reducing Throughput/PDR. QRT performed well by detecting the DoS attack efficiently and it can also be observed that QRT recovers the network performance. It enhances the Throughput/PDR and reduces the routing load and Delay. Proposed scheme can be extended to eliminate the DDoS attack over VANET using different protocols

6. 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.

[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.