Asian Journal of Engineering and Applied Technology
ISSN 2249-068X Vol. 8 No. 1, 2019, pp. 38-43

Differential Evaluation Based Secure Ad-Hoc Protocol for Vanets

Tamanna Gandotra[1] and Gurpadam Singh[2]
[1&2]Department of Electronics and Communication Engineering,
Beant College of Engineering and Technology, Gurdaspur, Punjab, India
E-Mail:tamannagandotra3@yahoo.com, gurpadam@yahoo.com

Abstract **- VANET is a special category of MANETs which is composed of moving vehicles, acting as nodes. Vehicular Ad-hoc Networks 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. Many studies have indicated that appropriate attack algorithms are essential to provide secure operation of a network. It has been observed that the use of optimum or sub-optimum values are ignored while detecting the wormhole attacks in VANETs. The use of differential evolution is ignored in existing literature which can find optimum values for attack detection based VANETs. It has been observed that the proposed technique outperforms existing techniques in terms of packet collision and throughput.**

Keywords: **VANET, AODV Protocol, Attacks, Differential Evolution**

I. INTRODUCTION

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. VANET is a special category of MANETs which is composed of moving vehicles, acting as nodes. Vehicular Ad-hoc Networks 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 do not require any infrastructure and use On-Board Units (OBU) and Road Side Units (RSU) like traffic signals and base stations for communications. Vehicles can collect the essential information and share it with other vehicles [*2*]. 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.

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.

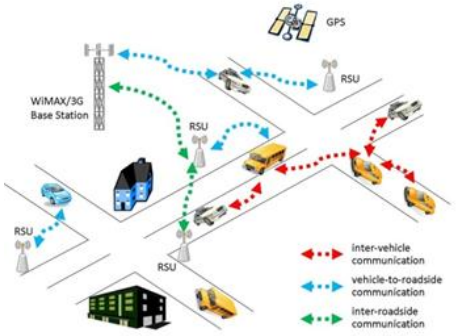

Fig. 1An Illustration of the VANETs [2]

A. Need for VANET

In a fast developing country like India, it is very important that physical infrastructures such as roads and traffic systems are geared up to meet the rising tide of vehicles and to regulate their movements in a safe manner. A total of 4, 73,416 traffic accidents cases were reported. Various steps have been taken to increase road safety for vehicles by the automotive industry. Some of them such as Anti-Braking System (ABS) brakes and air bags have become a standard feature in most vehicles, while advanced systems such as pre-crash systems are only offered in selective vehicles.

The next stage in the evolution of safety-enhancing technologies will likely be in the form of active cooperative systems in which vehicles are fitted with Global Positioning System (GPS) devices and can coordinate with each other to avoid collisions. The next generation of vehicle-safety enhancing technologies operating under the flagship of Intelligent Transportation systems (ITS) seeks to speed up this evolution. VANET is envisioned as a key component of the ITS framework for providing low-latency and highly-reliable vehicular communication.

B. Characteristics of VANET

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. Firstly, vehicles are travelling at very high speeds in a highly structured topology such as roads than in a MANET. Thus the routing protocols which were designed for MANET will not be suitable for a continually changing structure such as VANET, where communication links are expected to be valid for few minutes or seconds. Another individual character of VANET is that the existing roadmaps limit the topologies available for it, when compared to MANETs. High rise buildings and houses in urban areas act as obstacles, impacting the propagation of wireless waves through reflections and refractions [5, 6]. Finally, VANETs permit a large number of vehicles to be part of it, which makes scalability an important Quality of Service (QOS) parameter.

A few characteristics such as short radio transmission range, low bandwidth and self-organization are trivial for every ad-hoc network including VANETs. However, there are a number of characteristics which differentiate VANETs from other ad-hoc networks listed as follows:

1. Uneven distribution of vehicles on the roads affects the network connectivity. There are frequent network disconnections if the vehicle density is low.
2. Vehicle speed depends on two factors, driver's wish and the congestion on the road.
3. Due to the flexible speed of vehicles, there is a consistent change in the network topology.
4. Communication end points are not defined by identifiers; instead they are defined by geographical areas.
5. Nodes are vehicles, so there is no energy (power) and computation constraints.
6. Vehicles are equipped with on-board sensors to get the location information which is required for communication.
7. The mobility pattern of nodes is constrained as per the roadways, traffic rules, etc.
8. Speed values and variations of VANET nodes are higher than the nodes of MANETs.
9. Communication environment is either a highway or a city traffic scenario.
10. Vehicles moving in the same direction and similar speed generally have a stable communication than vehicles moving in the opposite directions.
11. 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.
12. While designing a network protocol for VANETs, the mobility model and prediction about the future position of a vehicle are important.

II. AD-HOC ON-DEMAND DISTANCE VECTOR (AODV) PROTOCOL

"AODV is an on-demand, loop-free protocol. Further, it is also a single path, distance vector protocol". It has combination approach of the on-demand route discovery mechanism in DSR with the concept of destination sequence numbers from DSDV. But, AODV takes a hop-by-hop routing approach unlike DSR that uses source routing. "AODV protocol results in lower network overhead as compared to the proactive protocols and reduces flooding in the network. AODV routing protocol reduces the routing table by generating a route whenever a node is required to send the information data packets to another nodes in the network". This effort reduces the requirement of memory size.

The Ad hoc On Demand Distance Vector (AODV) routing algorithm is a routing protocol that is designed for ad hoc mobile networks which is capable of both unicast and multicast routing. AODV builds and maintains the routes as long as they are required by the sources. The sequence numbers are being referred for the purpose of ensuring the freshness of routes. "AODV uses destination sequence numbers for route discovery process which excludes the route is looping and can provide the dynamic updates for adjusting the route conditions. The source node starts the discovery of routes by broadcasting a route request RREQ packet to its neighbours".

Under AODV when the packets are sent by nodes to the destination then data packets only contains destination address. Whereas under DSR , when a node sends a packet to the destination the full routing information is stored in the data packets that causes more routing overheads than AODV.

III. LITERATURE REVIEW

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.

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, 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 becomes 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*. [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.

Safi *et al*. [11] 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. Oliveira *et al.* [12] proved that the cooperation among vehicles is 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*. [13] 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*. [14] have 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. Parul, and Deepak Dembla *et al*. [15] have focused on well-known sybil attack which may happen in VANETs. In sybil attack, a malicious vehicle acts as if it is a huge number of vehicles. An unnamed authentication and sybil attack monitoring technique called ASAP-V is proposed. ASAP-V has provided more robust results against sybil attacks, with lesser number of overheads.

IV. 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.

Steps involved in developing the proposed technique in MATLAB tool:

Step I: Initialize a VANET network with its characteristics.
Step II: A node acting as a source sends data to its destination.
Step III: The Worm Hole Attack, the source node broadcasts route request (RREQ) to the nearby nodes in search for the shortest possible route to the destination. The intermediate nodes that receive the RREQ message transmit to the neighbouring nodes till they find a route to the destination.
Step IV: Meanwhile, one of the intermediate nodes may be a malicious node and it transmits a false route reply (RREP) message to the source node.
Step V: The source node transmits all the message packets to this malicious node, thus never transmitting them to the intended receiver.
Step VI: In the meantime, the source also rejects other RREP messages that contain a genuine path to the destination.
*Step VII***:** After receiving a false RREP, source node selects the route received from the malicious node and also ignores any forthcoming RREP messages from genuine nodes. By repeating this process, an intruder node can successfully capture other routes as well as message packets in the network by forcing most of the network traffic to flow through itself.
Step VIII: If a malicious node intercepts the transmitted RREQ message and sends a fake RREP message, there is no inherent mechanism in AODV to detect whether the received RREQ is from a genuine node or from a malicious node. This research focuses on Worm Hole Attack, where the legitimate data packets are absorbed by a malicious node, thus causing the information to be lost.
Step IX: The source node uses additional information known as pseudo reply packet (PRREP) by considering the differential evolution technique.

a. Generate initial solutions i.e., population for VANETs by considering the normal distribution with mean=0 and variance =1.
b. Now evaluate fitness value of each solution and elect solutions with best fitness values.
c. Now apply mutation operator on the solution with best fitness values.
d. Now apply recombination operator to generate the child solutions.
e. Now re-evaluate the fitness values of each solution and select the solution with best fitness values.
f. Repeat Step IX, until the stopping criteria met.

Step X: The source node stores the information about all the incoming packets in a look-up table i.e., RREP_T obtained from differential evolution. This table stores the PRREP sequences, arranged in ascending order using PUSH and POP operations.
Step XI: Any abnormality in the table sequences is considered to be a PRREP sequence received from a malicious node and is discarded by the source. Furthermore, the table is periodically updated, with all the PRREP sequences stores for a set duration defined by STR_dur.
Step XII: A header H_node attached to each message received from different nodes, assigns a priority to the

PRREP message and is considered in that order by the source node. The priority is calculated based on the sequence number, and the shortest sequence number is given the highest priority.

Step XIII: Node having abnormal sequence number is considered as a malicious node and source broadcast this message in network.

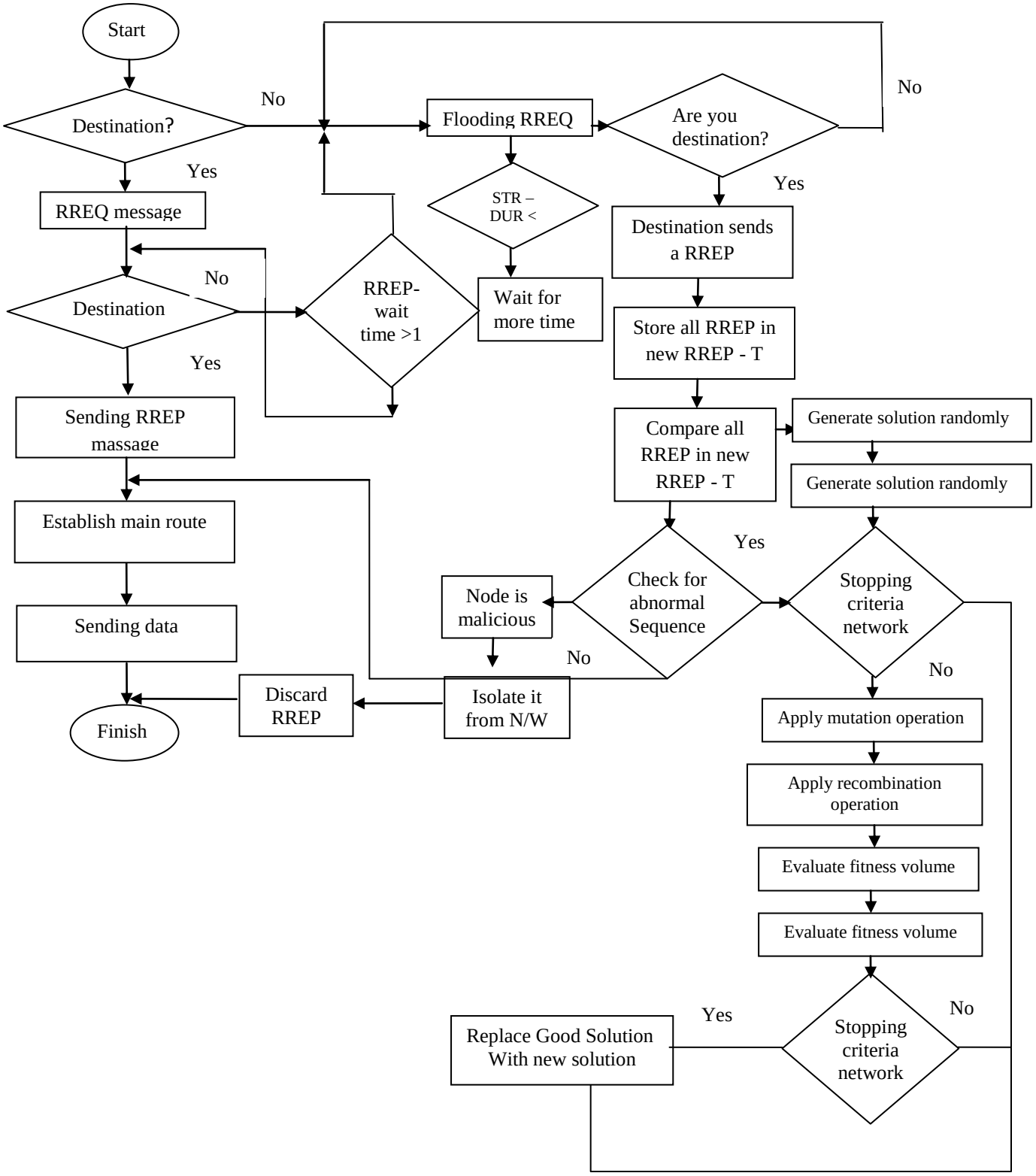

Fig. 2 Flowchart of the Proposed Technique

V. RESULT 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 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 Drop ratio, Bit Error rate, Accuracy, 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 I EXPERIMENTAL SETUP

PARAMETER	VALUE
Level_of_agg	1:5
Speed_of_vehicle(m/sec)	10:10:50
Distance(m)	50:50:150
Number of Nodes (S)	10
Min1(x and y-coordinate of nodes)	20
max1(x and y-coordinate of nodes)	80
oint1	10
oint2	20
simu_time(sec)	5
Coverage range(R)(m/sec)	50

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.

A. Packet Collision

A significant number of packets collide with the neighbouring 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.

$$\text{Packet collision (Collision Rate)} = \frac{\text{Unsucessfull Transmission}}{\Sigma\text{Total number of sent packet}}$$

Table II is indicated about quantized research into the packets collision. As packets collision ought to be lower which implies proposed algorithm is indicating the superior results when compared to access methods as the packets collision is lower in each case.

Fig. 3 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.

TABLE II PACKETS COLLISION

Nodes	Existing	Proposed
1	0.635	0.159
2	0.836	0.163
3	0.427	0.142
4	0.404	0.166
5	0.405	0.14
6	0.478	0.135
7	0.482	0.133
8	0.519	0.134
9	0.512	0.134
10	0.509	0.134

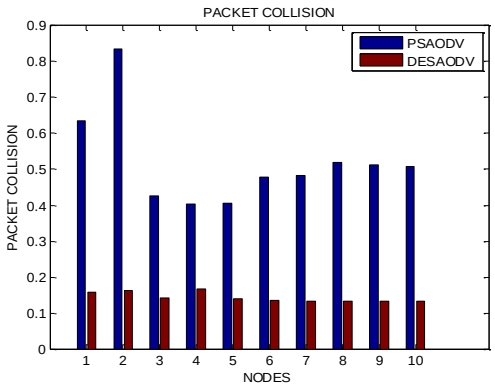

Fig. 3 Represent the packets collision

B. 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

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

Table III is indicated about quantized research into the throughput. As throughput ought to be higher which implies proposed algorithm is indicating the superior results when compared to access methods as the throughput is higher in each case.

Fig. 4 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.

TABLE III THROUGHPUT

Nodes	Existing	Proposed
1	0.868	0.913
2	0.857	0.911
3	0.875	0.923
4	0.892	0.91
5	0.9	0.923
6	0.891	0.926
7	0.895	0.927
8	0.889	0.927
9	0.891	0.927
10	0.89	0.927

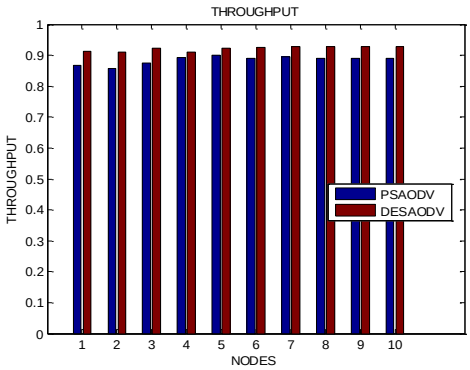

Fig. 4 Throughput Representation

VI. 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. It has been observed that the use of optimum or sub-optimum values are ignored while detecting the wormhole attacks in VANETs. The use of differential evolution is ignored in existing literature which can find optimum values for attack detection based VANETs. The effect of heterogeneous scenarios is also ignored by the most of existing researchers. In this research work, to detect wormhole attack, differential evolution-based attack detection technique is proposed. In high vehicular density situations, there exist several kinds to attackers who drop the packets communicated by vehicles. It has been proposed that the proposed method has better result as compared as existing methods in terms of packet drop ratio, accuracy and bit error rate. In future, the proposed approach will be further extended to accommodate different scenarios by following rural, highway, suburban and urban conditions.

REFERENCES

[1] G. Eason, B. Noble, and I. N. Sneddon, "On certain integrals of Lipschitz-Hankel type involving products of Bessel functions", *Phil. Trans. Roy. Soc. London*, Vol. A247, pp. 529–551, April 1955. *(references)*

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

[3] 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.

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

[5] A. Chinnasamy, 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.

[6] Doaa Al-Terri, HadiOtrok, Hassan Barada, Mahmoud Al-Qutayri, and Yousof Al Hammadi, "Cooperative based tit-for-tat strategies to retaliate against greedy behavior in VANETs" *Computer Communications*, Vol. 104, No. 17, pp.108-118, 15 May 2017

[7] Guowei Wu, Jie Wang, Yong chuan Wang, and Lin Yao, "Pollution Attack Resistance Dissemination in VANETs Based on Network Coding" *Procedia Computer Science*, Vol. 83, pp. 131-138,2016.

[8] Hamssa Hasrouny, Abed Ellatif Samhat, Carole Bassil, and Anis Laouiti, "VANET security challenges and solutions" *A survey, Vehicular Communications*, Vol. 7, pp.7-20, 2017.

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

[10] 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),*Vol.1, pp. 86-89, 2012.

[11] 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, 2016.

[12] QamasGul Khan Safi, SenlinLuo, Chao Wei, Limin Pan, and Qianrou Chen, "PIaaS: Cloud-oriented secure and privacy-conscious parking information as a service using VANETs", *Computer Networks*, Vol. 124, pp. 33-45,2017.

[13] Rene Oliveira, Carlos Montez, Azzedine Boukerche, and Michelle S.Wangham, "Reliable data dissemination protocol for VANET traffic safety applications", *Ad Hoc Networks*, Vol. 63, pp. 30-44, 2017.

[14] Sebastian Bittl, "Privacy conserving low volume information retrieval from backbone services in VANETs", *Vehicular Communications*, Vol. 9, pp. 1-7, 2017.

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

[16] 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* Vol.18, pp.133-139, 2013.