International Journal of Engineering Science Invention (IJESI)
ISSN (Online): 2319 – 6734, ISSN (Print): 2319 – 6726
www.ijesi.org ||Volume 7 Issue 1|| January 2018 || PP. 06-14

Trust-Based Multihop Routing for Vehicular Ad-Hoc Network

Babangida Zubairu[1],Dr. Savita Shiwani[2]
[1](*Research Scholar School of Computer & Systems Sciences, Jaipur National University, Jaipur, Rajasthan State, India,*
[2](*Associate Professor, Computer Engineering, Jaipur National University, Jaipur, Rajasthan State, India,*
Corresponding Author: Babangida Zubairu[1]

Abstract: *Vehicular ad-hoc network (VANET) is a brand of wireless technology that operates in an open environment, the specification of vehicle to vehicle (V2V) enables vehicles to share information related to the traffic status in real time. The communication in this wireless technology is self-organized and self-configured without the need of gateways. Security threat remains one of the disturbing challenges in the technology. Attack like packet drop could obstruct the performance and reliability of the communication. The paper is aimed at enhancing multihop communication by proposing Trust-Based scheme, the approach introduces the mechanism of portioning the communication signal into regions and zones and acknowledgment technique to provide holistic control and tracking of the packet flow from source node to the destination node.*

Key words: *multihop, packet drop, VANET, V2V, wireless*

Date of Submission: 11-01-2018 Date of acceptance: 22-01-2018

I. Introduction

In Vehicle to Vehicle (V2V) communication, the vehicle communicates wirelessly with one another via wireless medium [1], V2V is purely wireless communication between vehicles in ad-hoc mode; it enables data exchange platform for the vehicle to communicate and share information with other vehicle within a communication range [2]. In V2V communication, each vehicle is a node and can work as a source, a destination and/or a router to re-transmit traffic related information to other vehicles. The vehicles communicate either directly or indirectly, this mean, the nodes within the same signal range communicate directly and for the nodes that are out of the same signal range communication via an intermediate nodes by establishing route in multihop mode [3], this enables forwarding of data to an individual or group of node [4] .

Multihop communication enables message propagations in vehicular networks based on the principles of mediator approaches, through carry-forward process by neighbouring vehicles until the desired dissemination target node is reached **[5]**, the packet propagations are accomplishing through intermediary vehicles when a source vehicle send a message to destination vehicle. However, due to high mobility of vehicles and multipath propagation, communications in vehicular networks suffer from severe channel mutilations which make quality-of-service (QoS) provisioning in the networks seriously challenging. These have highlighted that, improving and securing the transmission reliability is critical issues in vehicular network **[6]**.

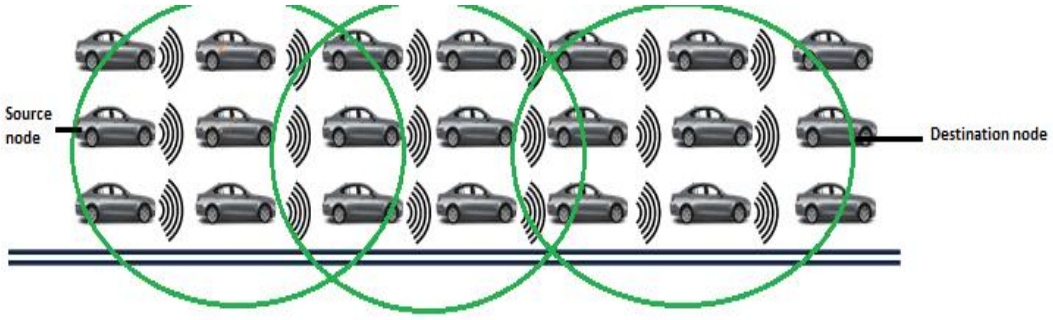

Figure 1: MultiHop communication in vehicular network

Fig. 1 represents multiHop communication in vehicular networks, the source node communicates with the destination node, these nodes are not within the same signal range and the remaining nodes are the intermediary nodes residing in different signal range that forward transmission in multihop mode, they provide relay services by re-broadcasting the packet sent from source node to reach the target destination node.

II. Literature Review

Nodes in vehicular settings are of equal status; this means each of them is capable of transmitting information from itself to another node within the network signal. A network path is the mechanism responsible for Information transmission in vehicular networks from one node to another; the path mechanism is guided by the routing protocol. Hence, the reliability of the path is an important issue since the nodes are mobile and require constant information updates of their neighbours. Security remains the significant important concern in vehicular network deployment **[7]**. Safety in VANET is essential, since it affects the life of people, it is essential that the message sent between nodes reaches the right destinations **[8]** .

In vehicular networks, a malicious vehicle can claim to have an active path to the destination vehicle and request the routing packets to be routed through itself before passing to the destination, while the passive vehicle is malicious and can drop the packet without passing it to the right destination [9]. According to [10] highlighted packet drop attack as one of the security threats that affects the performance of VANETs, this treat is potential to cause catastrophic consequences of violating routing protocol and vital segments of vehicular networks to develop serious problem and malfunctions [11]. However, this threat can lead to problems like delay, suspension of communication route or even generating erroneous information between the source node and destination node [12], these have shown that information exchange in VANET ought to be secured and save guarded against malicious node behavior [13]. Hence, the security issue is amongst the serious threats, which can restrict the applications, performance and functionality of the VANET [14].

In [15], solution to denial of service threat was proposed; the approach uses lines of defense to contradict attacker and its effect. The line of defense proposed was capable to handle DOS attack. However, the scheme controls congestion of network traffic and broadcast storm during propagating of emergency warning messages among vehicle even in the absence of DOS attacks. Similarly, c proposed batch verification technique to verify multi-signed messages; as described in the scheme, the RSU performs batch verification on behalf of vehicles. It turned out efficiently in the condition intensifies with cars per RSU. However, it is inefficient there is less intense of vehicles per RSU. Furthermore, it has a limitation of high overhead in processing ID-based signature verification for vehicles. To address similar threat, [16] proposed mechanism that classifies packets as legitimate or not using cryptographic techniques and filter the attack packets. Once packets are marked as an attack type, the packets are dropped at the border router of the target network before reaching the victim; the solution is infrastructure base, and the infrastructure can be attacked or damage, if one of these happens, the entire system can be compromised

III. Statement Of The Problems

The nodes in a vehicular network are the vehicle that communication in an open space, multihop is a communication mechanism that depends on intermediary nodes for a message to reach the destination node from source node in vehicular networks. A malicious node is considered among the intermediary nodes during the communication, the malicious node joined the network and pretends to be an active node and request for a communication flow through its route, when the a message passes through itself, the message is discarded and dropped without forwarding to the next or target node. This type of attack affects performance of the network, damage network topology and increase bandwidth consumption as well as creating unnecessary delay in the network that can affect network throughput performance. These imply the need of enhancing communication in vehicular network and protect the network against the act of a malicious node.

However, a malicious node can exploit knowledge about the protocol to perform an insider attack by analysing the importance of the packet transmission and during packet forwards; it intercepts and alter the message. Consequently, the malicious node could completely control the network operations

IV. Trust-Based Scheme

The promising wireless technology for enhancing transportation safety and improving highway efficiency of vehicular networks is IEEE 802.11p [17]. The IEEE 802.11p is one of the recently approved amendments to the IEEE 802.11 standard aimed to add Wireless Access in Vehicular Environments (WAVE). It appended some enhancements to the latest version of 802.11 that requires applications support of Intelligent Transportation Systems (ITS) [18]. The standard operates in the 5.9-GHz frequency band of 5.850 to 5.925 GHz bandwidth [19]. To improve and address the mentioned threat in V2V communication, a Trust-Based scheme was introduced that partition the nodes in the network into regions and zones.

4.1Signal region and region member formation

Signal region is defined as the signal range within which nodes could communicate directly without intervention of intermediary node and the nodes within a region are called region members.

Definition: Let R_1,R_2, and R_3 represent different signal ranges in 2-D space, where n_i represents the nodes within a signal range.

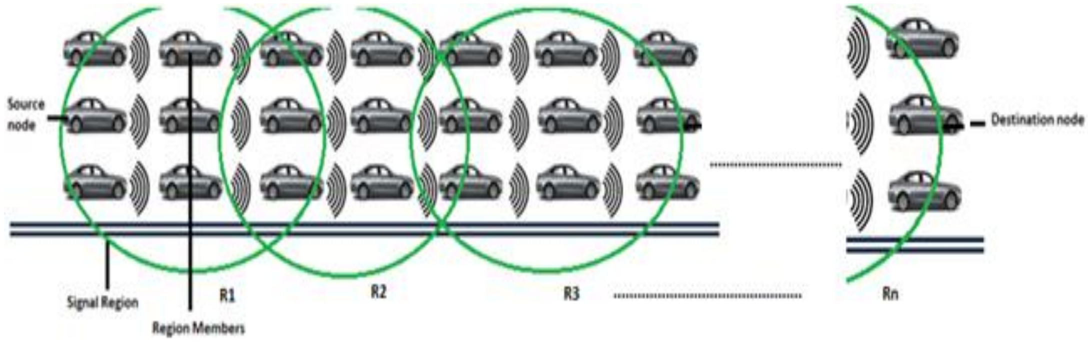

Figure 2: Signal Region and Region members

Therefore, a signal range can be defined as the boundary within which nodes could communicate directly without intervention of intermediary node and the nodes within a region are called region members. The region member for a signal range R_i can be defined as $\{n: n \epsilon \ R_i\}$, for instant nodes in R_1 and R_2 will be represented as:

$$\boldsymbol{R_1 \cup R_2 = \{n: n \epsilon \ R_1 \, or \, x \epsilon \ R_2\}} \ldots\ldots(1)$$

And nodes in R_2 and R_3 Will Be

$$\boldsymbol{R_2 \cup R_3 = \{n: n \epsilon \ R_2 \, or \, n \epsilon \ R_3\}} \ldots\ldots(2)$$

Therefore, nodes in R_1 , R_2, R_3 and R_n will be

$$\boldsymbol{R_1 \cup R_2 \cup R_3 \ldots \cup R_n = \{n: n \epsilon \ R_1 \ or \ n \epsilon \ R_2 \, or \ n \epsilon \ R_3 \, or \ n \epsilon \ R_n\}} \ldots(3)$$

The number of nodes in a region is defined as:

$$\bigcup_{r=1}^{k} \mathbf{R_r} = \{\mathbf{n}: \mathbf{n} \, \epsilon \ \mathbf{R_r} \ \ \mathbf{for \ r}, \mathbf{1} \leqq \mathbf{r} \leqq \mathbf{k}\} \ldots\ldots(4)$$

Where R is the signal range and r is the region member

4.2 Zone and zone member formation

For a set of signal range R_n , for n = 1,2 3,…….k, a zone is defined as the intersection of two regions , the nodes within a zone are called zone members. Represented as:

$$\mathbf{R_1 \cap R_2 = R_2 \cap R_1 = zon..e} \ldots\ldots(5)$$

The above set contains nodes members that belong to R_1 and R_2 see Fig. 3.

For a set of signal range R_n , $\{n = 1,2,3,4, k\}$, the intersection of two regions is called Zone, the nodes within a Zone are called zone members.

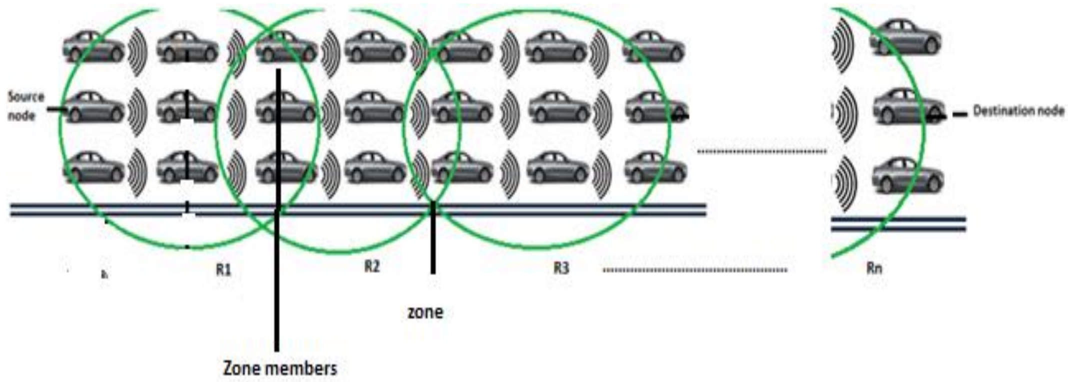

Figure 3: zone and zone members

Therefore, a set of zones R_i *and* R_j can be defined as:

$$\mathbf{R_i} \bigcap \mathbf{R_j} \ = \{\mathbf{n}: \mathbf{n} \, \epsilon \ \ \mathbf{R_i \ and \ n \, \epsilon \ R_j}\} \ldots\ldots(6)$$

In general, the zone can be symbolically represented as:

$$\mathbf{R_i \cap R_j} = \bigcap_{n=i}^{j} \mathbf{R_n} \ldots\ldots(7)$$

Where is R the region i,j= 1,2,3,…….n

4.3 Scheme flow chart

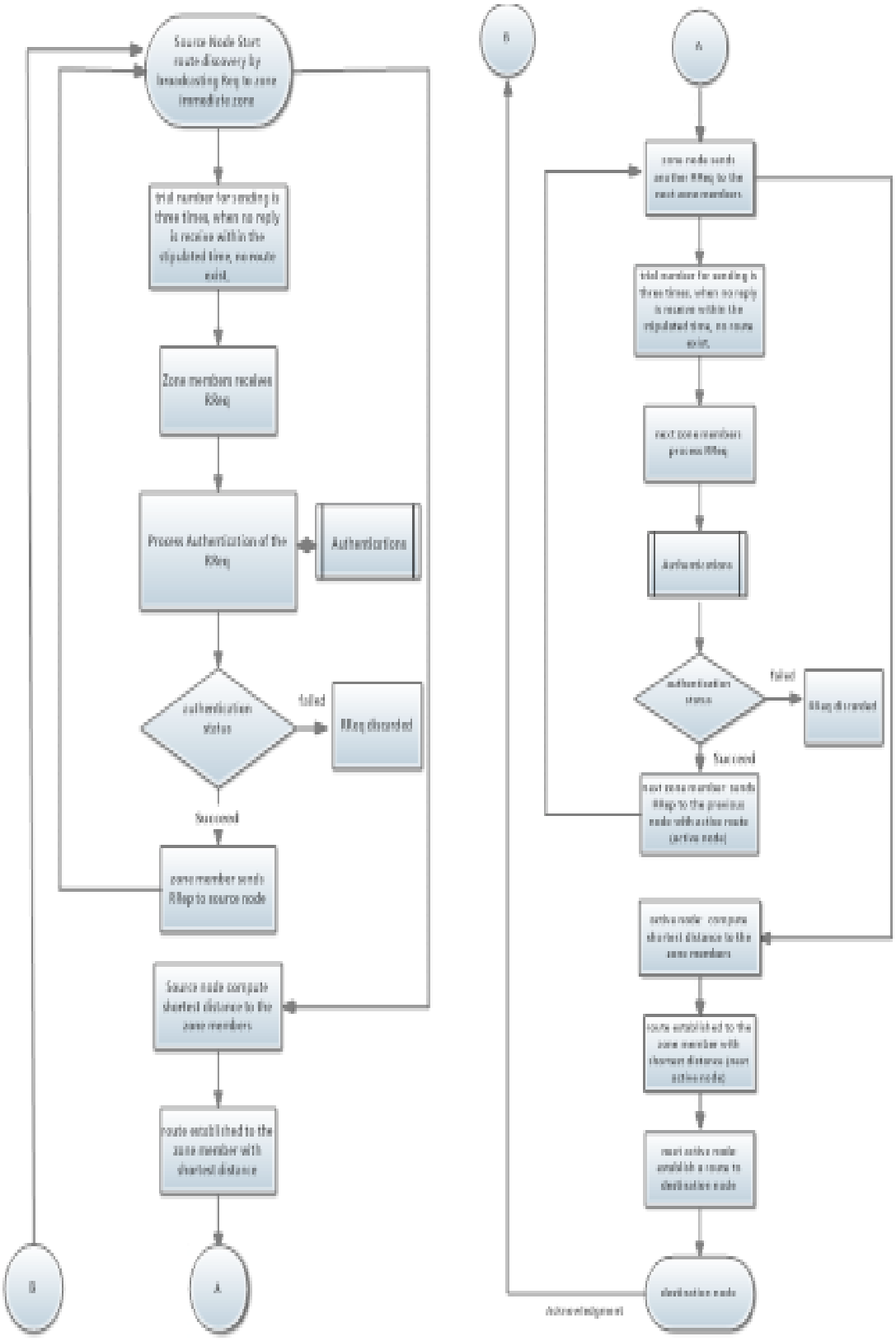

Figure 4: Trust-Based flow chart

4.4Assumptions

The following were used as the assumptions in the algorithm design:

- Any node that joins the network will be assigned with a unique network Identification number (ID) by the zone members and shared among the nodes in the network.
- The ID contains the vehicle's ID, radio ID, zone ID and region ID which are stored in the neighbours' table of each vehicle and updated periodically.
- The nodes in each region and zone maintains symmetric connection
- The transmission power of the nodes is based on the 802.11p specification

4.5The algorithms of the scheme

In an ad-hoc network, broadcasting a packet from one to another requires a route to be established from source node to the destination node, the following algorithms provide enhanced route discovery process from source to the destination node using Route Request (RReq) and Route Reply (RRep) messages, as well as the acknowledgment broadcast from destination node to the source node upon successful packet transmission.

Step 1: Source node broadcast Route Request (RReq) to all nodes in the 1st zone see Fig. 5.

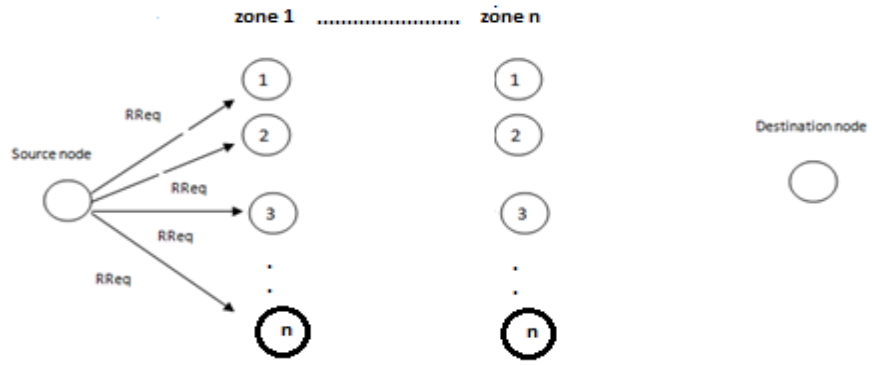

Figure 5: Route discovery initialisation

After sending the RReq message , the source node waits for a set of stipulated time as total number of RReq sent/60 seconds, if no Request Reply (RRep) received within a stipulated time it resend RReq again , the number of attempts is three times, if time exceeds , then the source will assume no route exist and route discovery discarded.

Step 2: The zone members reply with RRep message to source node

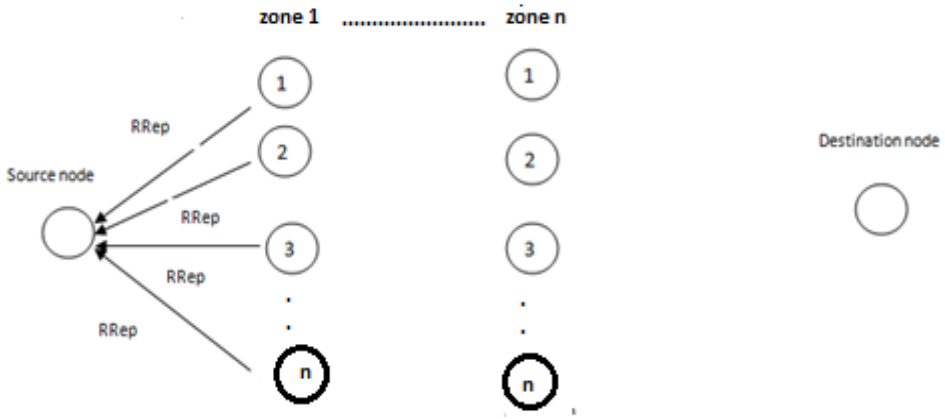

Figure 6: Route Reply broadcast

Step 3: The source node computes the shortage distance between the source node to the zone and established route to the node with the shortage distance. If the linked node does not send an acknowledgment to source node within a stipulated time, then the node is assumed to be a malicious node see Fig. 7, the established route discarded and the suspected node is rooted out of the neighbor's table.

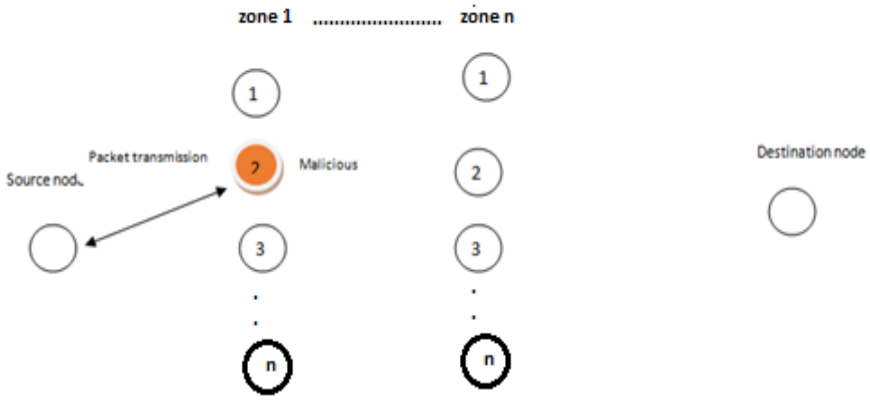

Figure 7: Route established from source node to the malicious node

Step 4: The source node re-broadcast RReq to all nodes in the zone members, excluding the suspected malicious node since is marked as malicious and the node ID is removed from neighbors' table see Fig. 8 And wait for another stipulated time to get the RRep message from the zone members in the same approach explained in step 1-3. Upon receipt of the RRep message from the zone members, an active route is established from source node to the zone member with the shortest distance see Fig. 9.

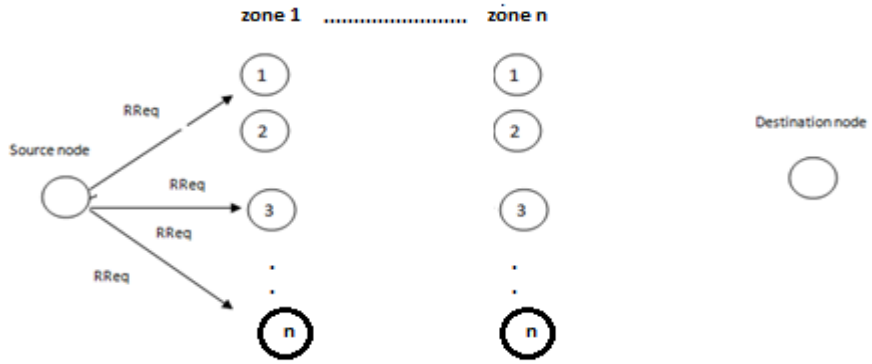

Figure 8: Re-broadcast of RReq to zone members excluding the suspected node from source node

Step 5: Upon successful route establishment, the zone node resend another RReq message to the nodes in the second zone members and wait for reply of RRep message in a similar approach explained in step 1-3 see Fig. 9.

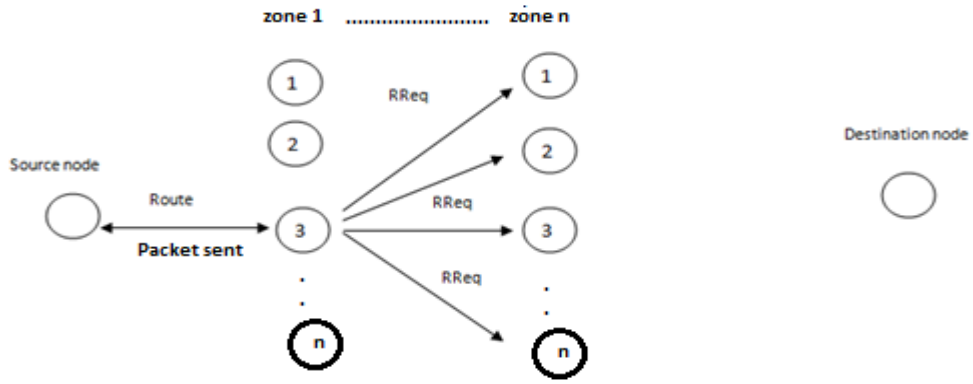

Figure 9: Route established from the source node to the zone member.

Step 6: The process continues until route is established to the target destination node, whenever a linked node suspected to be malicious, the route is discarded and node is rooted out of the neighbors' table and all other node members notified. The packet flows from the source node to the destination node along the established route see Fig. 10.

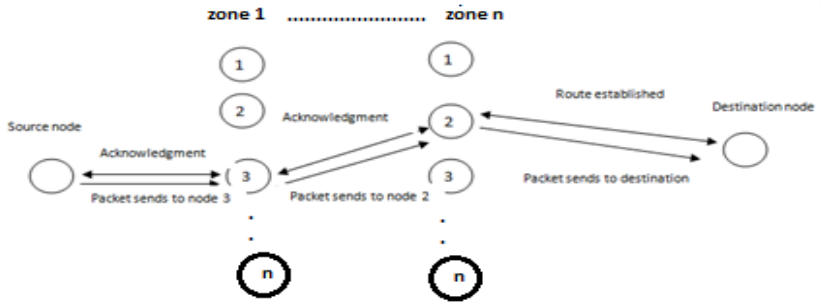

Figure 10: Route established from the source node to the destination node

Step 7: An acknowledgment is broadcast back to the source node from the destination node through the established route see Fig. 11; this mechanism enhances the communication by providing tracking and transmission control.

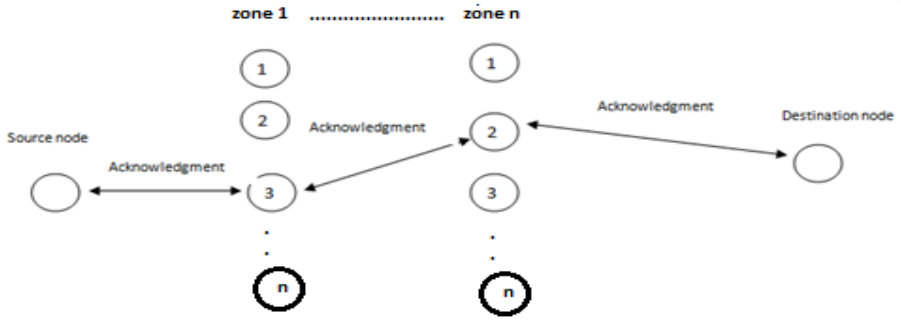

Figure 11: Acknowledgment broadcast from the source node to the destination node

V. Results And Discussion

To evaluate the performances of the proposed scheme model, NS-3 network and simulation tool was used, the tool is an open source software for discrete event network simulation, mainly for research and educational use [20]. The platform provides models of packet data flow in a network and performances as well as the simulation engine for conducting simulation experiments. Two scenarios were employed and implemented in the network simulator, the mentioned threats in section 3.0 were deployed in the first scenario, while the proposed schemed discussed in section 4.0 was implemented in the second scenario. XML files were generated from the scenarios for netAnim to visualize the simulation sequences.

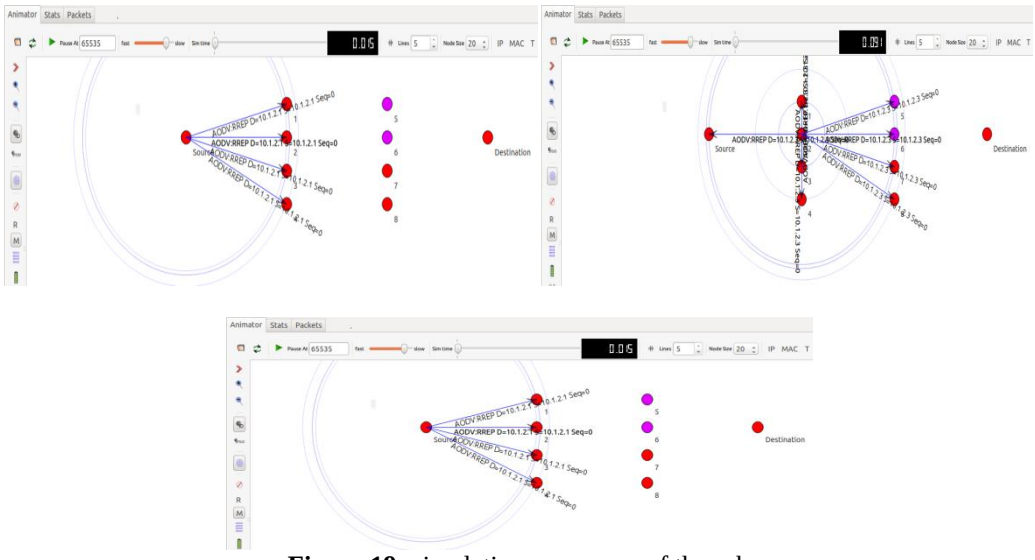

Figure 19: simulation sequences of the scheme

Trace files were generated from the scenarios and analyzed using TraceMetrics, a trace analyzer for Network Simulator 3, and pcap files were also generated and analyzed using Wireshark version 1.10.6 for the packet flow and protocol analysis, the results shows significant improvement in the network performance and channel utilizations from the proposed scheme.

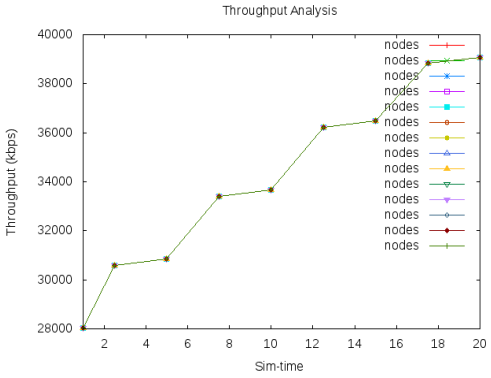

Figure 20: Network throughput of scenario 2

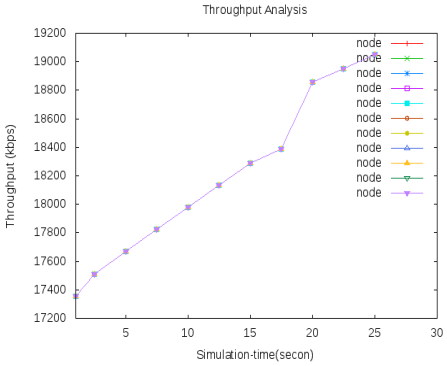

Figure 20: Network throughput of scenario 1

The network throughput and delay graphs were generated using Gnu plot from simulation results. The throughput in analysis shows that scenario 1 produces less throughput compared to scenario 2, this shows that attacks like packet drop could influence performance of vehicle to vehicle communication. However, the graph of scenario 2 shows that, the proposed scheme could serve as a remedy for this kind of attack and enhances network throughput.

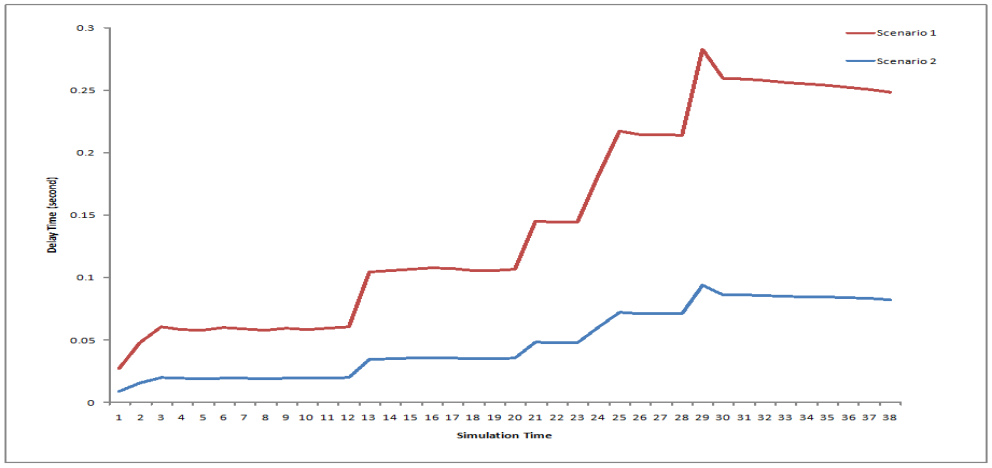

Figure 20: comparison of the Network delay between scenario 1 and 2

The delay analysis shows that, scenario 1 produces more delay compared to scenario 2, this indicated that, the delay affects the network performance and the delay have a significant effect on the network reliability and availability.

VI. Conclusion

Multihop communication is the ideal mode of communication when the communicating nodes are not within the same signal range; the openness future of vehicular network exposes this type of network to vulnerabilities such as the packet drop. A threat like packet drop is hazardous since a vehicle can claim to have an active route and drop the packet when is broadcasted through the route, thereby creating chaos and huge security risks in the network. The study presented in this paper, exposes the vulnerabilities and potential obstructions in V2V communication and presented a remedy to the threats. The proposed scheme as observed, proves to be effective in safeguarding packet drop vulnerability in V2V, the scheme presented enhancement in the network throughput and network delay reductions significantly.

References

Journal Papers:

[1]. Elias C. Eze Si-Jing Zhang En-Jie Liu Joy C. Eze, "Advances in Vehicular Ad-hoc Networks (VANETs):Challenges and Road-map for Future Development," International Journal of Automation and Computing: Springer, vol. 13, no. 1, pp. 1–18, JANUARY 2016.

[2]. Arun Kumar KA, "Worm Hole-Black Hole attack Detection and Avoidance in Manet with Random PTT using FPGA," International Conference on Communication Systems and Networks, pp. 21-23, 2016.

[3]. Dr.M.Yuvaraju M.Sindhuja, "CONGESTION CONTROL USING ON-BOARD DATA UNITS IN VANET SCENARIOS," International Journal of MC Square Scientific Research, vol. 7, no. 1, pp. 1-9, November 2015.

[4]. Shahzad F., Qayyum A., Mehmood R Gillani S., "A Survey on Security in Vehicular Ad Hoc Networks," in Springer, Berlin, Communication Technologies for Vehicles, Heidelberg, 2013, pp. 59-74.

[5]. Kiho Lim and Manivannan D., "An efficient protocol for authenticated and secure message delivery in vehicular ad hoc networks," Elsevier Inc: Vehicular Communications, vol. 4, no. 1, pp. 30–37, 2016.

[6]. Amit Joshi ,Kamlesh C. Purohit Priyanka Sirola, "An Analytical Study of Routing Attacks in Vehicular Ad-hoc Networks (VANETs)," International Journal of Computer Science Engineering (IJCSE) , vol. 3, no. 4, pp. 210-218, July 2014.

[7]. D. P. Dwivedi Bharti, "Performance Analysis of Black Hole Attack with AODV using Different No. of Nodes in VANET," International Journal of Science and Research, vol. 5, no. 7, pp. 1956-1959, 2016.

[8]. Martin Euku and Richard Ssekibuule Kennedy Edemacu, "P ACKET D ROP A TTACK D ETECTION T ECHNIQUES IN W IRELESS A D HOC N ETWORKS : A R EVIEW," International Journal of Network Security & Its Applications (IJNSA), vol. 6, no. 5, pp. 75-86, September 2014.

[9]. Farid.Naıt-abdesselam, Zonghua Zhang, Ashfaq Khokhar Soufiene Djahel1, "Defending Against Packet Dropping Attack in Vehicular Ad-Hoc Networks," security and communication networks, pp. 1–13, 2008.

[10]. Adil Mudasir Malla and Sahu Kant Ravi, "Security Attacks with an Effective Solution for DOS Attacks in VANET," International Journal of Computer Applications, vol. 66, no. 22, pp. 45-49, 2013.

[11]. Archana.S. Pimpalkar and Bhagat Patil R. A., "Defense against DDoS Attacks Using IP Address Spoofing," International Journal of Innovative Research in Computer and Communication Engineering, vol. 3, no. 3, pp. 1919-1926, 2015.

[12]. Wu Lenan Abdeldime M.S. Abdelgader, "The Physical Layer of the IEEE 802.11p WAVE Communication Standard: The Specifications and Challenges," in Proceedings of the World Congress on Engineering and Computer Science, San Francisco, USA, 2014.

[13]. Lorenzo Rubio, Vicent M. Rodrigo-Peñarrocha, Juan Reig Herman Fernández, "Path Loss Characterization for Vehicular Communications at 700 MHz and 5.9 GHz Under LOS and NLOS Conditions," IEEE Antennas And Wireless Propagation Letters, pp. 931 - 934, 2014.

[14]. ns-3. (2017, October) ns-3. [Online]. HYPERLINK "https://www.nsnam.org/" https://www.nsnam.org/

Book:

[15]. Mohamed Watfa, Advances in Vehicular Ad-Hoc Networks:Developments and Challenges, 1st ed., Kristin Klinger, Ed. New York, USA: IGI Global, 2010.

Proceedings Papers:

[16]. Florian Thomas, Jérôme Härri, Hannes Hartenstein Jens Mittag, "A Comparison of Single- and Multi-hop Beaconing in VANETs," in Proceedings of the sixth ACM international workshop on VehiculAr InterNETworking, Beijin, China, 2009, pp. 69-78.

[17]. Weihua Zhuang Hangguan Shan§, "Multihop Cooperative Communication for Vehicular Ad Hoc Networks," 6th International ICST Conference on Communications and Networking in China (CHINACOM), pp. 614-619, 2011.

[18]. Stefan Savage, Keith Marzullo Alper T. Mizrak, "Detecting Malicious Packet Losses," in IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, 2009 , pp. 191-206.

[19]. Amel Makhlouf, Mohsen Guizani Neji Mensi, "Incentives for Safe Driving in VANET," in International Conference on Control Engineering & Information Technology, , 2016, pp. 16-18.

[20]. Daniel D. Stancil, Hariharan Krishnan Fan Bai, "Toward Understanding Characteristics of Dedicated Short Range Communications (DSRC) From a Perspective of Vehicular Network Engineers," ACM: MobiCom '10 Proceedings of the sixteenth annual international conference on Mobile computing and networking, pp. 329-340 , 2010.

International Journal of Engineering Science Invention (IJESI) is UGC approved Journal with Sl. No. 3822, Journal no. 43302.

Babangida Zubairu. "Trust-Based Multihop Routing for Vehicular Ad-Hoc Network." International Journal of Engineering Science Invention (IJESI), vol. 07, no. 01, 2018, pp. 06–14.