IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-6, Issue-3 E-ISSN: 2347-2693

Adaptive Neuro-fuzzy System based Attack Detection Techniques for VANETS

Sahil Nayyar[1*], Anita Suman[2], Parveen Kumar[3]

[1] Dept.ECE, Beant College of Engineering and Technology, Gurdaspur, India
[2] Dept.ECE, Beant College of Engineering and Technology, Gurdaspur, India
[3] Dept.ECE, Beant College of Engineering and Technology, Gurdaspur, India

Available online at: www.ijcseonline.org

Received: 17/Feb//2018, Revised: 23/Feb2018, Accepted: 18/Mar/2018, Published: 30/Mar/2018

***Abstract*—**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, nonrepudiation, access control, etc. to provide secure VANETs to its users. Therefore, the overall goals of security protocols of VANETs are to recognize malicious nodes in the network by using suitable mechanism. In this work trustworthiness of VANETs has been improved by using some well-known adaptive Neuro-fuzzy system tools to detect the attacks in more efficient manner. Adaptive Neuro-fuzzy system tools have been used frequently to monitor the behavior of VANETs nodes and evaluate some malicious nodes based upon already developed model using historical knowledge of the same network. Since, training of the model is based upon the various features of VANETs nodes therefore, it is able to monitor the attack even in complex environment. Extensive analysis indicates that the proposed protocol outperforms others in terms of Packet Loss Ratio, Throughput, End to End Delay and Average Download Delay. .

***Keywords*—** VANET, Adaptive neuro-fuzzy system, Attacks, Malicious nodes.

I. INTRODUCTION

In this time private vehicles as well as transport vehicles such as car, scooter, motorcycles, truck, buses that are general utilized by incredible number of people. The significant issue is the quantity of sufferers rising because of the highway accidents that will be brought due to more utilization of transport [1], according to the World Health Organization, number of people expire every year across the world due to vehicle collisions on the highway, about 50 thousands of people indignant in vehicular incidents[2],

Therefore researchers of computer networking area planned a notion of wireless networks called VANETs that are categorized as a specific form of MANETs. With the emergence of MANETs, researchers conceptualized the scheme of connecting vehicles giving growth to VANETs that are the important topic for engineers working to turn cars into intelligent technology which commune for security as well as comfort purposes. It is independent as well as self-organizing wireless communication network, where nodes in VANET occupy themselves as servers or clients for exchanging as well as sharing data.

A VANET is created by vehicles which can be built with wireless communication devices, positioning systems, as well as digital maps. In VANETs, a packet could be relayed from a car to another by the way of direct forwarding or carry as well as forwarding. VANETs also permit vehicles for connecting to RSUs that are linked to the Internet as well as are often interconnected with one another with a mesh network.

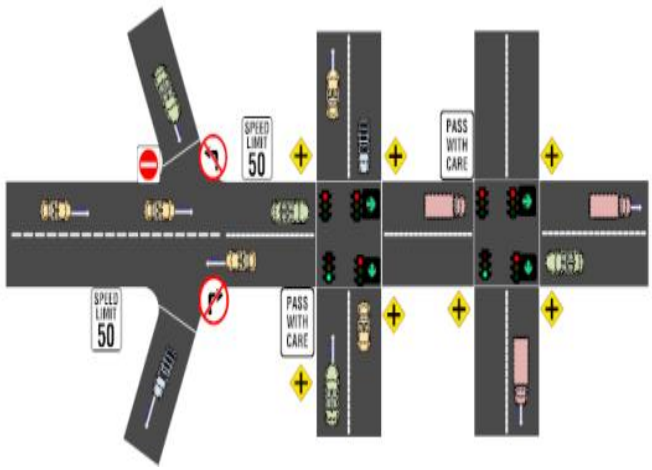

Figure 1. An Illustration of the VANETs

VANET may be the powerful technology which could give reliable vehicle to roadside infrastructure (V2I) communication and vehicle to vehicle (V2V) [1]. VANETs

are tend to be auto configuring network exactly where nodes are vehicle as well as WIFI technological innovation are helpful to confirm these kind of network [3],[4]. VANETs contain On Board Units (OBUs) and Roadside Units (RSUs).

A. Vehicular ad hoc networks

A promising area for the application of MANET is in the automotive sector. An individual vehicle generates a lot of self-contained information, available only to that particular vehicle. Vehicular Ad-hoc Networks (VANET) is a special category of MANETs which is composed of moving vehicles, acting as nodes. VANET is aimed at increasing inter-vehicular communication, so that information collected in a vehicle can be shared with other vehicle users, with the aim of improving driving experience. VANET nodes take on the role of sender, receiver and router to broadcast information to the vehicular network. They do not require any infrastructure and use On-Board Units (OBU) and Road Side Units (RSU) like traffic signals and base stations for communications.

Figure 2. Vehicular communication in VANETs

Vehicles can collect the essential information and share it with other vehicles. This information can be related to the traffic jam situation, road condition detection, accident warning, tourism information, etc. The collected information would be helpful for the users to plan their route. VANETs acts as a safety aid for the driver and passengers too. If the person caught up with some abnormal situation, current positional information of the vehicle can be sent to the police station or nearby hospital [*3*].

V2R communication is expensive as a large number of base stations and RSUs are needed to cover all the roads. To get some nearby information such as parking station, petrol stations, saloon etc.; it is important to have V2R communication. The work carried out in this thesis considers only V2V communication. The term node and vehicle are used interchangeably throughout the thesis. VANET is a kind of mobile ad-hoc networks with various distinct characteristics which evolve diversified prerequisites for it. The following section discusses all these important characteristics.

B. Characteristics of VANET

When WBAN is used as health purpose, the collected data has healthiness information. This information must be safe and not being accessed by unauthorized entities. Non reliable or insecure communication may highly affect health assistance of patient, so the communication must be reliable in wireless body area network (WBAN) [5]. Reliable and Secure communication is also necessary for another application of WBAN.

VANETs are characterized by high node mobility, constrained movement of nodes due to road topology, highly obstructive deployment fields and a chance for heavy congregation of nodes. There are a number of characteristics which differentiate VANETs from other ad-hoc networks listed as follows:

- Uneven distribution of vehicles on the roads affects the network connectivity. There are frequent network disconnections if the vehicle density is low.
- Vehicle speed depends on two factors, driver's wish and the congestion on the road.
- Due to the flexible speed of vehicles, there is a consistent change in the network topology.
- Communication end points are not defined by identifiers; instead they are defined by geographical areas.
- Nodes are vehicles, so there is no energy (power) and computation constraints.
- Vehicles are equipped with on-board sensors to get the location information which is required for communication.
- The mobility pattern of nodes is constrained as per the roadways, traffic rules, etc.
- Speed values and variations of VANET nodes are higher than the nodes of MANETs.
- Communication environment is either a highway or a city traffic scenario.
- Vehicles moving in the same direction and similar speed generally have a stable communication than vehicles moving in the opposite directions.
- The delay in sending the message is vital for some applications. For instance, if the vehicle in the front applies the brake, this message should be delivered to all the following vehicles instantly. The late arrival of the message is of no use in critical situation.
- While designing a network protocol for VANETs, the mobility model and prediction about the future position of a vehicle are important.

C. Problem Identification

In the literature review, some of the latest and standard paper are discussed in which, it is found that 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, nonrepudiation, access control, etc. to provide secure VANETs to its users. Therefore, the overall goals of security protocols of VANETs are to recognize malicious nodes in the network by using suitable mechanism.

In this work trustworthiness of VANETs will be improved by using some well-known adaptive Neuro-fuzzy system tools to detect the attacks in more efficient manner. Adaptive Neuro-fuzzy system tools will frequently monitor the behaviour of VANETs nodes and evaluate some malicious nodes based upon already developed model using historical knowledge of the same network. Since, training of the model is based upon the various features of VANETs nodes therefore, able to monitor the attack even in complex environment.

Rest of the paper is organized as follows, Section I contains the introduction of VANETs , Section II contains the related work of methodologies used by various researchers, Section III explains the proposed methodology with flowchart, Section IV describes the results and discussions, Section V provides the conclusion.

II. RELATED WORK

Various researchers are trying to solve many problems that are underway in data dissemination in vehicular adhoc networks. A few of the related issues to VANET are discussed.

Wu et al. [2] 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.

Terri et al. [4] 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 grayhole attack detection.

Hasrouny et al. [5] 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, not so efficient for real time applications.

Rupareliya et al. [6] proved that the authentication of information plays a significant role in VANETs. Therefore, providing end to end security become a significant role in VANETs. Watchdog and Bayesian filter based attack detection and prevention technique is implemented to improve the attack detection rate.

Zaidi et al. [7] 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.

Mehdi et al. [8] 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. [9] designed a secure end to end vehicular communication protocols which allows only authentic vehicles to transmit the data between vehicles. Thus, it prevents the unauthorised vehicles to communicate with authenticated devices and vehicles. However, this technique fails whenever any kind of attack occurs in the VANETs.

Muthumeenakshi et al. [10] 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.

Oliveira et al. [11] 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.

Bittl et al. [12] 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.

Dietzel et al. [13] implemented three graph-based measures to measure the redundancy of VANET routing techniques. These measures are applied on geo-cast protocol. Experimental results have proved that the proposed technique behaves almost optimally from a routing effectiveness. But fails to provide satisfactory redundancy for information consistency approaches in several scenarios.

O.A. Wahab et al. [14] has studied a numerous knowledge dissemination methods utilised in VANETs. In vehicular offer hoc sites knowledge move is usually finished with the aid of multi-hop conversation in that the top speed cars are working as the info carrier.

Medetov, S, et al. [15] storied versatile program which allows each car to instantly embrace probably the most appropriate dissemination system to be able to match the caution concept supply plan to each unique condition was studied.

Farooq, M. U, et al. [16] learned a bee-inspired algorithm for data dissemination in VANETs was learned wherever baby bees conversation together just in bee hives was taken as base for communication. The planned algorithm exploits bee conversation rules allowing cars talking with each other.

Sanguesa, J. A, et al. [17] learned knowledge dissemination methods and their benefits and limits were also studied. Their major intention is to supply a construction for knowledge dissemination in Vehicular ad-hoc sites such that it can be quite a variable enough to adjust to different vehicular traffic problems common worldwide.

M. Chaqfeh et al. [18] proposed an 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 focussed on ETSI Geo networking standards to efficiently handle the forwarding over VANETs. The authors have provided a novel strategy for data dissemination in multi-hop VANET. Their approach relies on the traffic estimation to provide selective broadcast in vehicular networks. Their approach provides low overheads and high packet delivery ratio.

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.

- 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.
- 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.
- 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.

III. METHODOLOGY

To do research we will use MATLAB (version15a). 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 an 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.

Steps involved in developing the proposed technique in MATLAB tool.

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.

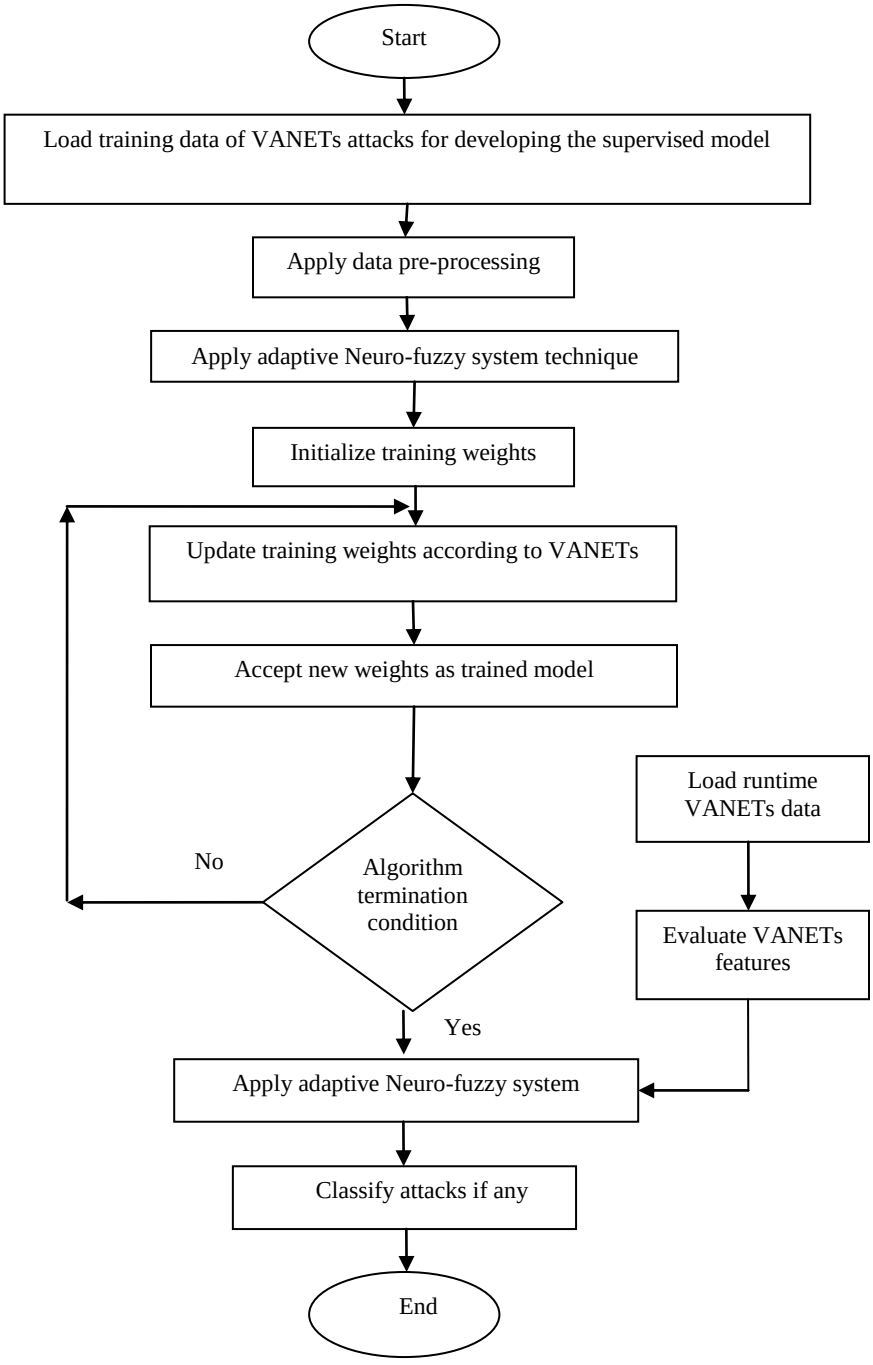

Figure 3. Flowchart of the Proposed Technique

IV. RESULT ANALYSIS AND DISCUSSION

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 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 Average download delay, Throughput, End to end delay, packet loss ratio. 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 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

1. Packet Lost Rate: Package damage occurs when number of 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.

Table 2: Packet Loss Ratio

Nodes	Existing	Proposed
5	14.3700	1.4963
10	22.4870	1.6336
15	34.8395	2.1234
20	45.7268	2.5615
25	58.6135	2.6077
30	63.5720	3.1423
35	76.8456	4.1230
40	89.8437	4.1023
45	97.5456	4.6103
50	138.2748	5.5281

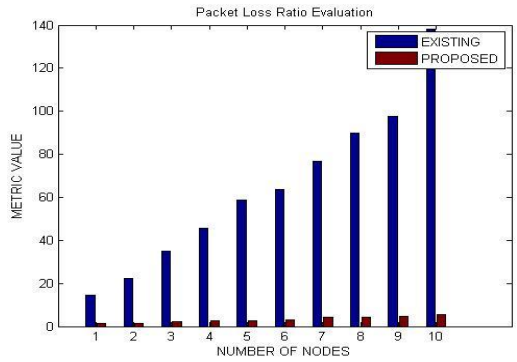

Figure 4. Represent the packet loss rate

Figure.4 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. Throughput: Throughput is actually the maximum charge connected with manufacturing or the maximum charge when something might be processed. Network throughput is actually the speed associated with the successive message supply on the communication channel.

Table 3: Throughput

Nodes	Existing	Proposed
5	11.1437	6.7037
10	7.3664	14.3664
15	6.1605	21.8766
20	5.2732	29.3923
25	4.4280	37.4385
30	3.7563	44.8540
35	3.2375	51.8770
40	2.9984	59.8977
45	2.1563	67.3897
50	1.5245	74.4719

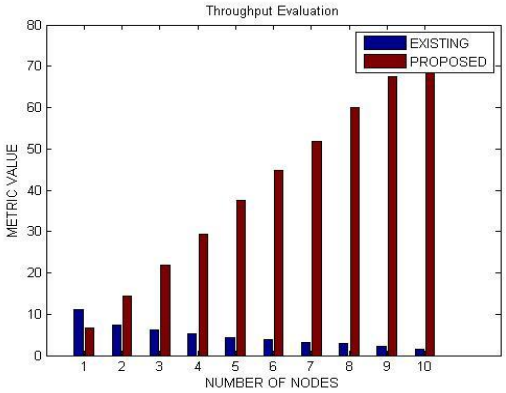

Figure 5. Represent the throughput

Figure.5 demonstrates the comparison of Throughput among the pre-existing and the proposed method where X-coordinate represents the Iterations and Y- coordinate values represents the Throughput per Iteration.

In our scenario the proposed technique's Throughput reasonably higher than the pre-existing technique.

3. 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.

Table 4: Average Download Delay

Nodes	Existing	Proposed
5	25.8957	15.1950
10	35.0577	24.9990
15	46.8075	37.1415
20	58.0048	45.8657
25	78.5689	56.9600
30	89.6407	67.4586
35	111.3880	88.4536
40	147.6137	94.8645
45	178.3184	105.7864
50	200.7825	154.4585

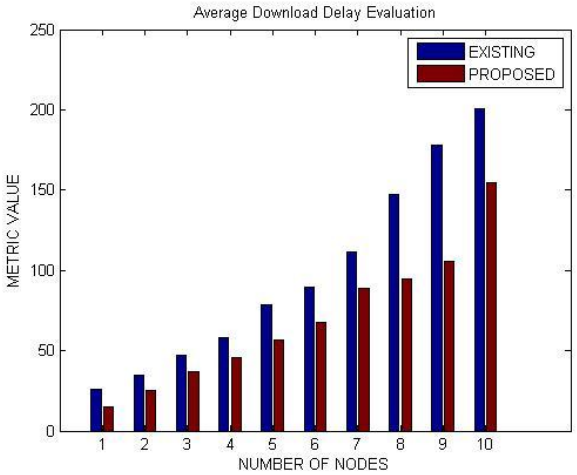

Figure 6. Represent the packet loss rate

Figure.6 demonstrates the evaluation of Average Download delay among the pre-existing and our proposed technique in which the X-coordinate represents the Iterations and the Y-coordinate represents the Average Download delay per Iteration.

In our scenario the proposed technique Average Download delay is reasonably lower than the pre-existing technique.

4. End to End delay

This metric represents the average delay experienced by the received data packet to reach the destination.

Table 5: End to End Delay

Nodes	Existing	Proposed
5	21.8957	11.1950
10	34.0577	22.9990
15	44.8075	34.1415
20	56.0048	44.8657
25	74.5689	58.9600
30	86.6407	69.4586
35	101.3880	82.4536
40	137.6137	100.8645
45	168.3184	115.7864
50	192.4563	159.4585

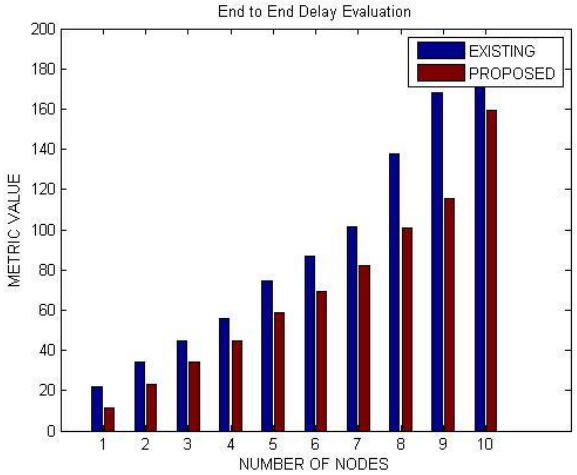

Figure 7. End to end delay

Figure 7. 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.

V. CONCLUSION

In this work an efficient data dissemination approach is proposed which not only improves the vehicle connectivity but also improves the QoS between the source and the destination. It utilizes properties of firefly optimization algorithm in collaboration with the fuzzy logic. 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 achievement of significant results in the parameters namely Packet Loss Ratio, Throughput, End to End Delay and Average Download Delay in comparison with existing approaches. In future the proposed approach will be further extended to accommodate different scenarios by following rural, highway, sub-urban and urban conditions.

ACKNOWLEDGMENT

The authors are really grateful to the reviewers for their honest comments which led to the improved version of this paper in terms of presentation and quality. The authors would like to thank the guest editors for their support. Also,

with the help of foundation of Beant College of Engineering and Technology, this work is at a successful stage.

REFERENCES

[1] Al-Kahtani, Mohammed Saeed. "Survey on security attacks in Vehicular Ad hoc Networks (VANETs)." In Signal Processing and Communication Systems (ICSPCS), 6th International Conference on IEEE , pp. 1-9, 2012.

[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, Hadi Otrok, Hassan Barada, Mahmoud Al-Qutayri, Yousof Al Hammadi, "Cooperative based tit-for-tat strategies to retaliate against greedy behavior in VANETs", Computer Communications, Vol.104, Pages 108-118, 2017.

[6] Guowei Wu, Jie Wang, Yongchuan Wang, Lin Yao, "Pollution Attack Resistance Dissemination in VANETs Based on Network Coding", Procedia Computer Science, Vol. 83, Pages 131-138, 2016.

[7] Hamssa Hasrouny, Abed Ellatif Samhat, Carole Bassil, Anis Laouiti, "VANet security challenges and solutions: A survey", Vehicular Communications, Vol. 7, Pages 7-20, 2017.

[8] Jay Rupareliya, Sunil Vithlani, Chirag Gohel, "Securing VANET by Preventing Attacker Node Using Watchdog and Bayesian Network Theory", Procedia Computer Science, Vol. 79, Pages 649-656, 2016.

[9] Kaur, Harbir, Sanjay Batish, and Arvind Kakaria. "An approach to detect the wormhole attack in vehicular adhoc networks." International Journal of Smart Sensors and Ad Hoc Networks (IJSSAN), pp. 86-89, 2012.

[10] 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.

[11] 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.

[12] Lo, Nai-Wei, and Hsiao-Chien Tsai. "Illusion attack on vanet applications-a message plausibility problem." In Globecom Workshops, IEEE, pp. 1-8., 2007.

[13] 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.

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

[15] 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, Pages 33-45, 2017.

[16] 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.

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

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

[19] Raw, Ram Shringar, Manish Kumar, and Nanhay Singh. "Security challenges, issues and their solutions for VANET." International Journal of Network Security & Its Applications, vol. 5, no. 5, pp. 95, 2013.

[20] D.Rewadkar, D.Doye, "Adaptive-ARW: Adaptive Autoregressive Whale Optimization Algorithm for Traffic-Aware Routing in Urban VANET", International Journal of Computer Sciences and Engineering, Vol.6, Issue.2, pp.303-312, 2018.

Authors Profile

Mr. Sahil Nayyar pursued Bachelor of Technology from Beant College of Engineering and Technology, Gurdaspur (under Punjab Technical University, Jalandhar) in 2011. He is currently pursuing M.Tech from Department of Electronics and Communication Engineering, Beant College of Engineering and Technology, Gurdaspur. His main research work focuses on attack detection techniques for VANETs. He has 2 years of teaching experience.

Mrs. Anita Suman pursued Master of Engineering from Thapar deemed University, Patiala in 2002. She is currently pursuing Ph.D from Punjab Technical University, Jalandhar and currently working as Assistant Professor in Department of Electronics and Communication Engineering, Beant College of Engineering and Technology since 2004. She has 13 years of teaching experience.

Mr. Parveen Kumar pursued Master of Technology from Punjab Technical University, Jalandhar in 2008. He is currently pursuing Ph.D from Punjab Technical University, Jalandhar and currently working as Associate Professor in Department of Electronics and Communication Engineering, Beant College of Engineering and Technology since 1998. He has 20 years of teaching experience.

