An Enhanced Approach for Attack Detection in VANETs Using Adaptive Neuro-Fuzzy System

Er. Jasleen Kaur
Department of Computer Science & Engineering
KCET, India
jasleen.aulakh87@yahoo.in

Dr. Tejpreet Singh
School of Computer Science & Engineering
Lovely Professional University
India
tejpreet.23874@lpu.co.in

Dr. Kamlesh Lakhwani
School of Computer Science & Engineering
Lovely Professional University
India
kamlesh.20980@lpu.co.in

***Abstract*-Vehicular Ad-hoc Networks (VANETs) are generally acknowledged as an extraordinary sort of Mobile Ad hoc Network (MANET). VANETs have seen enormous development in a decade ago, giving a tremendous scope of employments in both military and in addition non-military personnel exercises. The temporary network in the vehicles can likewise build the driver's capability on the road. In this paper, an effective information dispersal approach is proposed which enhances the vehicle-to-vehicle availability as well as enhances the QoS between the source and the goal. The viability of the proposed approach is shown with regards to the noteworthy gets accomplished in the parameters in particular, end to end delay, packet drop ratio, average download delay and throughput in comparison with the existing approaches.**

Keywords-VANETs, Routing Attacks, Packet Drop Ratio, End to End delay, Throughput.

I. 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].

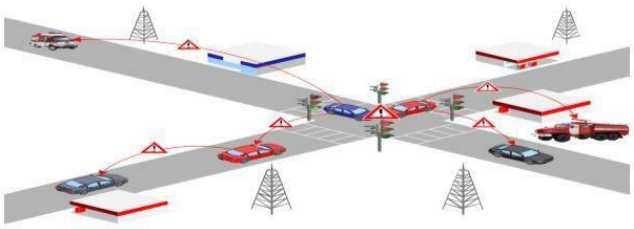

Fig. 1. VANETs Scenario [1]

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 neighbours [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:

a) Access point: The actual access points tend to be fixed as well as are generally connected to the internet.
b) 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].

II. RELATED WORK

Various researchers are trying to solve many problems that are underway in data dissemination in vehicular adhoc networks. There is a large quantity of challenges in VANET such as for example provisioning of QoS, high connectivity and bandwidth and security to vehicle and individual privacy. A few of the related issues to VANET are discussed. Network architecture, signal-modelling and propagation mechanism, mobility modelling, routing protocols and network security are number of them.

Kaur and Malhotra et al. [1] have carried a study on the selection of an appropriate routing approach in Nakagami propagation model over VANETs. With varying densities and size, the authors carried their analysis on the throughput, packet delivery ratio, routing load and end to end delay as network parameters. QoS based data dissemination is another aspect of networking with VANETs.

Terri et al. [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 gray hole attack detection.

Wu et al. [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.

Hasrouny et al. [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.

Rupareliya et al. [8] proved that the authentication of information plays a significant role in VANETs. Therefore, providing end to end security has become a significant role in VANETs. Watchdog and Bayesian filter-based attack detection and prevention technique is implemented to improve the attack detection rate.

Kaur et al. [9] proposed a strategy in which choice bundles used to identify the wormhole hubs in the system. What's more, to maintain the respectability of the parcels, hash estimation of every bundle is utilized. The source hub communicates the choice bundle to every one of the hubs in the wake of accepting the course answer message from the goal hub which contains the rundown of the course framing hubs. The choice bundles from the hubs are then assessed by the goal hub in view of the bounce check esteem. On the off chance that the bounce tally surpasses the edge esteem, it implies a wormhole is shaped between the hubs.

Zaidi et al. [10] 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.

Rizzo et al. [11] has talked about self-ruling composed driving in addition to in proactive security administrations, misusing the canny detecting and figuring assets which are probably going to be step by step penetrating the urban and vehicular conditions, is making provisioning of high assortment of QoS in vehicular systems a pressing issue. In the meantime, the spreading style of an incredible method to achieve auto, with bunches of infotainment applications, requires structures for vehicular correspondences exceptionally successful at supporting activity with various arrangement of execution prerequisites. As of now endeavours were rotated towards empowering some individual particular QoS level. Anyway, burdens of how-to help activity with tight QoS necessities (no parcel misfortune, and defers mediocre compared to 1ms), also outlining a framework competent in the meantime of effectively maintaining such movement together with movement from infotainment applications, keeps on opening.

Sharma et al. [12] with proficient steering, (WSNs) enhances lifetime with consistent transmission. Diverse steering conventions represent the distinctive outcomes over the WSNs. WSNs obtain exceptional place in cutting edge arrange applications, for example, body region systems, home liveliness, cell upgrade, and so on. Particularly, concentrating on the home robotization, a great deal of directing calculations and conventions has been proposed throughout the years that go for improving the lifetime of such systems. A portion of the well-known calculations incorporate RDSR, CR, RIDSR, and so forth. These conventions centre over tackling the steering circle issue alongside change in lifetime of the general system. In any case, the additions accomplished by these systems demonstrate a moderately less change. In this manner, thinking about the comparative issue of steering circle and a lifetime, a vitality productive directing calculation created on the foundation of the RIDSR is proposed. The proposed diverting calculation utilizes the closeness procedure to locate the right gathering of hubs for sign, therefore, enhancing life time and settling diverting snare issues. Intensity of the said Vicinity Centered Power Efficient Redirecting is appeared in as increments accomplished as far as enhanced life time, and vitality utilization.

S. Iadicicco et al. [13] Around the framework of the Vehicular Ad-Hoc Networks we propose HBEB (Hybrid Based Election Backbone), a distributed algorithm that can form multiple backbones of vehicles in command of propagating data during the VANETs in a rapid and efficient way. Differently from other clustering approaches we leverage the ETSI Geo networking recent standard to create and disseminate data in the backbones. We show that the formation of these backbones is quite easy to be implemented while their use enhances the dissemination performance in an urban scenario.

Mehdi et al. [14] 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. [15] 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.

Quyoom et al. [16] proposed a Malicious and Irrelevant Packet Detection Algorithm (MIPDA) which is utilized to examine and identify the Denial-of Service (DoS) assault.

Accordingly, the assault is in the long run kept to its source spaces, in this manner keeping away from inefficient assault traffic over-burdening the system foundation. It likewise lessens the overhead deferral in the data preparing, which builds the correspondence speed and furthermore upgrades the security in VANET.

Muthumeenakshi et al. [17] 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.

Baiad et al. [18] designed a cross-layer cooperative scheme 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.

M.Chaqfeh et al. [19] the authors focus on ETSI Geo networking standards to efficiently handle the forwarding over VANETs. Their approach is suitable for urban scenarios. But, the test of practicality is not carried on the real time. The authors focus on ETSI Geo networking standards to efficiently handle the forwarding over VANETs. Their approach is suitable for urban scenarios. But, the test of practicality is not carried on the real time. The authors have provided a novel strategy for data dissemination in multi-hop VANET. Their approach relies on the estimation to provide selective broadcast in vehicular networks. Their approach provides low overheads and high packet delivery ratio.

Oliveira et al. [20] proved that the cooperation among vehicles are required to improve the security of VANETs. An adaptive broadcast technique is proposed, which can deliver efficient end to end secure communication between vehicles. Typically, this technique utilizes several methods to dynamically regulate the attack detection rate.

Parul, and Deepak Dembla et al. [21] describes system for identification and anticipation of security assaults in routing conventions of vehicular specially appointed system (VANET) for explicitly black hole assault in VANETs.

III. Comparison of Various Routing Protocols

TABLE I. Comparison of Routing Protocols [19]

Protocols	*Proactive Protocols*	*Delay Bounded Protocols*	*Geo Cats Protocols*
Prior Forwarding Methods	Wireless Multi hop Forwarding	Carry & Forward	Wireless Multi Hop Forwarding
Realistic Traffic Flow	Yes	No	Yes
Digital Map Requirement	No	No	No
Recovery Strategy	Multi Hop Forwarding	Multi Hop Forwarding	Flooding
Virtual Infrastructure Requirement	No	No	No
Scenario	Urban	Sparse	Highway

IV. Proposed Solution to Detect Various Attacks in VANETs

Steps involved in developing the proposed technique in MATLAB tool:

Step 1. Generate the new catalog in MATLAB with any name where we can put our protocol.
Step 2. Append the different records like packet, routing and configuration in the new catalog.
Step 3. Initialize the system.
Step 4. Organize network arbitrarily in defined VANETs field.
Step 5. Apply adaptive neuro-fuzzy system approaches to assess the multiple attacks in VANETs.
Step 6. Evaluate the effect of network range and node scalability on the proposed adaptive neuro-fuzzy system-based attack detection for VANETs
Step 7. 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.

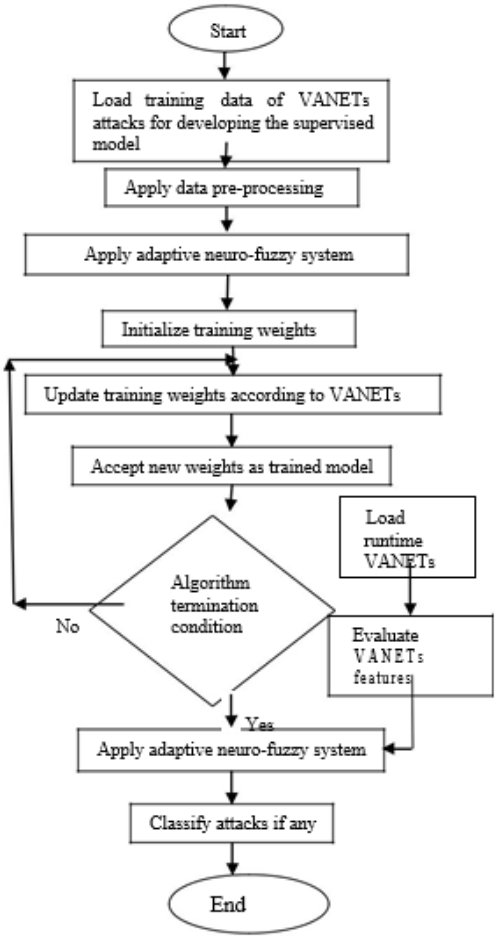

Fig. 2. Flow chart of proposed algorithm.

Facilities Required for Proposed Work

Hardware

- Hard Disk: 500 GB
- RAM: 4 GB
- Processor: Any Intel or AMDx86 processor
- Operating System: Windows7

Software

- MATLAB version 13a
- CD-ROM drive (for installation)
- Netscape Navigator 4.0 and above or Microsoft Internet Explorer 4.0 and above is required.
- Adobe Acrobat Reader 3.0 is mandatory to analyse and print the MATLAB online citations in PDF format.

V. Test Setup for Execution of Proposed Algorithm

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 (1.80 GHz Intel i3 processor with 4 GB RAM and 1 TB memory). It has been observed that proposed technique outperforms existing technique in terms of Packet loss rate, End to End delay, Average download delay, Throughput (KB/s). These parameters are generally standard values utilized as standards for VANETS. To be able to implement the proposed algorithm, design and implementation have been done.

Testing situation states of VANET in NCTUns:

1. A vehicular adhoc system is considered for learning.
2. The 30 m Lane Width is taken for vehicles.
3. The fundamental common division between two focus focuses amassed is 500 m.
4. 100 s accumulates as S.T.
5. 3000 bytes is given as RTS edge.

The mimicked focus focuses depend upon PHY/MAC systems. The vehicular structure situation is executed utilizing the Car Agent application. The re-enactment condition contains 18 focus focuses on 4-way street spread over a region of 1200 m. The commonplace speed 50 m/s with most unprecedented deceleration 1– 20 m for each Second Square in every condition. Table I displays the physical layer and channel show explicit of recreation condition.

TABLE II. Parametric Environment

Parameter	*Setting*
Total No. of Nodes	18
Attenuation Provided	50dBm
Average Node Speed	50 m/s
Min. Deceleration	1 m/s^2
Max. Deceleration	20 m/s^2
Simulation Time	100s

Performance Metrics

Different execution estimation and examination measurements exist that assess the convention productivity and execution in various rush hour gridlock situation in VANET condition. This work centers around throughput, parcel misfortune and crash rate parameters to explore the execution of VANET steering conventions [18].

a. Packet Loss

It is defined by subtracting the received packets from the packets transmitted.

Packets lost = (Σ Packets transmitted – Σ Packets received)

$$\textit{Packet Loss Ratio} = \frac{(Packets\ lost \times 100)}{\sum Packets\ transmitted}$$

TABLE III. Packet Loss Ratio

Nodes	*Existing*	*Proposed*
10	8.487	1.1525
11	12.283	1.6642
12	16.568	1.6616
13	15.767	1.3213
14	20.4	1.4243
15	21.567	2.4539
16	27.398	2.5293
17	26.648	1.8382
18	31.108	2.6266
19	31.743	2.0434
20	32.747	2.9476

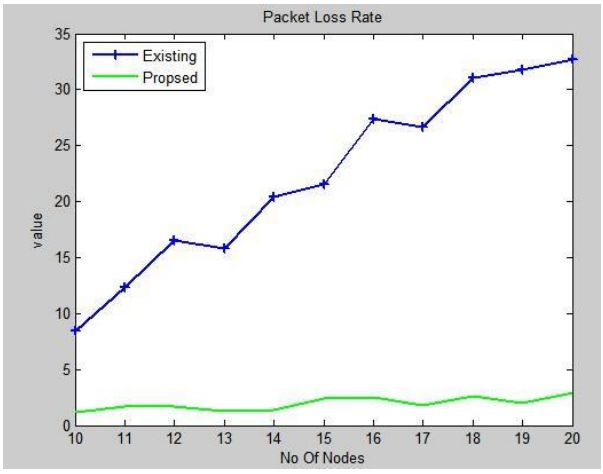

Fig. 3. Packet Loss Rate

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

TABLE IV. END TO END DELAY

Nodes	*Existing (ms)*	*Proposed (ms)*
10	18.2603	8.5906
11	18.4545	8.484
12	16.3155	9.8048
13	19.1041	11.3192
14	18.8489	9.5159
15	20.895	13.0368
16	15.438	15.5012
17	19.9668	12.9163
18	25.3951	14.5636
19	18.2977	12.801
20	23.4653	13.58

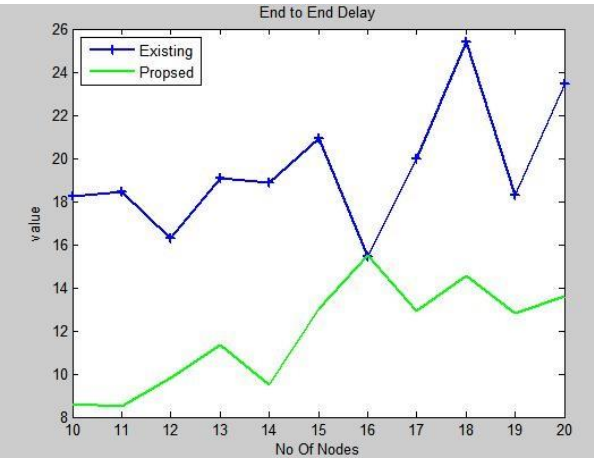

Fig 4. End to End Delay

Above graph demonstrates the comparison of End to end delay among the existing and the proposed technique. In this graph, the green colored line represents the proposed technique and blue colored line represents the existing technique. In our scenario the proposed End to end delay is reasonably lower than existing one.

c. 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 V. AVERAGE DOWNLOAD DELAY

Nodes	*Existing (ms)*	*Proposed (ms)*
10	18.2496	8.5843
11	18.4433	8.4776
12	16.3043	9.799
13	19.0925	11.3131
14	18.8365	9.5097
15	20.8826	13.0304
16	15.4253	15.4946
17	19.9536	12.907
18	25.3802	14.5568
19	18.2843	12.7928
20	23.4501	13.5717

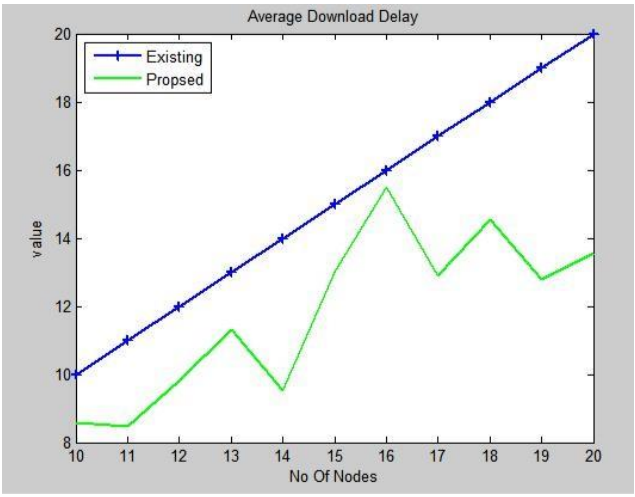

Fig. 5. Average Download Delay

Above graph demonstrates the comparison of Average Download delay between the existing and the proposed technique. In this graph, the green colored line represents the proposed technique and blue colored line represents the existing technique. In our scenario the proposed Average Download delay is reasonably lower than existing one.

d. Throughput

It is portrayed as the time typical of the amount of bits that can be transmitted by each center point to its objective is known as the per center point throughput. The entire of per-center point throughput over all of the center points in a framework is known as the throughput of the framework. The throughput is gotten by isolating the aggregate number of bundles gotten by the aggregate time taken for simulation.

$$Throughput = \frac{(recieved\ packets \times packet\ size)}{simulation\ time}$$

Throughput of the system is conversely relative to the normal deferral amongst source and destination. Throughput of the system can likewise be assessed as follows:

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

ETT (Expected Transmission Time) is utilized to boost the throughput of the way by estimating the connection limits and would build the general execution of the system. ETT is characterized as:

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

TABLE VI. THROUGHPUT

Nodes	*Existing*	*Proposed*
10	11.513	14.8475
11	9.7173	15.9358
12	7.4316	17.5384
13	10.2333	19.4787
14	7.5996	20.9757
15	8.433	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

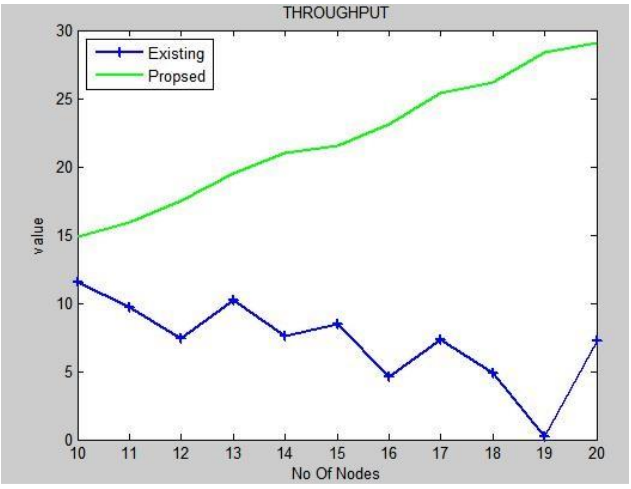

Fig. 6. Throughput

VI. CONCLUSION AND FUTURE WORK

Vehicular specially appointed systems (VANETs) have seen colossal development in a decade ago, giving a tremendous scope of uses in both military just as regular citizen activities. The impermanent availability in the vehicles can likewise build the driver's ability out and about. Be that as it may, such applications require substantial information bundles to be shared on a similar range without the prerequisite of over the top radios. In this way, productive methodologies are required which can furnish enhanced information spread alongside the better nature of administrations to enable overwhelming information to be effectively shared between the vehicles.

In this theory, a productive information scattering approach is proposed which enhances the vehicle to vehicle availability as well as enhances the QoS between the source and the goal. The proposed methodology is analyzed as opposed to the current situation with the-workmanship approaches. The adequacy of the proposed methodology is shown with regards to the importance. It gets accomplished in the parameters in particular, parcel misfortune proportion, end-end delay, normal download delay and throughput in correlation with the current methodologies. 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 thesis which utilizes the properties of neural optimization algorithm 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] Kaur, Aarja, and Jyoteesh Malhotra. "On the Selection of Efficient Back-off with QoS Aware Routing in VANET." *International Journal of Future Generation Communication and Networking* 9.2 (2016): 163-176.

[2] Bibhu, Vimal, et al. "Performance analysis of black hole attack in VANET." International Journal of Computer Network and Information Security 4.11 (2012): 47.

[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] A. Chinnasamy, S. Prakash, and P. Selvakumari PhD. "Enhance trust-based routing techniques against sinkhole attack in AODV based VANET." International Journal of Computer Applications (0975–8887) Volume (2013): 22-28.

[5] Al-Terri, Doaa, et al. "Cooperative based tit-for-tat strategies to retaliate against greedy behavior in VANETs." Computer Communications 104 (2017): 108-118.

[6] Wu, Guowei, et al. "Pollution Attack Resistance Dissemination in VANETs Based on Network Coding." Procedia Computer Science 83 (2016): 131-138.

[7] Hasrouny, Hamssa, et al. "VANET security challenges and solutions: A survey." Vehicular Communications 7 (2017): 7-20.

[8] J. Rupareliya, S Vithlani, C Gohel. "Securing VANET by Preventing Attacker Node Using Watchdog and Bayesian Network Theory." Procedia Computer Science 79 (2016): 649-656.

[9] H. Kaur, S Batish, and A. Kakaria. "An approach to detect the wormhole attack in vehicular adhoc networks." International Journal of Smart Sensors and Ad Hoc Networks (IJSSAN) ISSN 2248-9738 (2012): 86-89.

[10] Zaidi, Kamran, et al. "Host-based intrusion detection for vanets: a statistical approach to rogue node detection." *IEEE transactions on vehicular technology* 65.8 (2016): 6703-6714.

[11] Rizzo, Gianluca, et al. "Content and context aware strategies for QoS support in VANETs." *Advanced Information Networking and Applications (AINA), 2016 IEEE 30th International Conference on*. IEEE, 2016.

[12] Sharma, Vishal, Ilsun You, and Rajesh Kumar. "Energy efficient data dissemination in multi-UAV coordinated wireless sensor networks." *Mobile Information Systems* 2016 (2016).

[13] Iadicicco, Silvia, et al. "Multi-originator data dissemination in VANETs." *Wireless On-demand Network Systems and Services (WONS), 2016 12th Annual Conference on*. IEEE, 2016.

[14] Mehdi, Muhammad Mohsin, Imran Raza, and Syed Asad Hussain. "A game theory-based trust model for Vehicular Ad hoc Networks (VANETs)." *Computer Networks* 121 (2017): 152-172.

[15] Safi, Qamas Gul Khan, et al. "PIaaS: Cloud-oriented secure and privacy-conscious parking information as a service using VANETs." *Computer Networks* 124 (2017): 33-45.

[16] Quyoom, Abdul, et al. "A novel mechanism of detection of denial of service attack (DoS) in VANET using Malicious and Irrelevant Packet Detection Algorithm (MIPDA)." *Computing, Communication & Automation (ICCCA), 2015 International Conference on*. IEEE, 2015.

[17] Muthumeenakshi, R., T. R. Reshmi, and K. Murugan. "Extended 3PAKE authentication scheme for value-added services in VANETs." *Computers & Electrical Engineering* 59 (2017): 27-38.

[18] Baiad, Raghad, et al. "Novel cross layer detection schemes to detect black hole attack against QoS-OLSR protocol in VANET." *Vehicular Communications* 5 (2016): 9-17.

[19] Chaqfeh, Moumena, and Abderrahmane Lakas. "A novel approach for scalable multi-hop data dissemination in vehicular ad hoc networks." *Ad Hoc Networks* 37 (2016): 228-239.

[20] Oliveira, Renê, et al. "Reliable data dissemination protocol for VANET traffic safety applications." *Ad Hoc Networks* 63 (2017): 30-44.

[21] Tyagi, Parul, and Deepak Dembla. "Performance analysis and implementation of proposed mechanism for detection and prevention of security attacks in routing protocols of vehicular ad-hoc network (VANET)." *Egyptian Informatics Journal* 18.2 (2017): 133-139.