International Journal of Research Publication and Reviews, Vol (5), Issue (10), October (2024), Page – 1690-1697

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

SecureVehicle Ad hoc Networks from Denial of Service Attack using unprecedented method

Nayan Prajapati[1], Dr. Harsh Lohiya[2], Dr.SudeshChouhan[3]

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

ABSTRACT

Due to the mobility of VANET's, secure routing is a primary issue. because of its dynamic nature, modifications are regular and can also be problem to community outages because of boundaries along with homes, tunnels and bridges. Intermittent connections can purpose packet loss, that may result in terrible network performance. figuring out the motive of packet loss with VANETs may be quite difficult as it can occur due to protection threats. VANET is a wi-fi ad hoc community in mobile ad hoc networks (MANETs) this is subject to many attacks which includes denial of carrier (DoS), black holes, grey holes, and ghost attacks. Researchers have developed various security mechanisms for relaxed routing thru MANETs. communique infrastructure (V2I) to initiate verbal exchange thru which automobiles can communicate with every other (V2V) or through. a solution desires to be created to save you the relationship among those two forms of verbal exchange. This paper describes a protection approach that identifies and mitigates existing safety threats.

Keyword: Bandwidth, Denial of Service, Spoofing, Fabrication,Jamming.

1. Introduction

Vehicular adhoc networks (VANETs) aim at improving protection and performance in transportation systems. They com- prise network nodes, this is, motors and road-aspect infrastructure devices (RSUs), prepared with on-board sensory, processing, and wireless conversation modules. automobile-to-car (V2V) and vehicle-to infrastructure (V2I) verbal exchange can permit a number programs. among those, ordinarily safety can be enabled, as numerous research and improvement initiatives indicate, via automobiles regularly beaconing their position, along with warnings on their situation or environment. nonetheless, VANETs can be susceptible to assaults and jeopardize users' privateness. for instance, an attacker ought to inject beacons with fake data, or gather vehicles' messages, track their places, and infer sensitive user data. To thwart such assaults, safety and privacy-improving mechanisms are necessary or, in reality, a prerequisite for deployment.

Security issues for VANET are as follows:

- 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.
- Commonplace attacks for VANET are computer virus/Black/gray hollow, Sybil attack, DoS, DDoS, Spoofing, fabrication and sign jamming and so on. on this paper, security solution protects the routing information thru Dos attack that's explained beneath:

1.1 Denial of Service (DoS) Attack

The most risky assault inside the community is Denial of service (DOS) attack. In DOS attack (fig. 1) dummy or faux nodes are created to transmits fake messages like "course ahead is closed. It stops the verbal exchange between car-to-car and vehicle-to-infrastructure. This sort of assault is finished to reduce the performance and overall performance of the machine [48]. within the state of affairs given below the malicious node transmit the wrong

facts to RSU (roadside unit) that path is not to be had in advance in order that RSU offers or transmit the incorrect statistics to the opposite nodes that are behind the attacker node.

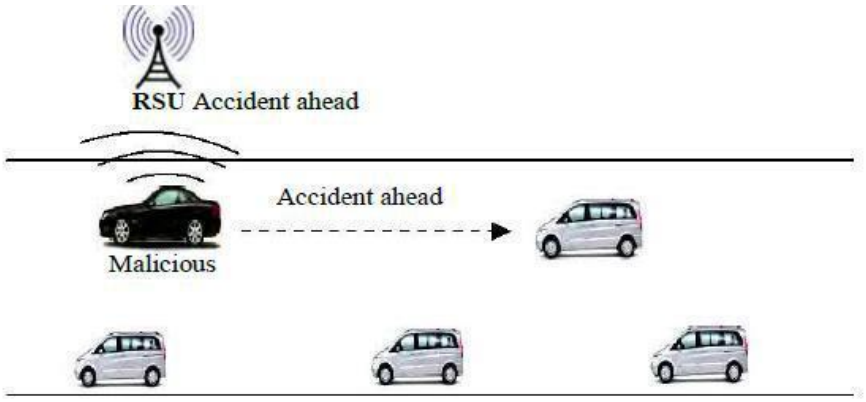

Fig. 1: Denial of Service Attack

In case of Dos assault, intruder intercepts the channel and brings down the to be had community sources by means of following:

• aid consumption: Intruder can consume the available bandwidth by means of injecting faux messages for this reason ensuing in congestion over network and degrading the stop person's revel in.

• sign Jamming: an outsider 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 agree with gadget for Detecting Selective Forwarding assaults in VANETs," in this paper, they are running at the selective forwarding assault in which malicious nodes acts as a everyday node by means of making the consider based totally system

1) Mutual tracking is used for finding the attacks among nodes by way of using the local and worldwide statistics.

2) Detection of attacker node based upon odd or horrific riding styles of malicious nodes.

when you consider that both in-band and out-band information is used. VANET is a high natural portability and takes data, to share the statistics among specific vehicles. Selective forwarding attack, are the assault wherein masquerade nodes acts as normal nodes which drop the statistics packets, damage the actual form of information and damages the legitimacy of actual VANETs packages. it's miles very difficult to acquire the selective forwarding assault because the attacker node constantly acts as a regular node and try and conflict with every different on every occasion they want to exchange the integrity of information and in order that damage occur within the VANET gadget.

2. Literature Survey

AmritaChakraborty et al."Swarm Intelligence: A evaluate of Algorithms," This paper describes the look at of insect and animal based totally algorithms. this is the analysis of manner in which those algorithms function. the specified areas for these protocols had been brought after the analysis of thought. specific areas wherein those algorithms may be relevant had been highlighted. Swarm intelligence is an fundamental part of the synthetic intelligence. This study is supplying the basic idea of the technical aspects and the destiny scope of algorithms [23].

AhmadShaheenetal.“assessment and evaluation look at among AODV and DSR Routing Protocols in VANET with IEEE 802.11b," in this paper, the AODV and DSR are done in a VANET over two wonderful conditions. both protocols are finished in my view through different duties after which evaluated the performances of each protocols. As we recognize that MANET is a category of VANET. The protocols which are used in MANET may be used in VANET but now not immediately with a few modification [24].

TareqEmadAliet al."Review and Performance ComparisonofVANET Protocols: AODV,DSR,OLSR,DYMO,DSDV&ZRP,"Thispaperisproviding thebriefstudy ofad- hocprotocolsforrouting thatarebeingusedinaVehicularad-hocnetwork.Thevehicular networkisproviding communicationamong thevehiclesthatare moving onroads.The protocolsthatarebeingusedforcommunicationarebeing affectedby thehighspeedof vehicleswhichisleading tothepathbreaks.Themainmotiveofavehicularnetworkisthe assembly ofdatasysteminvehicleswhicharemovingontheroads.Inthispaperrouting protocolshas beencomparedonthe basisofadelivery ratioofpackets,delay,throughputetc[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. advanced an algorithm to discover the DoS assault over VANET, known as EAPDA. It uses time slots and Threshold values. communique hole is used to discover the intruder nodes. sooner or later, complete community is isolated from detected hazard. Simulation results show that it complements the Throughput of the network and does now not produce fake alarms[6].

R. Saranya et al. conducted a survey of the DDoS and Wormhole attack and as compared diverse current prevention schemes. study indicates that FireCol method can reduce the depth of the assault over network while site visitors Matrices may be used to reveal the site visitors for P2P primarily based applications. Use of Bloom filters can guard the routing statistics. Survey additionally includes the contrast of these methods[7].

3. Proposed Work

Allroutinginformation isloggedaspertheeventsoccurred overnetwork.Ifthereisanypacketdropatanyspecificroute anditscauseisunknown, itsdropcount isincremented automaticallyandafterreachinga Thresholdvalue,current pathisisolatedfrom network,ifnodeisdrooping thepacket, withoutanyvalidreason.

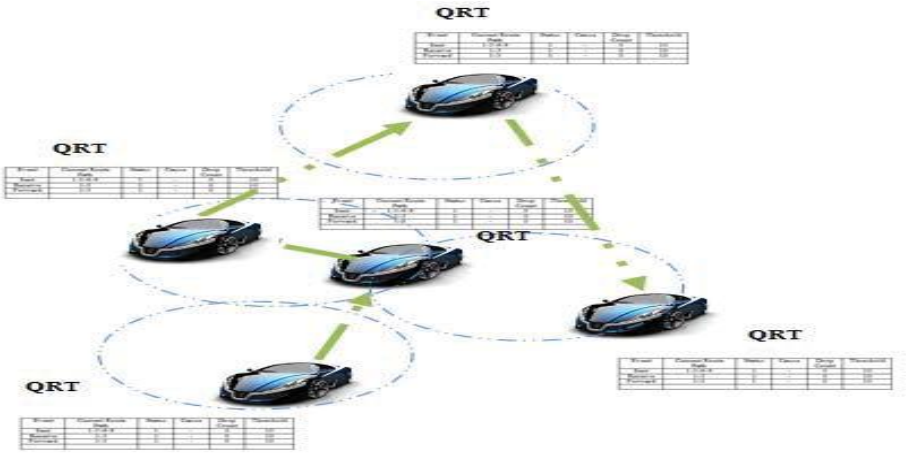

Fig. 2:QRT for routing

During route maintenancephase, usingQRT,identified routesandnodesareignoredandcannotbeconsidered for routingpurpose.

Table1:QRTforroutinginformationanalysis

Event(s)	Current RoutePath	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

Table2:QRTfordosdetection

Event	Current Route Path	Status	Cause	Drop Count	Threshold
Sent	1-3-6-9-12-18	1	-	6	10
Receive	1-3	0	Unknown Drop	39	10
Forward	6-9	0	Drop,if pathnot found	19	10

Table2aboveshowsthatthereisahugepacket dropat routepath1-3anditsreason isknownwhereasforroute6-9, packets aredropped duetoinvalid pathinformation. SoQRT assumesthatroute1-3hasbeencompromised andthereisa needtoisolatethisfromnetwork.

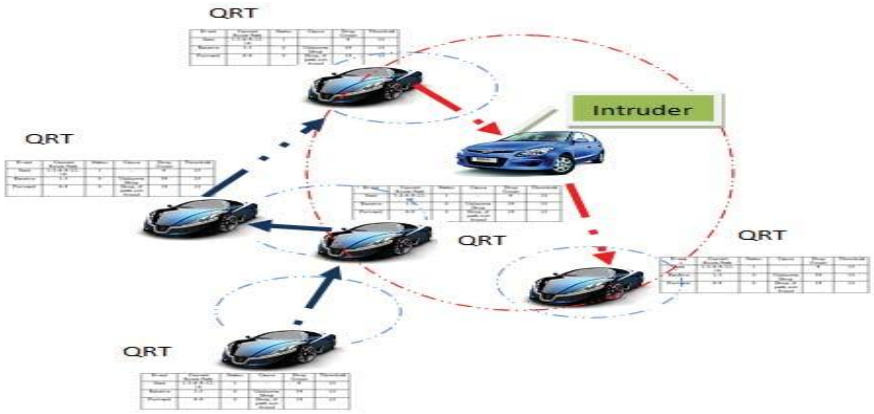

Fig 3:.QRT response for DoSattack

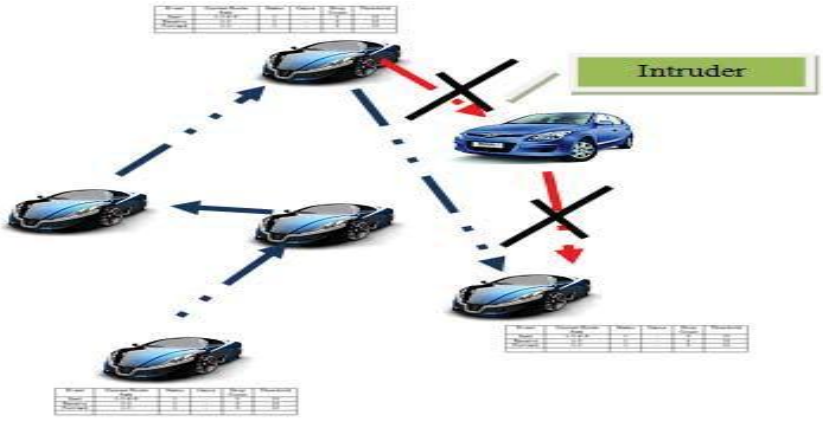

Fig.4:Route buildingbyisolating themaliciousnodeusing QRT

AlgorithmtodevelopQRT:

EventUsed:

S:=PacketSent; D:=PacketDrop;
R:=PacketReceived; F:=PacketForward;
DCount:PacketDropCount; Cr:=Get_Info(CurrentRoute)
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);
}
}

RouteMaintenance:

RouteMaintenance()
{ Ifexists(node->ID,QRT)
{ FindRoute(node->ID)//maliciousnodes
DeleteRoute(node->ID) // Delete entry malicious nodes fromexistingroutes
AvoidRoute(node->ID)//Avoidmaliciousnodesforroute selection
} else{ Addroute(node->ID)
}
}

4.Result Analysis

To research the effectiveness of the proposed approach in protecting against VANET's DoS attacks, the simulation on a topology become achieved the usage of network Simulator version (NS 2.35)

Table 3: 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 (CompromisedNetwork) c. QRT: DoS: Quick Response Tables forDoS attack

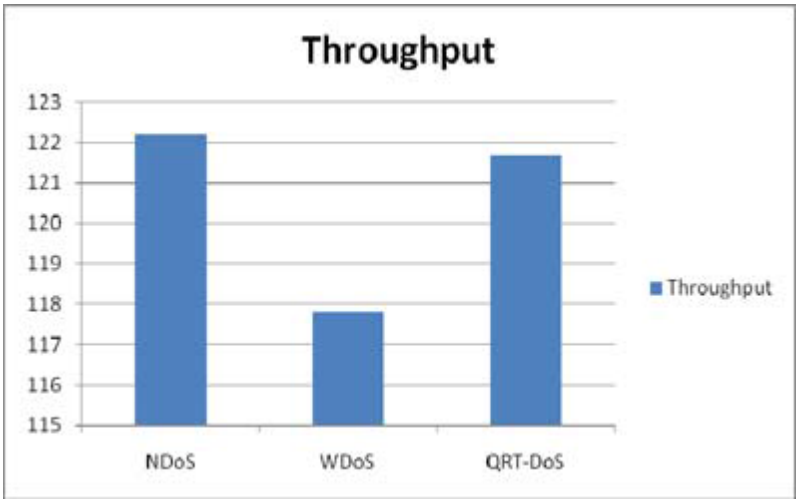

Fig. 4.1: Throughput

Fig. 4.1 above explains the effect of DoS attack (WDoS) in Throughput of DSR protocol. It could be determined that without QRT, Throughput is very minimum and with QRT Throughput enhanced.

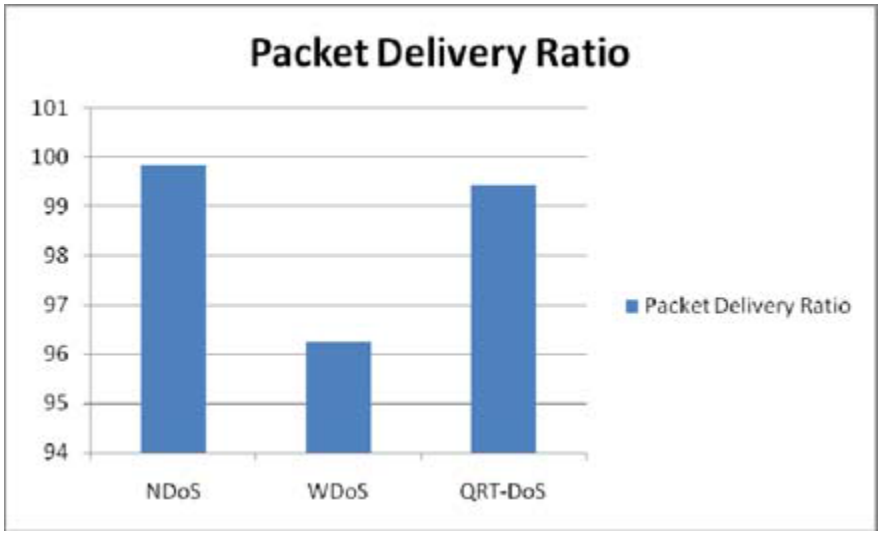

Fig. 4.2: Packet Delivery Ratio

Fig. 4.2 above expresses the effect of DoS attack (WDoS) in PDR. It could be determined that without QRT, PDR is very minimum and with QRT PDRenhanced.

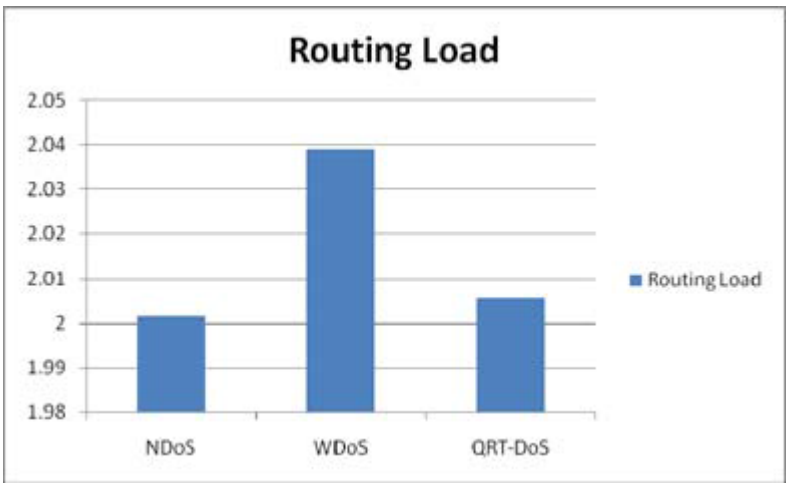

Fig. 4.3: Routing Load

Fig. 4.3 expresses the effect of DoS attack (WDoS) in routing load. It could be determined that without QRT, routing load is maximum and with QRT, routing load reduced.

Fig. 4.4 expresses the effect of DoS attack (WDoS) in Delay. It could be determined that without QRT, delay rises and QRT minimize delay.

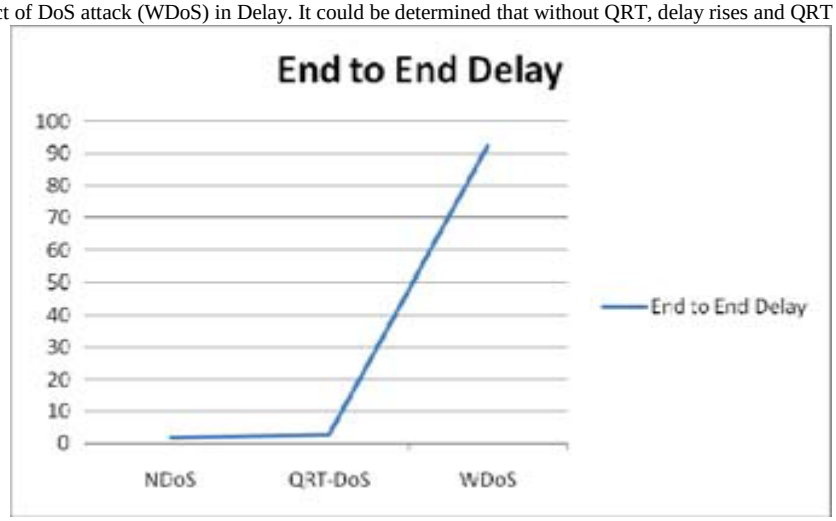

Fig. 4.4: End to End Delay

5. Conclusion

Wehaveintroducedan innovative approach to secure the VANET from DoS, by using Quick Response Tables (QRT) which continuously analyse the modification in routing tablewith comparison of reference table. If any node behave as an intruder, then its popularity is stored in QRT desk for future use. subsequently, all nodes are knowledgeable approximately this Log and it is in addition used for course renovation to avoid the entries of malicious nodes. safety analysis suggests that packet drop at in advance degrees is considered as everyday packet drop but at a later level, on the premise of QRT Logs, big scale packet drop can be identified without difficulty, hence ensuing inside the isolation of intruder from routing desk. QRT maintains a reference of each event at modern-day routing route and once a Log for a selected node is created, diagnosed node is ignored via pals and finally, QRT prevents the whole network from DoS assault. Simulation effects display the depth of DoS assault over VANET, as it's miles growing Routing Load and reducing Throughput/PDR. QRT finished well by using detecting the DoS attack efficiently and it could also be discovered that QRT recovers the network overall performance. It enhances the Throughput/PDR and decreases the routing load and put off. Proposed scheme may be extended to get rid of the DDoS attack over VANET the usage of one of a kind 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. RezazadehBaee, 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, EhabSalahat and Chan YeobYeun, "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.SenthamaraiKannan,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.WangandY.He,“ATrustSystemforDetectingSelectiveForwardingAttacksin VANETs,”Springer InternationalPublishing Switzerland, 2016, vol.4,pp. 377–386.

[9] M.KaurandM.Mahajan,“ProtectionAgainstDDOSUsingSecureCodePropagation InTheVANETs,”AnInternationalJournalofEngineeringSciences, 2016,vol.17, no. 1, pp. 573–577.

[10]K.Lim,“SecureandAuthenticated MessageDisseminationinVehicular adhoc NetworksandanIncentive-BasedArchitecture forVehicular Cloud,”2016,vol.19, pp. 1-104.

[11] A.Info,“DesignandAnalysisofSecureVANETFrameworkpreventingBlackHole andGrayHoleAttack,” InternationalJournalofInnovativeComputerScience & Engineering**,** 2016**,** vol. 3, no. 4, pp. 9-13.

[12] M.N.Mejri,NadjibAchir,MohamedHam,"ANewSecurityGames Based Reaction Algorithm against DOS Attacks in VANETs", 13th IEEE Annual Consumer Communications &Networking Conference (CCNC), pp.837 – 840, 2016.

[13] G.Kumaresan,T.AdilineMacriga,"GroupKey Authentication scheme for VanetINtrusiondetection (GKAVIN)", Wireless Networks, Springer,pp1–11,2016.

[14] FarhanJamil,AnamJavaidTariqUmer,MubashirHusain Rehmani"A comprehensive survey of networkcoding invehicular ad-hocnetworks", Wireless Networks,Springer,pp1–20,2016.

[15] M. J. Faghihniya, SeyedMojtabHosseiniMaryam Tahmasebi, "Security upgradeagainstRREQfloodingattackby using balanceindex onvehicularadhocnetwork",WirelessNetworks,Springer,pp.1–12,2016.

[16] S.Ibrahim,MohamedHamdy,EmanShaaban,"AProposedSecurityServiceSetforVANETSOA",SeventhInternationalConferenceonIntelligentComputingand InformationSystems(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. RezazadehBaee, 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.ChakrabortyandA.K.Kar,"Swarm Intelligence :AReviewof Algorithms," SpringerInternational PublishingAG,2017, vol. 10, pp. 475–494
[24] A.Shaheen,"ComparisonandAnalysisStudybetweenAODVandDSRRouting ProtocolsinVANETwithIEEE,"Journal ofUbiquitousSystems&Pervasive Networks,2016, vol. 7, no. 12, pp. 7-12.
[25] T. E. AliandL. A. Khalil, "Review and Performance Comparison of VANET Protocols:AODV,DSR,OLSR,DYMO,DSDV &ZRP,"Al-SadeqInternational ConferenceonMultidisciplinaryinIT andCommunicationScienceandApplications (AICMITCSA),2016, vol. 5, pp. 1-6.