A light-weight reputation based intrusion detection system for service-oriented vehicular networks

Abdul Azeez Shaik Md.,

PG Scholar, Department of Digital Systems & Computer Electronics, JNTUA, Anantapur, Andhra Pradesh, INDIA

Abstract-Vehicular ad hoc networks (VANETs) are remote systems that give high-rate information correspondence among moving vehicles and between the vehicles and the street side units. VANETs are considered as the fundamental remote correspondence stages for the intelligent transportation systems (ITS). Administration arranged vehicular systems are exceptional classifications for VANETs that help various framework based business infotainment administrations including, for example, Internet get to, constant activity observing and administration, video gushing. Security is an essential issue for this administration arranges because of the important business data dealt with in these systems. In this paper, we plan and actualize a light-weight reputation based intrusion detection system, called reputation based intrusion detection mechanism for vehicular network (RPIDS) that aims to protect the network against possible attacks without dropping data in network for this trust management helps. RPIDS is in light of an arrangement of tenets that recognizes malicious vehicles and prevention purpose calculates reputation values for individual nodes and provides the security of data process. We introduce the execution investigation of our location instrument utilizing NS-2 test system. Our reproduction comes about demonstrate that RPIDS shows an abnormal state security regarding exceedingly precise identification rate and displays a lower overhead contrasted with contemporary structures.

I. INTRODUCTION

With the development and advancement of wireless communication technology, researchers conceptualized the idea of vehicular communication networks, also known as vehicular *ad hoc* networks (VANETs). These systems expect to transform autos into clever machines that speak with each other (V2V) or with a framework (V2I) keeping in mind the end goal to enhance activity wellbeing and solace of driving [1]. VANETs applications can be arranged into two classes: street movement wellbeing and administration situated applications. With service-oriented applications, street side units (RSUs) are sent along the streets for clients to ask for any area based administration (discovering eateries, downloading a guide, finding a corner store or a parking spot, and so on.), web based administrations (interactive media, moment emissary), or constant activity concerns. It is normal that administration arranged vehicular systems pull in a lot of interest in substantial scale organization of remote foundations [1], [2].

The accomplishment of such administration arranged vehicular systems depends basically on the fundamental correspondence framework, and especially, the data security since these systems are presented to assaults produced and dealt with by these systems [3]. The Intrusion Detection System's (IDSs) strategies demonstrate that they are extremely powerful in ensuring the system against both interior and outside assaults [4]– [8]. Along these lines, in this paper, we plan and build up a proficient and lightweight intrusion detection mechanism for vehicular networks (ELIDVs) that mean to secure the system against malignant vehicles. In this examination work, we center to recognize three sorts of assaults: 1) refusal of administration (DoS) that intends to bother the system task; 2) honesty focus on that adjusts the message that is traded between real vehicles or gives false data (FI, for example, false areas; and 3) false ready's age that communicates a false alarm message. ELIDV depends on an arrangement of discovery rules identified with each assault to show an ordinary (and peculiarity) conduct of a vehicle. Furthermore, with the assistance of the proposed discovery system, we built up a vehicle's conduct assessment (VBE) convention that assesses the reliability level of a vehicle as indicated by its behavior and the available information it provides. We have designed a light-weight detection framework with no need to any additional hardware resource (e.g., firewall) to achieve a high level of security. What's more, ELIDV is extensible for new functionalities that would permit recognizing more mind boggling assaults.

We take note of that, to the best of our insight, we are the primary managing the interruption issue on benefit situated VANETs, and the recognition of the most hazardous assaults that could happen in such systems. Indeed, the majority of the works, for example, [1], [2], [9] apply cryptography systems to avert outer aggressors entering the system.

The network process should be as followed below:

A. Network flow

There is three principle segments in a sensor arrange. These are the sensor nodes, sink and checked events. Beside the not very many setups that use portable sensors, the vast majority of the system design expects that sensor nodes are stationary. Then again supporting the mobility of sink or cluster heads (entryways) is some of the time regarded vital.

B. Node Deployment

Another thought is the topological arrangement of the nodes which is application dependent and influences the execution of the routing protocol. The arrangement is either deterministic or self sorting out. In deterministic circumstances, the sensors are

physically put and information is directed through pre determined ways. Anyway in self dealing with structure the sensor nodes are scattered arbitrarily makes a foundation in an uncommonly designated way.

C. Energy Consideration

During the formation of a framework, the procedures of setting up the routes are significantly impacted by energy considerations. Since the transmission energy of a remote radio is corresponding to the distance squared or considerably higher request within the sight of obstacles, multi hop routing will consume less energy than coordinate correspondence. Be that as it may, multi hop routing presents huge overhead topology administration and medium access control. Coordinate directing would perform well advice if every one of the nodes is near the sink. More often than not sensors are scattered arbitrarily finished a zone of intrigue and multi hop directing winds up plainly unavoidable.

II. RELATED WORK

In previous section, described different attacks that target service-oriented networks and attempt to detect these attacks using framework, namely, DoS, Integrity target, and false alert's generation attacks.

i) **DoS attack:** The malicious vehicle that dispatches such an assault plans to aggravate the system activity or the utilized steering convention. The vehicle that completes such an assault intends to drop all the got packets from legitimate vehicles.

ii) **Integrity target attack:** such an assault plans to adjust the message that is traded between real vehicles or give false information (FI) such as location.
Sybil attack: In vehicular systems, the vehicles ordinarily find their neighbors by intermittently broadcasting cooperative awareness messages, in which they claim their identities and positions; in this way, a Sybil node expects to make numerous personalities with giving false areas.

iii) **False alert's generation attack:** For this situation, the pernicious vehicle sends an alarm message to its k-jump neighbors to encourage them to take some sly activities. The idea of the attackers is to send a false alarm message all together, for example, to clear the street for itself or make a traffic jam in the road.

III. PROPOSED SYSTEM

The proposed system consists of the following components, as below mentioned: The monitor, the reputation system, the path manager, and the trust manager. The components are present in every node.

The monitor:

In a remote systems administration condition, the hubs well on the way to distinguish rebellious conduct are the hubs in the region of the guilty party and for some situation the source and the goal, in the event that they recognize surprising behavior or do not get proper responses. The latter is not always the case, for instance in the case of replay. One way to deal with convention requirement and recognition of harming conduct recommended here is what might as well be called an area watch, where nodes locally search for veering off nodes.

The nodes of the area watch can identify deviations by the following node on the source course by either tuning in to the transmission of the following node or by watching course convention conduct. By keeping a duplicate of a bundle while tuning in to the transmission of the following node, any content change can also be detected.

The Trust manager:
In an ad-hoc condition, trust administration needs to be circulated and versatile. This segment manages approaching and active ALARM messages.

The trust manager consists of the following components.

- An alert table containing data about got cautions.
- A trust table overseeing trust levels for nodes to decide the reliability of a caution.
- A companions list containing all companions a node conceivably sends cautions to.
- For routing and forwarding, trust is important when making a decision about providing or accepting routing information, accepting a node as part of a route, and taking part in a route originated by some other node.

The Reputation system:
Reputation frameworks are utilized as a part of some online sale in frameworks. The notoriety framework in this convention deals with a table comprising of passages for nodes and their rating. The rating is changed just when there is adequate proof of vindictive conduct that is noteworthy for a node and that has happened various circumstances surpassing a limit to discount occurrences.

The Path manager:
The path manager plays out the accompanying capacities:

- Path re-positioning as indicated by security metric, e.g., notoriety of the nodes in the way.
- Deletion of ways containing pernicious nodes.
- Action on getting a demand for a course from a pernicious node.
- Action on getting demand for a course containing a malignant node in the source course.

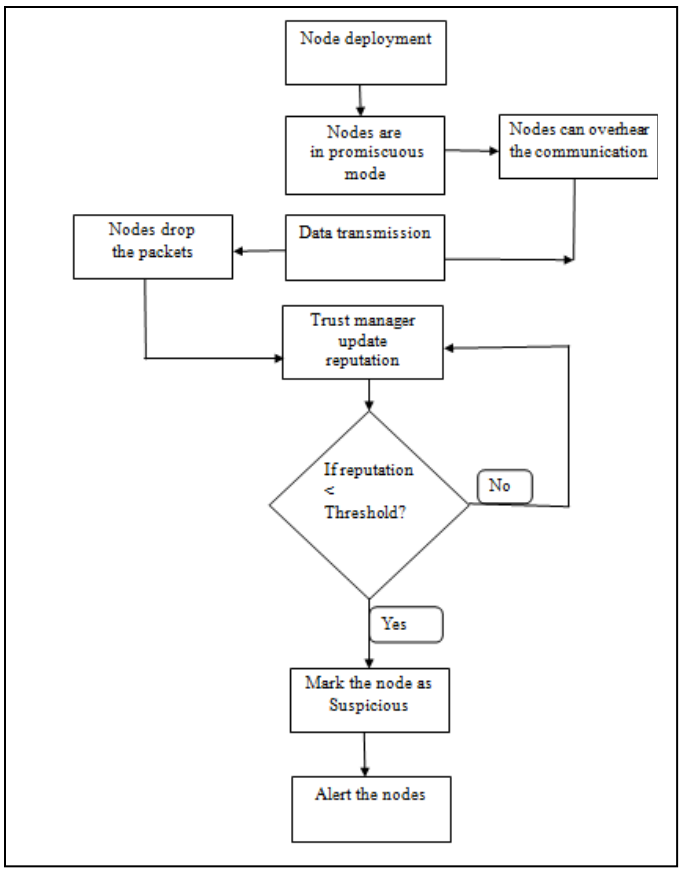

Fig1: Framework of proposed system

As shown in Figure 1, each node monitors the behavior of its next-hop neighbors. Once promiscuous mode applicable to all nodes place in network, nodes can overhear the communication. So further step data transmission occurs. On the off chance that a suspicious occasion is recognized, the data is given to the notoriety framework. In the event that the occasion is critical for the node, it is checked whether it has happened more regularly than a predefined edge, which is sufficiently high to recognize think pernicious conduct from straightforward incidents, for example, crashes. What constitutes the significance rating can be defined for different types of nodes according to their security requirements. On the off chance that the event limit is surpassed, the notoriety framework refreshes the rating of the node that caused the occasion. In the event that the rating ends up being heinous, the data is handed-off to the way supervisor, which continues to erase all courses containing the horrendous node from the way reserve. The hub keeps on observing the area, and an ALARM message is sent as portrayed underneath.

So as to pass on notice data, an ALARM message is sent by the trust supervisor part. This message contains the sort of convention infringement, the quantity of events watched, regardless of whether the message was self-started by the sender, the address of the announcing node, the address of the watched node, and the goal address (either the source of the route or the address of a friend that might be interested). In the present simulation implementation, the ALARM is sent to the source of the concerned route. In this paper, k-means algorithm introduces and mentioned in below.

The k-mean calculation intends to partition the system graph into K number of clusters with the end goal that the separation between the nodes inside each cluster is minimized. At to begin with, K number of nodes is chosen indiscriminately as the underlying focus nodes of the clusters. At that point, in every emphasis, every node is appointed to its closest cluster. When the sum total of what nodes have been along these lines allocated, the center node for each cluster is recalculated, and the procedure is rehashed from the earliest starting point in light of the personality of the new focus nodes. The clustering step stops when they obtained centre nodes still the same in two sequential emphases.

IV. EXPERIMENTAL RESULTS

In this paper, we assume that 30 sensor nodes are randomly distributed over a 1600x1600m^2 fields where existing traffic based network. At any time during the simulation CBR-connections are active. In the defenseless network, the number of packets dropped intentionally is up to two orders of threshold greater than in the network fortified by proposed scheme. Table1 shows the system parameters used in our simulations. In this paper, in order to simplify scheduling for the VANET area, we accept that the information gathered by sensor nodes is the deferral tolerant information.

PARAMETER	VALUE
Application Traffic	CBR
Transmission rate	50 packets/sec
Radio range	250m
Packet size	512 bytes
Maximum speed	25m/s
Simulation time	30s
Number of nodes	30
Area	1600x1600
Routing protocol	AODV

Table1: System parameters

- **Evaluation results**

In this section, the results are fairly constant with respect to mobility, only decreasing slightly in the case of an almost static network at a pause time of 30s. The fortified network is a little more sensitive to mobility. This can be explained by the increased probability of meeting a previously unknown malicious node when nodes move around more.

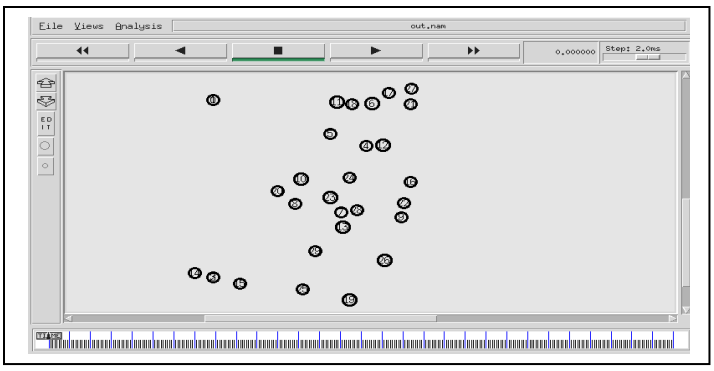

Figure 2: Network Deployment

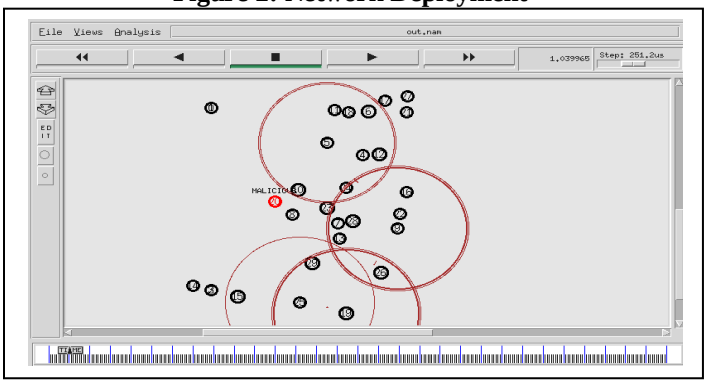

Figure 3: Broadcasting in Network

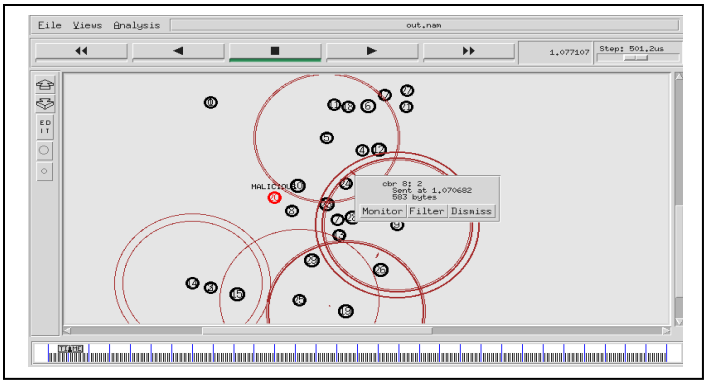

Figure 4: Data communication through routing path

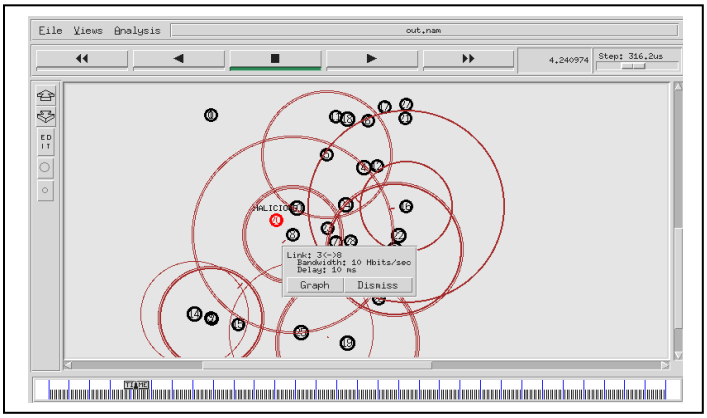

Figure 5: Data communication through alternate path

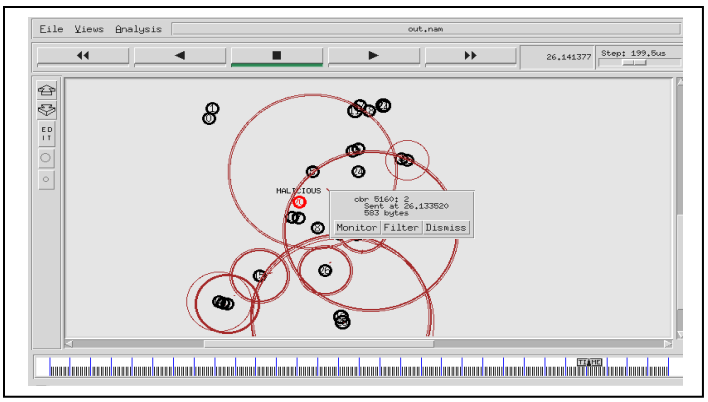

Figure 6: Malicious node tried to disrupt the routing path

multipath.txt

```
============= Result At 1.01104 ==============
Source        : 25
Destination   : 5
Token Node    : 7
Total Routes  : 1
============= Result At 1.01225 ==============
Source        : 25
Destination   : 5
Token Node    : 13
Total Routes  : 2
============= Result At 1.01320 ==============
Source        : 25
Destination   : 5
Token Node    : 28
Total Routes  : 3
============= Result At 4.00097 ==============
Source        : 1
Destination   : 0
Token Node    : 1
Total Routes  : 1
============= Result At 1.01104 ==============
Source        : 25
Destination   : 5
Token Node    : 7
Total Routes  : 1
============= Result At 1.01225 ==============
Source        : 25
Destination   : 5
```

Figure 7: Multipath file information

out.tr

```
M 0.0 nn 30 x 1600 y 1600 rp
M 0.0 prop Propagation/TwoRayGround ant Antenna/OmniAntenna
M 0.00000 4 (473.35, 542.36, 0.00), (473.37, 542.36), 0.12
M 0.00000 5 (386.10, 576.59, 0.00), (386.11, 576.57), 0.12
M 0.00000 6 (489.55, 664.51, 0.00), (489.54, 664.49), 0.12
M 0.00000 7 (412.50, 350.00, 0.00), (412.48, 350.02), 0.12
M 0.00000 8 (300.00, 375.00, 0.00), (300.02, 374.98), 0.12
M 0.00000 9 (559.81, 334.42, 0.00), (559.79, 334.42), 0.12
M 0.00000 10 (315.86, 444.71, 0.00), (315.85, 444.69), 0.12
M 0.00000 11 (403.75, 668.00, 0.00), (403.77, 668.00), 0.12
M 0.00000 12 (516.02, 544.05, 0.00), (462.49, 550.02), 0.12
M 0.00000 13 (417.57, 307.01, 0.00), (399.75, 345.67), 0.12
M 0.00000 14 (55.80, 173.67, 0.00),(106.37, 154.34), 0.12
M 0.00000 15 (166.35, 144.35, 0.00), (166.37, 144.36), 0.12
M 0.00000 16 (582.00, 436.85, 0.00), (582.00, 436.87), 0.12
M 0.00000 17 (529.43, 694.76, 0.00), (493.77, 668.02), 0.12
M 0.00000 18 (438.90, 660.91, 0.00), (438.89, 660.93), 0.12
M 0.00000 19 (433.86, 96.98, 0.00), (433.88, 96.98), 0.12
M 0.00000 20 (257.10, 411.51, 0.00), (309.15, 380.31), 0.12
M 0.00000 21 (582.00, 661.85, 0.00), (581.99, 661.87), 0.12
M 0.00000 22 (565.76, 376.05, 0.00), (559.79, 334.42), 0.12
M 0.00000 23 (387.09, 391.85, 0.00), (412.37, 335.37), 0.12
M 0.00000 24 (433.17, 450.27, 0.00), (433.17, 450.25), 0.12
M 0.00000 25 (318.86, 126.98, 0.00), (318.88, 126.97), 0.12
M 0.00000 26 (520.12, 210.61, 0.00), (520.10, 210.62), 0.12
M 0.00000 27 (583.92, 706.22, 0.00), (574.98, 675.02), 0.12
M 0.00000 28 (451.16, 355.95, 0.00), (412.52, 350.01), 0.12
M 0.00000 29 (350.00, 237.50, 0.00), (350.02, 237.51), 0.12
```

Figure 8: Trace file in network

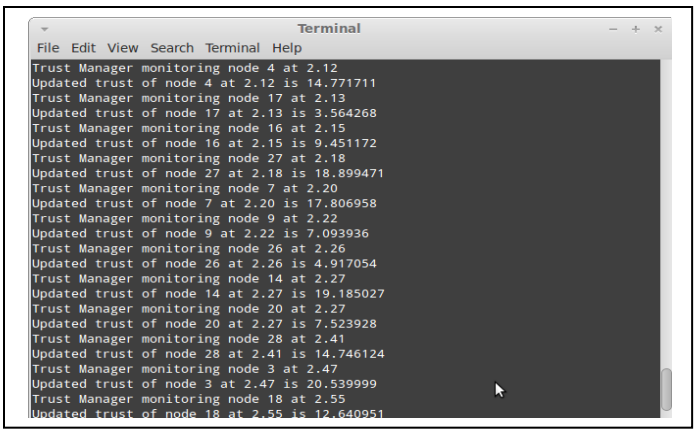

Figure 9: Reputation system data file

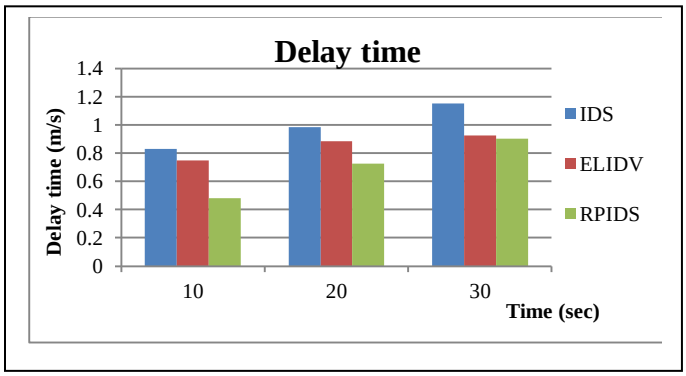

Figure 10: Performance on Delay

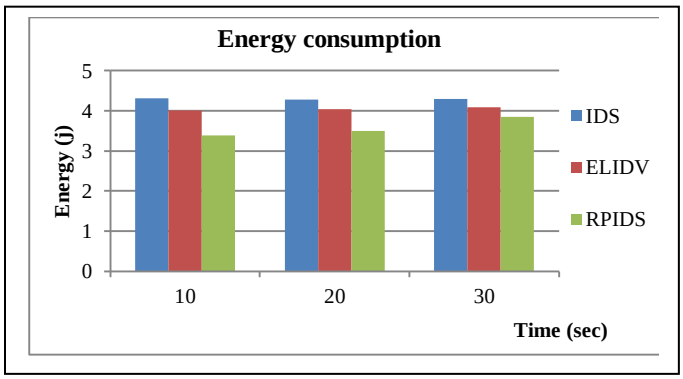

Figure 11: Energy level routing

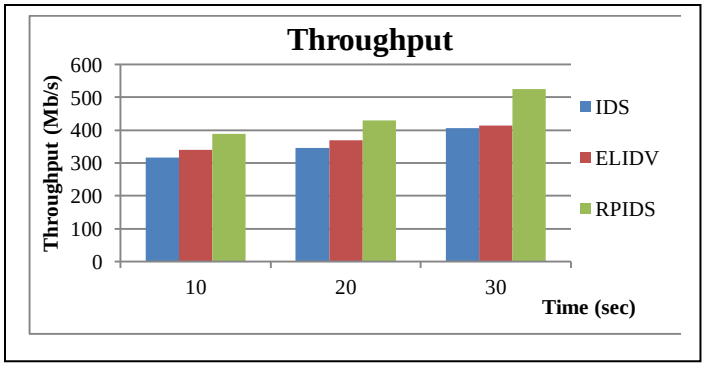

Figure 12: Network performance

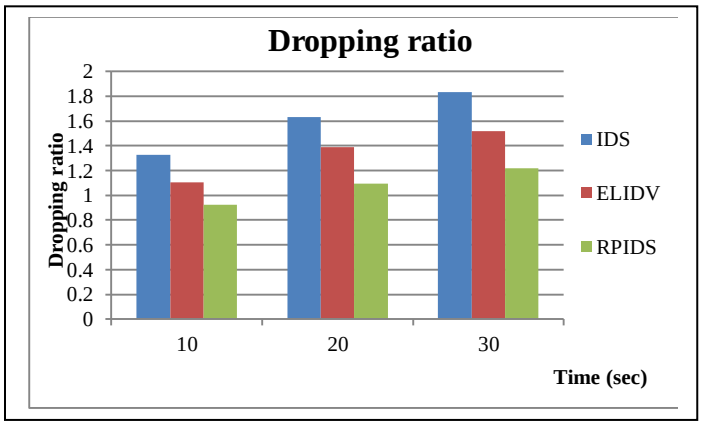

Figure 13: Dropping ratio in network

In above screenshots, Fig 2 shows all nodes placed in Vehicular network and deployment of nodes is in network properly. Here all nodes displayed based on topology values and all properties of NAM window it should be mentioned. Fig 3 shows the broadcasting occur throughout the network. Here broadcasting occurs for communication purpose. All nodes should be involved in this process. Fig 4 shows that communication between users through routing path.

Fig 5 shows that, data communication process through alternate path. Here malicious node trying to access the data. Fig6 shows that, user to user communication occur in VANET but here malicious node tries to access the system for disrupt the network communication. The proposed system has provided the security for network. Fig 7 shows that displayed the multipath file it means shows result of number of routes between source and destination, token node and which nodes are participate in communication. Fig 8 indicates trace file representation in network. This file set the routing level and whatever using variables, different time intervals in network shows. Fig 9 shows and represents the trust management system output values. Here which node has a more reputation value it represented based on time interval.

In Fig 10, graph shows and represents end2end delay and it shows a simulation time versus delay. The performance of reputation based intrusion detection system improves delay time it means decrease the delay between communication nodes compare to efficient and light weight intrusion detection mechanism and normal Intrusion detection system. Fig 11 shows and represents energy consumption and it shows a simulation time versus energy. The performance of reputation based intrusion detection system improves energy values compare to light weight intrusion detection mechanism and normal Intrusion detection system. Fig 12 shows and represents throughput and it shows a simulation time versus throughput. The performance of reputation based intrusion detection system improves the throughput compare to light weight intrusion detection mechanism and normal Intrusion detection system. Fig 13 shows

and represents dropping ratio and it show a simulation time versus dropping ratio. The performance of reputation based intrusion detection system decreases the dropping ratio compare to light weight intrusion detection mechanism and normal Intrusion detection system.

V. CONCLUSION

The security in service-oriented VANETs is a challenging issue. In this paper, we proposed and implemented RPIDS, a new intrusion detection mechanism, in terms of cooperation, robustness, and fairness, and analyze the performance of a plan to adapt to them by retaliating for pernicious conduct and cautioning partnered nodes to keep away from terrible experiences. Observable assaults on sending and routing in vehicular ad-hoc networks can be thwarted by the suggested RPIDS scheme of detection, alerting, and reaction. Performance investigation by methods for reproduction appears a significant change as far as better results when AODV is fortified with the RPIDS protocol extensions. We also conducted simulation by using NS2 and exploratory outcomes demonstrate that our reputation based intrusion detection system is practical for the vehicular network. The RPIDS protocol is scalable in terms of the total simulation time in a network and performs will even with a dropping ratio decreased without effect of malicious nodes.

REFERENCES

[1] K. Mershad and H. Artail, "A framework for secure and efficient data acquisition in vehicular ad hoc networks," *IEEE Trans. Veh. Technol.*, vol. 62, no. 2, pp. 536–551, Feb. 2013.

[2] H. Zhu, R. Lu, X. Shen, and X. Lin, "Security in service-oriented vehicular networks," *IEEE Wireless Commun.*, vol. 16, no. 4, pp. 16–22, Oct. 2009.

[3] T. Zhang, H. Antunes, and S. Aggarwal, "Defending connected vehicles against malware: Challenges and a solution framework," *IEEE Internet Things J.*, vol. 1, no. 1, pp. 10–21, Feb. 2014.

[4] H. Sedjelmaci, S. M. Senouci, and M. Feham, "An efficient intrusion detection framework in cluster-based wireless sensor networks," *Secur. Commun. Netw.*, vol. 6, no. 10, pp. 1211–1224, 2013.

[5] A. Daeinabi, A. G. P. Rahbar, and A. Khademzadeh, "VWCA: An efficient clustering algorithm in vehicular ad hoc networks," *J. Netw. Comput. Appl.*, vol. 34, no. 1, pp. 207–222, 2011.

[6] M. Raya, P. Papadimitratos, I. Aad, D. Jungels, and J.-P. Hubaux, "Eviction of misbehaving and faulty nodes in vehicular networks," *IEEE J. Sel. Areas Commun.*, vol. 25, no. 8, pp. 1557–1568, Oct. 2007.

[7] S. Ruj, M. A. Cavenaghi, Z. Huang, A. Nayak, and I. Stojmenovic, "On data-centric misbehavior detection in VANETs," in *Proc. IEEE Veh. Technol. Conf. (VTC Fall)*, San Francisco, CA, USA, 2011, pp. 1–5.

[8] N. Kumar and N. Chilamkurti, "Collaborative trust aware intelligent intrusion detection in VANETs," *Comput. Elect. Eng.*, vol. 40, no. 6, pp. 1981–1996, 2014.

[9] E. Coronado and S. Cherkaoui, "Service discovery, and service access in wireless vehicular networks," in *Proc. SUPE Workshop IEEE Globecom*, New Orlean, LA, USA, 2008, pp. 1 6.