www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 7 Issue 7 July 2018, Page No. 24109-24118
Index Copernicus Value (2015): 58.10, 76.25 (2016) DOI: 10.18535/ijecs/v7i7.02

An efficient adaptive neuro-fuzzy system based attack detection technique for VANETs

Manpriya Kaur[1], Dr. Tejpreet Singh[2]

KCET, ASR, India
TPO, KCET, ASR, India

Abstract
Vehicular Ad-hoc Networks (VANETs) are generally accepted as an exceptional type of Mobile Ad hoc Network (MANET). VANETs have seen tremendous growth in last decade, providing a vast range of uses in both military as well as civilian activities. The temporary connectivity in the vehicles can also increase the driver's capability on the road.
In this paper, an efficient data dissemination approach is proposed which not only improves the vehicle to vehicle connectivity but also improves the QoS between the source and the destination. The effectiveness of the proposed approach is demonstrated when it comes to the significant gets achieved in the parameters namely, end to end delay, packet loss ratio, average download delay and throughput in comparison with the existing approaches.

Introduction

Vehicular Ad-hoc Networks (VANETs) are generally accepted as an exceptional type of Mobile Ad hoc Network (MANET). In VANET each vehicle acts as a move to alter data between nodes in the network. It is essential with regard to vehicle-to-vehicle (V2V) and infrastructure-to-vehicles (I2V) communication. These networks are usually within traffic management applications, basic safety applications, driver guidance and location centered services. Within VANETs electricity consumption and storage-space are not limited and the position of the nodes may be determined by utilizing GPS [2]. VANETs offer special features such as high mobility while using the confinement associated with the road topology, originally lower current market insertion percentage, unbounded multilevel sizing, infrastructure support which vary them through MANET. From the above described features, it's observed that traditional MANET routing protocols have issues to find the stable routing paths in VANET environment [3].

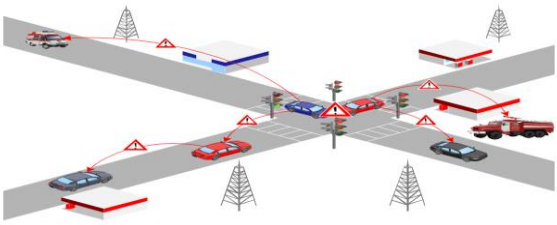

Fig 1: VANETs scenario

VANETs are generally part regarding MANET referred as a new age group regarding ad-hoc networks [4]. To obtain the actual connection VANET, every automobile usually a node which can behave equally like receiver and sender and hereby broadcasts various information regarding the vehicles. Within the networks, the automobiles include wireless terminals specifications with sending limit extendable up to 1000m. Due to constrained radio range of each and every node in VANETs, it is necessary to re-broadcast the actual obtained information message for your neighbors [5].
This type of sending is called multi-hop and requires routing algorithms. Routing in VANETs is very complicated and difficult because of some characteristics like high dynamism, high speed of vehicles and high broadcasting scale of information and the old routing methods are not

sufficient in these networks [6]. Inside multi-hop transmitting, the actual obtained limit associated with a message is gradually expanded. However, the actual rapid growing associated with the number of nodes re-broadcasting the solution brings the solution associated with the broadcast storm in broadcasting of associated information [7].

VANETs consist of the following entities:

1. **Access point:** The actual access points tend to be fixed as well as are generally connected to the internet.
2. **Vehicle:** Vehicle is usually nodes associated with the vehicular network. VANET addresses the particular wireless communication between the vehicles (V2V) and between vehicles and infrastructure access point [9].

Characteristics of VANETs

1. **High Mobility:** The particular nodes obtained in VANETs move with an extremely high speed. These transferring nodes may be protected from problems along with basic safety threats provided that their location will be predictable. Large moving ability leads to various other issues throughout VANET [10].
2. **Time Critical:** Timely delivery of information is extremely essential. Actions could be performed accordingly only when information can be acquired if it is required
3. **Frequent changing information:** Ad-Hoc nature of VANET motivates the nodes to gather information from other automobiles and road side units. As automobiles move and change their path, information linked to traffic and environment also changes very rapidly.
4. **High computability ability:** Because of computational resources and sensors, the computational capacity of the node is increased.

Types of Vehicular Communication Systems

1. Vehicle–to-Vehicle (V2V) Communication

a) The vehicle-to-vehicle (V2V) communication platform is really a typical research topic, with many different approaches. Many approaches exist, each with a significantly different focus.

b) Vehicle-to-vehicle (V2V) communications comprises an instantaneous network where automobiles send messages along with information regarding what they're doing. This kind of data would include speed, location, direction of travel and insufficient stability. Vehicle-to-vehicle technology uses dedicated short-range communications (DSRC).

c) It uses two kinds of broadcasting.
   i. Naive broadcasting
   ii. Intelligent broadcasting

2. Vehicle-to-Infrastructure (V2I) Communication

a) The V2I protocol represents a practical solution for many applications to bridge the inherent network fragmentation that exists in almost any multi-hop network formed over moving vehicles through expensive connectivity infrastructure [15].

b)Vehicle-to-Infrastructure (V2I) Communications for Safety could be the wireless exchange of critical safety and operational data between vehicles and roadway infrastructure, intended primarily to prevent motor vehicle crashes [16].

a) It has higher data transfer link with automobile and roadside equipment.

b) Roadside units transmit messages.

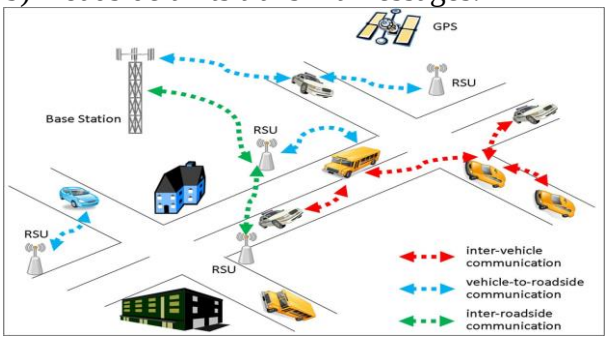

Fig 2: Communication in vehicular network [17]

3. Vehicle-to-Roadside Unit (V2R) Communication

a) Within the V2R link vehicles may easily communicate having fixed infrastructure together with the path system to be able to give particular person transmission plus data companies

b) It needs to be noted that the architecture does not depend across the infrastructure to be able to function but rather exploits the item to further improve the system overall performance.

c) The cross-network significance the actual lifestyle of the two vehicles and as well as roadside equipment [17].

Routing Attacks in VANETs

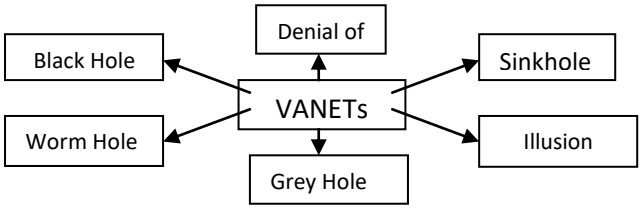

Fig 3: Routing Attacks in VANETs

In this type of attack, the attacker either drops the packet or disturbs the routing process of the network. Following are the most common routing attacks in the VANET.

1. Black hole attack

A black hole is an area where the network traffic is redirected. However, either there is no node in that area or the nodes reside in that area refuse to participate in the network. In a black hole attack, a malicious node introduces itself for having the shortest path to the destination node and thus, cheats the routing protocol [2].

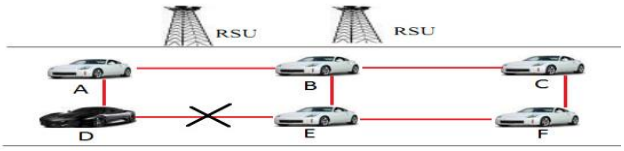

Fig 4: Black Hole Attack [2]

2. Wormhole attack

In this attack, an adversary receives packets at one point in the network, tunnels them to another point in the network, and then replays them into the network from that point. This tunnel between two adversaries are called wormhole [1].

3. Grey hole attack

This is the extension of black hole attack. In this type of attack the malicious node behaves like the black node attack but it drops the packet selectively.

4. Denial of service (DOS) attack

This type of attack can be done by the network insiders & outsiders. An insider attacker may jam the channel after transmitting dummy messages & thus, stops the network connection [12]. An outsider attacker can launch a DOS attack by repeatedly disseminating forged messages with invalid signatures to consume the bandwidth or other resources of a targeted vehicle. The impact of this attack is that, VANET losses its ability to provide services to the legitimate vehicles [18]. Figure 10 shows the whole scenario when the attacker A launches DOS attack in vehicular network and Jams the whole communication medium between V2V and V2I. As a result, authentic users (B, C, and D) cannot communicate with each other as well as with infrastructure.

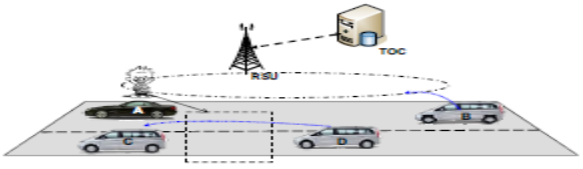

Fig 5: DOS Attack between V2V and 2I

5. Illusion attack

In this attacker tries to purposely manipulate his/her sensor readings for giving falsifies information about his/her vehicle. As a result, the system reaction invokes and false traffic warning messages are broadcast to neighbors. The impact of this attack is that it can easily change the driver's behavior by spreading the wrong traffic information & can cause accidents; traffic jams and reduces the vehicular network efficiency by dropping the bandwidth consumption. Existing message authentication & message integrity approaches cannot secure networks against this attack as the malicious vehicle directly manipulates & misleads the sensors of its own vehicle to produce & broadcast the wrong traffic information [8].

6. Sinkhole attack

In Sinkhole attack, a malicious vehicle broadcasts the fake routing information so that it can easily attract all the network traffic towards it. The impact of this attack is that it makes the network complicated and degrades the network performance either by modifying the data packets or by dropping them [1]. Figure illustrates a Sinkhole attack in which a malicious vehicle drops the data packets received from a legitimate vehicle & broadcasts fake routing information to the legitimate vehicles behind it.

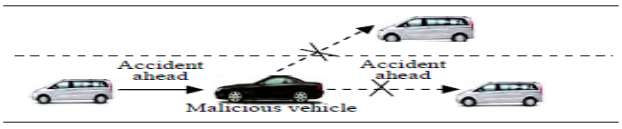

Fig 6: Sinkhole attack

Literature Survey

Terri, et al., (2017) [5] designed two collaborative-based approaches i.e. Group Reputation (GR) and Cooperative Detection (CD). Both techniques have ability to detect malicious nodes at MAC-layer in VANETs. Both approaches outperform over the available techniques for detecting the Distributed Denial of Service (DDOS) attacks only. However, performs poorly especially in case of wormhole and grey hole attack detection.

Bittl, et al., (2017) [18] implemented a novel data retrieval approach for improving the robustness of backbone to DDOS attacks and reduced the size of nodes' request messages. Thus, designed approach has better throughput compared to earlier approaches. Because the packet size is quite less compared to earlier DDOS attack detection ratio.

Muthumeenakshi, et al., (2017) [16] implemented an Extended Three-Party Password based Authenticated Key Exchange (E-3PAKE) approach. It has priority based applications which addresses the end to end security issue in available approaches. E-3PAKE concentrates on a server-client safety protocol and batch message communication to enhance the accuracy of attack detection techniques.

Mehdi, et al., (2017) [13] proposed a game theory based safety approach for VANETs. This technique is based on an attacker and defender security game to monitor and detect the malicious vehicles. This approach has ability to detect the DDOS attack in more efficient way compared to earlier approaches.

Safi, et al., (2017) [14] designed a secure end to end vehicular communication protocols which allows only authentic vehicles to transmit the data between vehicles. Thus, it prevents the unauthorized vehicles to communicate with authenticated devices and vehicles. However, this technique fails whenever any kind of attack occurs in the VANETs.

Hasrouny, et al., (2017) [7] demonstrated an improved attack prediction technique. This technique can predict several kinds of VANETs attacks. Due to its complex methodology this approach comes up with potential overheads. Thus, it is not so efficient for real time applications.

Wu, et al., (2016) [6] proved that network coding is widely utilized in the broadcasting approaches of VANETs because network coding has ability to enhance the packet delivery ratio. But, it will bring pollution attack into the network, making the decoding process error. Therefore, vehicles are unable to recover the actual information. Thus, a signature based approach is required to validate a section without decoding.

Dietzel, et al., (2013) [8] implemented three graph-based measures to measure the redundancy of VANET routing techniques. These measures are applied on geocast protocol. Experimental results have proved that the proposed technique behaves almost optimally from a routing effectiveness. But it fails to provide satisfactory redundancy for information consistency approaches in several scenarios.

Zaidi, et al., (2016) [9] implemented an intrusion detection system (IDS) for VANETs. IDS can be determined using the existence of rogue nodes (RNs) which can initiate several VANETs attacks. The designed approach has ability to monitor a false data attack by considering statistical approaches effectively and can also monitor other kinds of attacks.

Baiad, et al., (2016) [17] designed a cross-layer cooperative schemes for detecting black hole attack that commonly targets the quality of service secure optimized link state routing protocol (QoS-OLSR) in vehicular ad-hoc networks (VANETs). The QoS-OLSR relies mainly on the multi-point relays (MPRs) that are responsible for establishing the routing among the nodes in the network.

Safi, et al., (2009) [1] introduced an efficient method to prevent wormhole attack in vehicular ad hoc networks and detect malicious nodes as far as possible. Authors used packet leashes and new method of authentication called HEAP. Also, some correction has been done on packet leashes method.

Quyoom, et al., (2015) [15] proposed Malicious and Irrelevant Packet Detection Algorithm (MIPDA) which is used to analyze and detect the Denial-of Service (DoS) attack. As a result, the attack is eventually confined within its source domains, thus avoiding wasteful attack traffic overloading the network infrastructure. It also reduces the overhead delay in the information processing, which increases the communication speed and also enhances the security in VANET.

7.PROBLEM FORMULATION

The review has shown that the most of the existing techniques have neglected at least one of

the following issues while detecting the attack in existing environment.

1. The utilization of adaptive neuro-fuzzy system techniques such as neural networks, support vector machines, neuro-fuzzy systems are ignored by the majority of existing VANETs researchers.
2. Majority of existing protocols are based upon certain specific attacks only like DDOS based attack detection, Sybil attack detection, Wormhole attack detection, Black hole attack detection etc. Thus, in such kind of protocols researchers assumed that only one kind of attack exist at a time.
3. The use of the historical information of VANETs is ignored while detecting the attacks, which can be beneficial to detect malicious nodes in more promising manner.

Problem Definition

VANETs have potential to change the system. Individuals travel through the formation of a safe interoperable wireless transportations system which comprises different vehicles, mobile phones, traffic signals etc. But, VANETs are susceptible to safety threats due to cumulative dependence upon transmission, computing, and control mechanisms. Therefore, securing the end to end communication in VANETs becomes a major area of research. Many researchers have proposed several security protocols so far to improve the integrity, confidentiality, no repudiation, access control, etc. to provide secure VANETs to its users. Therefore, the overall goal of security protocols of VANETs is to recognize malicious nodes in the network by using suitable mechanism.

In this work trustworthiness of VANETs will be improved. Adaptive neuro-fuzzy system tools will frequently monitor the behavior of VANETs nodes and evaluate some malicious nodes. It will be able to monitor the attack even in complex environment.

Objectives

1. To study and evaluate the performance of some well-known recently proposed security protocols for VANETs.
2. To design and implement adaptive neuro-fuzzy system based attack detection techniques for VANETs.
3. To evaluate the security effect of network scalability issue in terms of nodes and network area for secured VANETs.
4. The comparison will be drawn between existing, and proposed protocols based upon the following parameters: -
   a) Packet loss rate
   b) End to End delay
   c) Accuracy
   d) Average download delay
   e) Packet collisions
   f) Throughput (KB/s)

Methodology/Planning Of Work

Methodology

To do research we will use MATLAB (version13a). It is a High-level language which is utilized for numerical calculation, representation, and application improvement. It has an Interactive domain for iterative investigation, configuration and critical thinking. It gives backing to recreation of TCP, directing, and multicast conventions over all systems remote. It provides support for simulation of TCP, routing, and multicast protocols over all VANETs networks.

The proposed convention performs in wired and remote systems. In this we will build a adaptive neuro-fuzzy system approach which incorporates a lot of versatile operators in the pursuit space. The adaptive neuro-fuzzy system based approach will have the ability to detect multiple attacks in VANETs by using various adaptive neuro-fuzzy system approaches.

Planning of Work

Steps taken in developing the proposed technique are:

Step1: Generate the new catalog in MATLAB with any name where we can put our protocol.

Step2: Append the different records like packet, routing and configuration in the new catalog.

Step3: Initialize the system.

Step4: Organize network arbitrarily in defined VANETs field.

Step5: Apply adaptive neuro-fuzzy system approaches to assess the multiple attacks in VANETs.

Step6: Evaluate the effect of network range and node scalability on the proposed adaptive neuro-fuzzy system based attack detection for VANETs

Step7: Compare the proposed technique with existing attack detection protocols based upon different quality metrics. Record the data & run

the simulation code for wireless & wired networks.

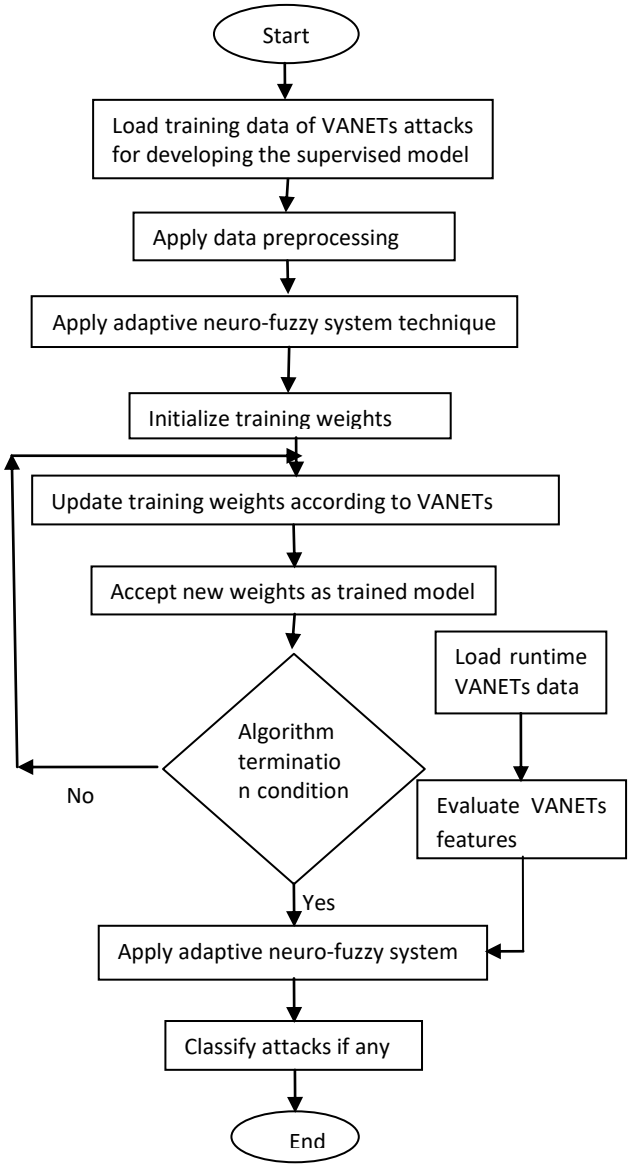

Fig. 7**:** Flowchart of the Proposed Technique

Performance Analysis

In order to assess the efficiency and competence of the proposed technique, MATLAB based simulation is done for VANETS coding organizations. The existing and proposed techniques are implemented on a Windows (2.4 GHz Intel i7 processor with 4 GB RAM and 1 TB memory). Table 5.1 has shown various different constants and variables essential for simulating the work. It has been observed that proposed technique outperforms existing technique in terms of Packet loss rate, End to End delay, Accuracy, Average download delay, Packet collisions, Throughput (KB/s). These parameters are generally standard values utilized as standard for VANETS. To be able to implement the proposed algorithm, design and implementation have been done.

Table 5.1: Experimental Setup

Parameter	Value
Level_of_agg	1:5
Speed_of_vehicle	10:10:50
D	50:50:150
N	50
min1	20
max1	80
oint1	8
oint2	12
simu_time	10

Comparison Parameters

This section represents the comparison between some well-known differential evolution based attack detection techniques with the proposed technique. To evaluate the following metric using proposed mechanism as well as to compare the performance of our technique on basis of following parameters with previous results:-

1. Packet Lost Rate

Package damage occurs when number packages of internet data over a laptop fail to get to their particular destination. Package damage can be calculated as a percentage of package damage rates as compared to the package sent. Packet loss is obtained by subtracting the number of packets received at Access Point from the total number of packets transmitted.

$$\text{Packets losts} = \Sigma\text{Packets transmited} - \Sigma\text{Packets received}$$

$$\text{Packet loss ratio} = \frac{(\text{Packets losts} * 100)}{\Sigma\text{Packets transmitted}}$$

Table 5.2: Packet Loss Ratio

Nodes	Existing	Proposed
10	8.4870	1.1525
11	12.2827	1.6642
12	16.5684	1.6616
13	15.7667	1.3213
14	20.4004	1.4243
15	21.5670	2.4539
16	27.3978	2.5293
17	26.6482	1.8382
18	31.1083	2.6266
19	31.7433	2.0434
20	32.7473	2.9476

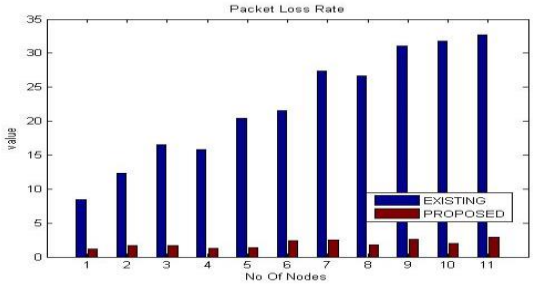

Fig 8**:** Represent the packet loss rate

Fig.5.1 demonstrates the analysis of Packet Lost Rate among the pre-existing and our proposed technique. In this figure, red line represents the proposed technique and blue line represents the previous one.

In our case the proposed Packet Lost Rate are reasonably lower than the existing one.

2. End To End Delay

This metric represents the average delay experienced by the received data packet to reach the destination. The formula to calculate E2ED is given as:

$$End\ to\ End\ Delay = \frac{1}{\sum_{i=1}^{n} R_i}\left(\sum_{i=1}^{n}\sum_{j=1}^{R_i} TR_{ij} - TS_{ij}\right)$$

Where TR_{ij} the receiving time of j[th] packet is sent by the i[th] source at the destination and TS_{ij} is the sending time of j[th] packet sent by the i[th] source.

Table 5.3: End to End Delay

Nodes	Existing	Proposed
10	18.2603	8.5906
11	18.4545	8.4840
12	16.3155	9.8048
13	19.1041	11.3192
14	18.8489	9.5159
15	20.8950	13.0368
16	15.4380	15.5012
17	19.9668	12.9163
18	25.3951	14.5636
19	18.2977	12.8010
20	23.4653	13.5800

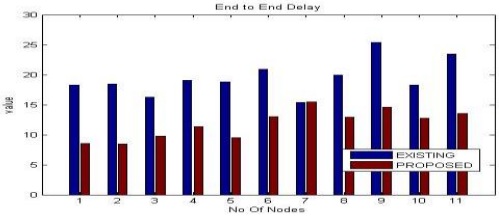

Fig 9**:** End to end delay

Fig 9 demonstrates the comparison of End to end delay among the pre-existing and the proposed technique. In this figure the red colored lines represents the proposed technique and blue colored lines represents the pre-existing technique. In our scenario the proposed End to end delay is reasonably lower than existing one.

3. Accuracy

Accuracy is the proportion of true results among number of cases. Accuracy is the depiction of proximity of an amount to the true value. Accuracy describes systematic errors. When this is practical to sets of dimensions, it involves a constituent of random error and a constituent of systematic error. Accuracy is also called as rand accuracy or rand index. Accuracy is measured with respect to reality. Accuracy is calculated by following equation. In which truepositive (TP), truenegative (TN) and falsepositive (FP), falsenegative (FN) is considered for the calculation.

$$Accuracy = (truepositive + truenegative)/(truepositive + trueneagtive + falsepositive + falsenegative) \times 100$$

Table 5.4: Accuracy

Nodes	Existing	Proposed
10	10.2603	8.5906
11	17.4545	8.4840
12	16.3155	9.8048
13	14.1041	11.3192
14	19.8489	9.5159
15	24.8950	13.0368
16	18.4380	15.5012
17	22.9668	12.9163
18	24.3951	14.5636
19	18.2977	12.8010
20	22.4653	13.5800

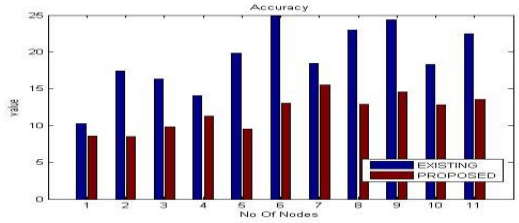

Figure **10:** Represent the Accuracy

Figure 10 demonstrates the comparison of Accuracy among the pre-existing and the proposed technique. In this figure the red colored lines represents the proposed technique and blue colored lines represents the pre-existing technique. In our scenario the proposed Accuracy is reasonably lower than existing one.

4. Average Download Delay

It represents the time spent during the receiving of packet. It is basically the difference between packet arrived at node and the time packet is extracted at that node.

$$Average\ Download\ Delay = \frac{\sum_{i=1}^{N} PAT_i - PET_i}{N}$$

where PAT_i is Packet arrived time and PET_i is packet extracted time

Table 5.5: Average Download Delay

Nodes	Existing	Proposed
10	18.2496	8.5843
11	18.4433	8.4776
12	16.3043	9.7990
13	19.0925	11.3131
14	18.8365	9.5097
15	20.8826	13.0304
16	15.4253	15.4946
17	19.9536	12.9070
18	25.3802	14.5568
19	18.2843	12.7928
20	23.4501	13.5717

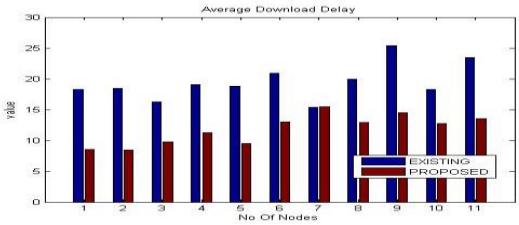

Fig 11**:** Represent the Average Download delay

Fig 11 demonstrates the comparison of Average Download delay among the pre-existing and the proposed technique. In this figure the red colored lines represents the proposed technique and blue colored lines represents the pre-existing technique. In our scenario the proposed Average Download delay is reasonably lower than existing one.

5. Packet Collision

A significant number of packets collide with the neighboring packets due to limited availability of communication bandwidth or congestion. This metric is defined as the ratio of the unsuccessful transmissions from the vehicle to the total number of sent packets over CCH.

$$\mathbf{CR(Collision\ Rate)} = \frac{\mathbf{Unsucessfull\ Transmission}}{\mathbf{\Sigma Total\ number\ of\ sent\ packet}}$$

Table 5.6: packets collision

Nodes	Existing	Proposed
10	.635	.159
11	.836	.163
12	.427	.142
13	.404	.166
14	.405	.14
15	.478	.135
16	.482	.133
17	.519	.134
18	.512	.134
19	.509	.134
20	.635	.159

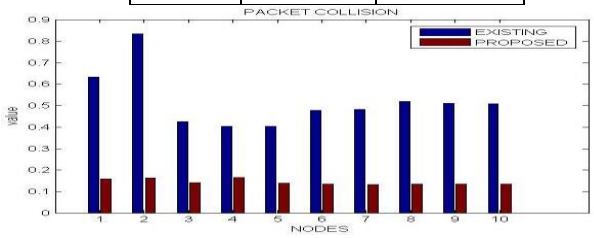

Fig 12**:** Represent the packets collision

Fig 12 demonstrates the comparison of packets collision among the pre-existing and the proposed technique. In this figure the red colored lines represents the proposed technique and blue colored lines represents the pre-existing technique. In our scenario the proposed packets collision is reasonably higher than existing one.

6. Throughput

It is defined as the time average of the number of bits that can be transmitted by each node to its destination is called the per node throughput. The sum of per-node throughput over all the nodes in a network is called the throughput of the network. The throughput is obtained by dividing the total number of packets received by the total time taken for simulation

$$\mathbf{Throughput} = \frac{\mathbf{(received\ packets * packet\ size)}}{simulation\ time}$$

Throughput of the network is inversely proportional to the average delay between source and destination. Throughput of the network can also be estimated as follows:

$$\mathbf{Throughput}(T_h = \frac{ETT.(n+1).L}{nR})$$

where R is transmission range, n is number of neighbors in the direction of destination node and ETT (Expected Transmission Time) is used to maximize the throughput of the path by measuring the link capacities and would increase the overall performance of the network. ETT is defined as

$$ETT = \frac{S}{L(1-p)}$$

where S is the size of a packet and L is the bandwidth of the link and p is the probability to deliver a packet successfully.

Table 5.7: Throughput

Nodes	Existing	Proposed
10	11.5130	14.8475
11	9.7173	15.9358
12	7.4316	17.5384
13	10.2333	19.4787
14	7.5996	20.9757
15	8.4330	21.5461

16	4.6022	23.0707
17	7.3518	25.3618
18	4.8917	26.1734
19	2.2567	28.3566
20	7.2527	29.0524

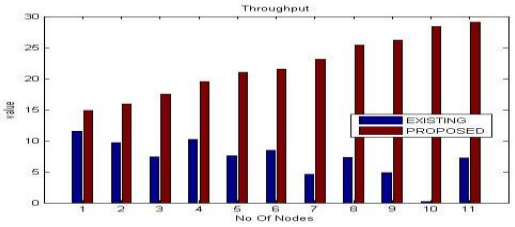

Fig **13:** Represent the throughput

Fig 13 demonstrates the comparison of throughput among the pre-existing and the proposed technique. In this figure the red colored lines represents the proposed technique and blue colored lines represents the pre-existing technique. In our scenario the proposed throughput is reasonably higher than existing one.

Conclusion and Future Scope

Vehicular ad hoc networks (VANETs) have seen tremendous growth in last decade, providing a vast range of uses in both military as well as civilian activities. The temporary connectivity in the vehicles can also increase the driver's capability on the road. However, such applications require heavy data packets to be shared on the same spectrum without the requirement of excessive radios. Thus, efficient approaches are required which can provide improved data dissemination along with the better quality of services to allow heavy to be easily shared between the vehicles.

In this paper, an efficient data dissemination approach is proposed which not only improves the vehicle to vehicle connectivity but also improves the QoS between the source and the destination. The proposed approach is examined and in contrast to the present state-of-the-art approaches. The effectiveness of the proposed approach is demonstrated when it comes to the significant gets achieved in the parameters namely, end to end delay, packet loss ratio, average download delay, through-put, and message dissemination rate in comparison with the existing approaches. Data dissemination is one of the key issues with the VANETs. While, a few strategies have been proposed through the years to provide effective data dissemination, yet provisioning of the quality of services is still an issue with these networks. Considering this, a novel approach is proposed in this paper which utilizes the properties of neural networks in collaboration with the fuzzy logic to provide efficient data dissemination. The proposed strategy is capable of providing successful data forwarding combined with the development in Quality of Services when compared with the existing approaches In future, the proposed approach will be further extended to accommodate different scenarios by following rural, highway, suburban and urban conditions.

References

[1] Safi,Seyed Mohammad,Ali Movaghar and Misagh Mohammadizadeh."A novel approach for avoiding wormhole attacks in VANET."In *Computer Science and Engineering, 2009.WCSE'09.Second International Workshop on*,vol.2,pp.160-165.IEEE, 2009.

[2] Bibhu, Vimal, Roshan Kumar, Balwant Singh Kumar, and Dhirendra Kumar Singh. "Performance analysis of black hole attack in VANET." *International Journal of Computer Network and Information Security*, vol. 4, no. 11, pp. 47, 2012.

[3] C. Lai, K. Zhang, N. Cheng, H. Li and X. Shen, "SIRC: A Secure Incentive Scheme for Reliable Cooperative Downloading in Highway VANETs," in *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no. 6, pp. 1559-1574, June 2017.

[4] Chinnasamy, A., S. Prakash, and P. Selvakumari. "Enhance trust based routing techniques against sinkhole attack in AODV based VANET." *International Journal of Computer Applications*, vol. 65, no. 15, 2013.

[5] Doaa Al-Terri, HadiOtrok, Hassan Barada, Mahmoud Al-Qutayri, Yousof Al Hammadi, Cooperative based tit-for-tat strategies to retaliate against greedy behaviour inn VANETs, Computer Communications, Volume 104, 15 May 2017, Pages 108-118.

[6] Guowei Wu, Jie Wang, Yongchuan Wang, Lin Yao, Pollution Attack Resistance Dissemination in VANETs Based on Network Coding, Procedia Computer Science, Volume 83, 2016.

[7] HamssaHasrouny, Abed EllatifSamhat, Carole Bassil, Anis Laouiti, VANET security challenges and solutions: A survey, Vehicular Communications, Volume 7, January 2017.

[8] S. Dietzel, J. Petit, G. Heijenk and F. Kargl, "Graph-Based Metrics for Insider Attack Detection in VANET Multihop Data Dissemination Protocols," in *IEEE Transactions on Vehicular Technology*, vol. 62, no. 4, pp. 1505-1518, May 2013.

[9] K. Zaidi, M. B. Milojevic, V. Rakocevic, A. Nallanathan and M. Rajarajan, "Host-Based Intrusion Detection for VANETs: A Statistical Approach to Rogue Node Detection," in *IEEE Transactions on Vehicular Technology*, vol. 65, no. 8, pp. 6703-6714, Aug. 2016.

[10] Kim, Yeongkwun, Injoo Kim, and Charlie Y. Shim. "A taxonomy for DOS attacks in VANET." In *Communications and Information Technologies (ISCIT), 2014 14th International Symposium on*, IEEE, pp. 26-27., 2014.

[11] Lo, Nai-Wei, and Hsiao-Chien Tsai. "Illusion attack on vanet applications-a message plausibility problem." In *Globecom Workshops*, IEEE, 2007.

[12] Lyamin, Nikita, Alexey Vinel, Magnus Jonsson, and Jonathan Loo. "Real-time detection of denial-of-service attacks in IEEE 802.11 p vehicular networks." *IEEE Communications letters*, vol. 18, no. 1, pp: 110-113, 2014.

[13] Muhammad Mohsin Mehdi, Imran Raza, Syed Asad Hussain, A game theory based trust model for Vehicular Ad hoc Networks (VANETs), Computer Networks, Volume 121, 5 July 2017.

[14] Qamas Gul Khan Safi, Senlin Luo, Chao Wei, Limin Pan, Qianrou Chen, PIaaS: Cloud-oriented secure and privacy-conscious parking information as a service using VANETs, Computer Networks, Volume 124, 4 September 2017, Pages 33-45.

[15] Quyoom, Abdul, Raja Ali, Devki Nandan Gouttam, and Harish Sharma. "A novel mechanism of detection of denial of service attack (DoS) in VANET using Malicious and Irrelevant Packet Detection Algorithm (MIPDA)." In *Computing, Communication & Automation (ICCCA), 2015 International Conference on*, IEEE, pp. 414-419. 2015.

[16] R. Muthumeenakshi, T.R. Reshmi, K. Murugan, Extended 3PAKE authentication scheme for value-added services in VANETs, Computers & Electrical Engineering, Volume 59, April 2017.

[17] Raghad Baiad, Omar Alhussein, HadiOtrok, Sami Muhaidat, Novel cross layer detection schemes to detect black hole attack against QoS-OLSR protocol in VANET, Vehicular Communications, Vol. 5, pp. 9-17, 2016.

[18] Sebastian Bittl, Privacy conserving low volume information retrieval from backbone services in VANETs, Vehicular Communications, Volume 9, July 2017, Pages 1-7.