ISSN: 2633-4828 Vol. 5 No.3, September, 2023

International Journal of Applied Engineering & Technology

PAODV_RTPDR- A HYBRID APPROACH FOR BLACKHOLE ATTACK PREVENTION IN VANET

Dr. Ajay N. Upadhyaya[1], Dr. Dushyantsinh B. Rathod[2], Dr. Vijay Gadhvi[3], Dr.Ramesh T. Prajapati[4] and Prof. Jashvantkumar R. Dave[5]

[1]Associate Professor, Computer Engineering Department, SAL Engineering & Technical Institute, Ahmedabad, India

[2]Professor, Computer Engineering Department,Ahmedabad Institute of Technology, Ahmedabad, India

[3]Professor, Computer Engineering DepartmentSwaminarayan University, India

[4]Professor, Information Technology Department, Shree Swaminarayan Institute of Technology,Bhat, Gandhinagar, India

[5]Assistant Professor, Information Technology Department, Vishwakarma Government Engineering College, Ahmedabad, Gujarat, India

ABSTRACT

Vehicular Ad hoc Network (VANET) is an advancement of Mobile Ad hoc Network (MANET) which specifically created to do the wireless communication between vehicles and infrastructure. VANET primarily focuseson safety applications and infotainment applications. Most of the safety applications are time constraint and hence timely delivery of VANET messages must be guaranteed. One of the major challenges for VANET is its security. To ensure safety and reliability of the system, security mechanism needs to be implemented which can detect malicious node and take remedial actions. This paper focuses on detection and recovery of Blackhole attack in which a malicious node immediately replies to route requests by source nodes without having an active route to a specified node and drops all the receiving data packets. To improve the performance of the system, authors have presented hybrid approach. Performance of the proposed approach is evaluated based on Packet Drop Rate, Throughput, Average, End to End Delay, Jitter and Network Routing Load.Simulation result shows that the proposed approach outperforms the traditional AODV under Blockhole attack.

Keywords: VANET Security, AODV, Routing Attack, Blackhole Attack, Blackhole Attack Prevention, Drop Rate

1. INTRODUCTION

VANET (*Vehicular Ad hoc Network*) has become an active area of research because it has tremendous potential to improve traffic efficiency and provide vehicular safety with a huge comfort level. Two types of communication are possible in VANET: V2V (Vehicle to Vehicle) and V2I (Vehicle to Infrastructure). Each vehicle is equipped with On Board Unit(OBU) and each cross road is enabled with Road Side Unit (RSU). Many researchers are working on various challenges of VANET likeon-demand communication, dynamic routing, efficient broadcasting, security and QOS (Quality of Service). One of the biggest challenges in VANET is routing due to its high mobility and hence chance of malpractice is also very high. A malicious single node or group of nodes may spoof, modify or block valid routing messages and send corrupted or updated routing information in the network. This malicious activity might result in redirection of some or all network traffic, connectivity issues, high bandwidth consumption and potential denial of services. Blackhole attack, Wormhole attack and Grayhole attack are the different type of VANET routing attacks which attract the network traffic by various methods and disturb the network. For secure VANET communication, there is a need to find the approach which can detect and prevent the network from such malicious activities without adding extra burden on the network.

Paper discusses about a hybrid approach which works in two phases. Initially each node will maintain the list of trusted nodes and non-trusted nodes. First phase detects the attack based on value of Packet Drop Rate (PDR). If high PDR is detected then it will be treated as a probable Blackholeattack. Once Blackhole attack is detected, second phase will be activated to detect and isolate malicious node. In this phase, transmission is done only through trusted nodes.In the said approach, RSU is having the responsibility to detect malicious activities. All the nodes travelling on road maintain the list of trusted nodes and non-trusted nodes.

2. RELATED WORK

VANET is different from other ad-hoc networks due to its unique advantages and characteristics. But due to lack of centralized administration and infrastructure, it becomes vulnerable. There is a need to find a full secure support system if we want to adopt VANET applications and solutions in our real life. Only detection of malicious nodes is not sufficient, there is a need to develop a recovery mechanism through which network's performance can be improved. Sometimes group of nodes work together and do collaborative attacks, which increase the difficulty level of detection and recovery. Many researchers had proposed different solutions for different attacks occurred in VANET.

In [1], authorsdiscussed about detecting and removing malicious nodes from the network using Electronic Vehicle Identification (EVI), manufacturer-signed Electronic Vehicle Identifier Numbers (VIN) and Digital Signature. In [2], authors presented adetailed survey for detection and prevention of Blackhole attack in wireless networks. Comparative analysis for different trust based and hierarchical approaches is also presented. In [3], authors presented the adverse effect of single and collaborative attack and proposed a method for finding a secure routing path under Blackhole attack. Detailed comparative analysis presented for AODV protocol based on performance parameters like throughput, packet delivery ratio, end-to-end delay, network load and node's mobility. Co-operative Bait Detection Approach (CBDA) is a combination of both proactive & reactive detection strategies for detecting malicious activities. In [4], authors proposed methods to defend against Blackholeattack in the network using CBDAwith a malicious node detection algorithm. Packet delivery ratio, end-to-end delay and normalized routing overhead are considered as performance parameters. In [5], authorsdiscussed about detection and avoidanceof wormhole and collaborative Blackhole attack using a trusted AODV routing method with detailed study of different parameters like energy, throughputs and packet delivery ratio using simulator NS2. BPAODV protocol to provide the protection against collaborative Blackhole attack performed by multiple malicious nodes is proposed in [6]. In [7], authorsdiscussed about cooperative cross layer detection in VANET using OLSR Protocol andproposed a cooperative intrusion detection system based on cross layer architecture with a two level monitoring scheme that correlates both MAC and network layers detections. Mobisim simulator is used to simulate the proposed idea. Secure routing mechanism for Blackhole and Grayhole attack is proposed by authors in [8]. In [9], authors proposed a secure MANET routing protocol called BP-AODV (Blackhole Protected AODV) to enhance the security in SAODV protocol and AODV protocol. Proposed protocol provides security against collaborative Blackhole attack and it uses a challenge-response-confirm pattern to establish trusted routes. Implementation is done in NS2 and detailed comparative analysis presented with different scenarios and with various performance parameters like average throughput, average end-to-end delay and average packet delivery ratio. Authors in [10] focused on detection of collaborative attack by malicious nodes with proactive and reactive defense architectures. Proposed approach is simulated using QualNet 4.5 to study effects on performance parameters like packet delivery ratio, routing overhead, average end-to-end delay and throughput. In [11],authorsproposed a secure routing protocol for VANET. Performance analysis is presented using a cryptosystemwith an improved MD5 method. Authors in [12] focused on how to detect malicious nodesin a network using their abnormal behavior and comparison is presented with different performance parameters.

3. PERFORMANCE MEASUREMENT PARAMETERS

In this paper,five parameters are considered for measuring the performance of the proposed system.

Packet Drop Rate (PDR): It defines the total number of packets which are not successfully transmitted over total forwarded packets.

$$PDR_i = \frac{PR_i - PD_i - PS_i}{PR_i - PD_i}$$

Where PDR_i = Packet Drop Rate of Node i, PR_i = Packet Received by Node i, PD_i = Packet destined for Node i, PS_i = Packet Sent by Node i

Average End-to-End Delay: Delay of each packet can be calculated as the difference of start time and end time for a packet. Average End to End Delay can be calculated based on the ratio of total delay of each transmitted packet over total number of transmitted packets.

$$\text{Avg. E2E Delay} = \frac{\sum_{i=0}^{n} [\text{End Time (t2)} - \text{Start Time (t1)}]}{\text{Total No. of Packets}}$$

Network Throughput: Network Throughput is the success rate of message transmission over a particular communication medium.

$$\text{Throughput (Th)} = \frac{\text{Total Data Sent (Kb)}}{\text{Total Time (S)}}$$

Jitter: - Average Jitter is the ratio of variation in the delay over the total number of transmitted packets.

$$\text{Avg. Jitter} = \frac{\sum_{i=0}^{n} [|D(i+1) - D(i)|]}{\text{Total No. of Packets}}, \text{Where Di} = \text{R(time)} - \text{S(time)}$$

Normalized routing load (NRL): It is a ratioof total routing packets over total data packets. For managing packet transmission smoothly some extra routing packets are transmitted with actual data which leads to an extra load or Routing Overhead.

$$\text{Normalized routing load (NRL)} = \frac{\text{No. of Routing Packet Sent}}{\text{No. of Data Packet Sent}}$$

4. PAODV_RTPDR - HYBRID APPROACH FOR BLACKHOLE ATTACK DETECTION AND RECOVERY

PAODV_RTPDR (Preventive AODV - Reactive Trusted Path based on Drop Rate) is a hybrid approach based on trusted path and drop rate. This method will provide a secure solution where there is a chance of collaborative Blackhole attack. In the first phase, RSU checks drop rate and if higher drop rate is observed then it is considered as attack scenario and second phase of isolating malicious node will be triggered.

Algorithm:

Procedure of phase-1 and phase-2 will be repeated after the period of CheckPointTime.

Phase-1 Checking for the attack scenario

This phase is intended to check the network state whether network is safe or affected by Blackhole attack. Detection of Blackhole attack is done based on the value of PDR.

Step 1: All the nodes maintain their list of trusted nodes and list of non-trusted nodes. Initially all the nodes in the neighborhood will be consideredas trusted nodes and will be added in list of trusted nodes and list of non-trusted nodes is empty

Step 2: RSU maintains vector of *PDRList<NodeID, PDR>* and calculates average PDR based on the PDR of individual node. RSU stores the value of *AvgPDR* calculated in each interval.

$$AvgPDR[intervalNo] = \frac{\sum_{i=0}^{N-1} PDR_i}{N}$$

Where PDRi = PDR of i^{th} node, N = Total nodes under consideration

Step 3: If the value of *AvgPDR[intervalNo]* is greater than PDR threshold (*ThPDR*) then it is considered as Blackhole attack situation and phase-2 will be triggered for identifying and isolating malicious node from the network.

Phase-2 Identifying and isolating malicious node

Step 4: RSU sorts the vector *PDRList* based on the value of PDR and the node with highest PDR will be considered as suspected node.

SusNodeID = PDRList[N-1]<NodeID>

Step 5: After identifying suspected node, RSU broadcasts its details to each node within the range of RSU by route notification message *RouNoti<SusNodeID, "Suspend", RecoveryTime>*and inform them not to do any communication with suspected node for the period of SuspendTime to avoid packet loss. The value of SuspendTime is double the value of CheckPointTime. The route notification message is also communicated to other RSUs.

Step 6: After the period of SuspendTime, RSU again calculates *AvgPDR[intervalNo]*. Based on the comparison of *AvgPDR[intervalNo]* and *ThPDR* there are three possible cases.

Case-1: If the value of *AvgPDR[intervalNo]*is found less than *ThPDR* then the suspected node is actually a malicious node. RSU broadcast route notification message *RouNoti<SusNodeID, "Non-trusted">* to inform all other nodes about the same. Upon receiving this route notification message, all the nodes will put SusNodeID in their list of non-trusted nodes.

Case-2: If the value of *AvgPDR[intervalNo]* is greater than the *ThPDR*but improved with compare to previous value of *AvgPDR[intervalNo-1]* then there may be possibility of collaborative Blackhole attack. In this case, RSU broadcasts route notification message *RouNoti<SusNodeID, "Non-trusted">*stating that current suspected node is malicious node. Upon receiving this route notification message, all the nodes will put SusNodeID in their list of non-trusted nodes. Along with this, to detect other malicious nodes, system repeats step-4 to step-6 skipping *SusNodeID*.

Case-3: If the value of *AvgPDR[intervalNo]* is greater than *ThPDR* and it is almost similar to the *AvgPDR[intervalNo-1]*, then suspected node is actually not a malicious node and RSU broadcasts route notification message *RouNoti<SusNodeID, "Trusted">* stating that current suspected node is trusted node. System repeats step-4 to step-6 to find actual malicious node.

5. Simulation Result and Discussion

Performance of the proposed protocol is compared with the performance of simple AODV protocol and AODV with Blackhole attack. Simulation parameters mentioned in Table 1 are used to configure traffic simulator SUMO and network simulator NS-2. Performance of the proposed approach is evaluated based on Packet Drop Rate (PDR), Network Throughput, Average End-to-End Delay, Jitter and Normalized Routing Load (NRL). To get accurate result, all the scenarios are simulated five times and the average result of observations is presented in Table 2.

Table 1. Simulation Parameters

Parameters	Specification
No. of Vehicle	100,500,1000,2000
Simulation Time	1000 Sec
Type of Packet Send	UDP (User Datagram Protocol)
Max. Speed of Vehicle	10/20/30 m/s
Length & Type of Vehicle	3 meter - Car
Transmission of OBU & RSU	100 m-OBU & 250m- RSU
Routing Protocol	AODV

Simulator	SUMO 0.32.0, MOVE, NS2-2.34
Node Movement	Random

Table 2 Average Result

Sr. No.	Protocol	No. of Nodes	PDR (%)	Th (kbps)	E2ED (ms)	Jitter (ms)	NRL (%)
1	AODV	100	3.57	114.17	75.18	0.0359	2.9628
		500	3.90	548.49	86.45	0.0448	6.1744
		1000	4.53	1055.98	90.26	0.0621	9.6363
		2000	5.03	2004.99	106.02	0.1042	12.2412
2	AODV Under Blackhole Attack	100	86.18	16.36	325.1	0.1553	2.7553
		500	88.70	64.46	456.92	0.1856	5.1251
		1000	90.38	106.42	557.03	0.2155	7.6378
		2000	91.98	169.36	778.35	0.2475	9.4966
3	PAODV_RTPDR	100	14.50	101.23	79.71	0.0875	3.0680
		500	16.40	477.19	93.41	0.0976	6.5299
		1000	17.68	910.54	98.40	0.1061	10.3401
		2000	19.10	1707.99	116.98	0.1021	13.4955

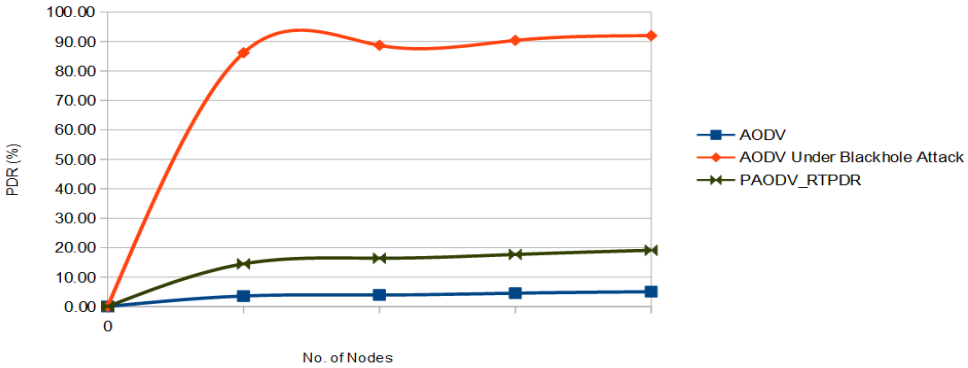

Fig1: Packet Drop rate Analysis

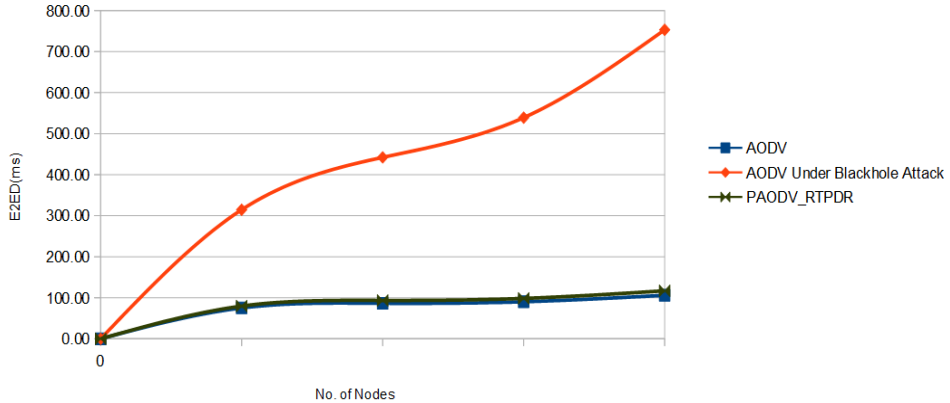

Fig 2: Average End to End delay Analysis

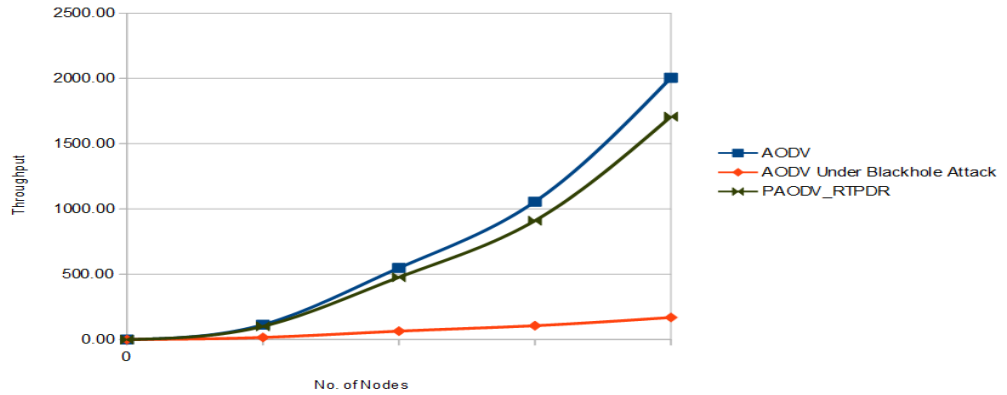

Fig 3: Throughput Analysis

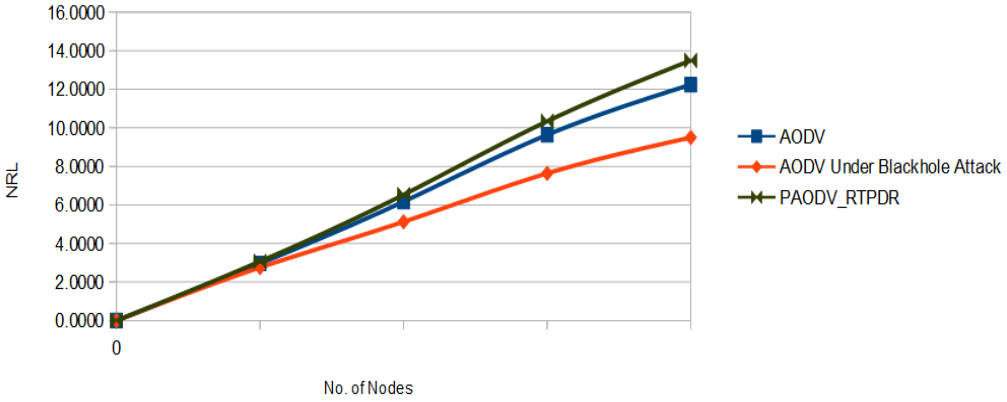

Fig4: Normalized Routing Load Analysis

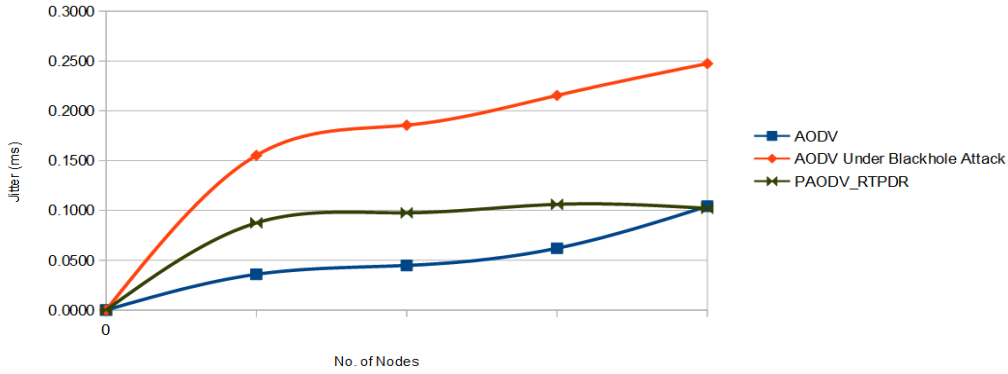

Fig5: Jitter Analysis

Figure 1 plots changes in PDR for five different network scenarios (viz., network in normal state, under Blackhole attack, under proposed approach with one, two and three malicious nodes). It is evident that PDR remains steady when the network is in normal state (PDRnorm) and it jumps to a very high level (PDRatt) and remains at same level under Blackhole attack. Our proposed approach helps the network recover in a short span and attain PDR near to its normal value. When the network is under Blackhole attack, PDR shoots up to a higher value (PDRhigh1) and gradually reduces near to PDRnorm. It is important to note that PDRhigh1 is significantly less than PDRatt. This is so considering only one malicious node. PDR for two malicious nodes case (PDRhigh2)

jumps to a higher value than PDRhigh1 but remains less as compared to PDRatt and reduces near to PDRnorm in very short time. Similar behavior is noted in case of three malicious nodes as well.

Figure 2 and Figure 5 demonstrate the effect of Blackhole attack on End-toend delay and Jitter. End-to-end delay and Jitter is observed to be increasing by a significant margin once the network is under Blackhole attack. This increase can be due to two reasons. Blackhole attack blocks routes to the destination nodes resulting in packets reaching the destination via alternate path. For many nodes, the blocked path could be the shorter path and hence the packets delivered via alternate path take more time resulting in increase in E2E delay. Also, this attack may fully isolate nodes which are reachable only via the malicious node(s). For such nodes, the E2E delay is infinity as the packet never reaches the destination.

Due to Blackhole attack, many packets get dropped by malicious node and hence as shown in Figure 3, the throughput value is very low. In proposed approach, malicious node will be detected and isolated in quick time which shall increase the throughput value.

In proposed approach, control messages like route notification messages are exchanged between the nodes and RSU for detection and isolation of malicious node(s). This increases overall traffic overhead of the network. But the Figure 4 clearly shows that increase in traffic due to these notification messages is not significant as compared to overall traffic of the network.

Improvement observed for all the performance parameters due to implementation of proposed approach is presented in Table-2 and the same is visually presented in Figure 6.PDR is improved by 72.39%, approximately 13% improvement is observed for Throughput, End-to-end delay and Jitter is improved by 19.41% and 49.88% respectively and additional 6.71% load needs to be bared by network.

Table 3 Improvement through Blackhole Prevention Methods PAODV_RTPDR

No. of Nodes	PDR Improvement (%)	Throughput Improvement (%)	E2ED Improvement (%)	Jitter Improvement (%)	NRL Additional Load (%)
100	71.68	16.16	24.52	56.37	3.5524
500	72.30	13.51	20.44	52.61	5.7579
1000	72.70	11.69	17.67	49.26	7.3036
2000	72.88	9.92	15.03	41.26	10.2460

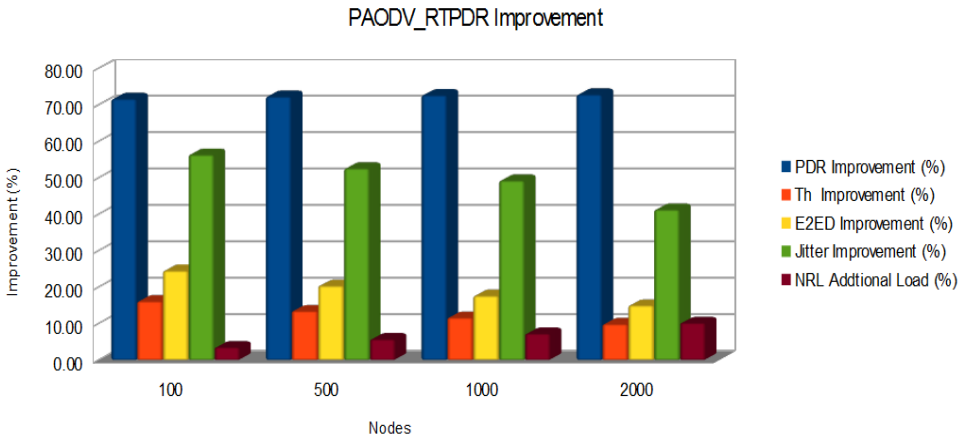

Fig 6: Improvement using Hybrid method

6. CONCLUSIONS

Packet Drop Rate and Trusted path based detection and recovery form Blackhole attack is presented in the paper. Both single and collaborative Blackhole attack scenarios are simulated using SUMO and NS-2. Authors have presented performance analysis of the proposed approach based on various performance parameters like packet drop rate, throughput, End- to-end delay, jitter and network routing load. Comparing the Blackhole attack scenario, approximately 71% improvement is observed in packet drop ratefor the proposed approach.Value of other performance parameters is also improved whereas minor increase in network routing load is observed.

REFERENCES

[01] J. Tobin, C. Thorpe and L. Murphy, "An Approach to Mitigate Black Hole Attacks on Vehicular Wireless Networks," *2017 IEEE 85th Vehicular Technology Conference (VTC Spring)*, Sydney, NSW, 2017, pp. 1-7.

[02] S. Ali, M. A. Khan, J. Ahmad, A. W. Malik and A. ur Rehman, "Detection and prevention of Black Hole Attacks in IOT & WSN," *2018 Third International Conference on Fog and Mobile Edge Computing (FMEC)*, Barcelona, 2018, pp. 217-226.

[3] V. G. Mohite and L. Ragha, "Security agents for detecting and avoiding cooperative blackhole attacks in MANET," *2015 International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT)*, Davangere, 2015, pp. 306-311.

[4] N. G. Wakode, "Defending blackhole attack by using acknowledge based approach in MANETs," *2017 International Conference on IoT and Application (ICIOT)*, Nagapattinam, 2017, pp. 1-6.

[5] N. Arya, U. Singh and S. Singh, "Detecting and avoiding of worm hole attack and collaborative blackhole attack on MANET using trusted AODV routing algorithm," *2015 International Conference on Computer, Communication and Control (IC4)*, Indore, 2015, pp. 1-5.

[6] A. M. El-Semary and H. Diab, "BP-AODV: Blackhole Protected AODV Routing Protocol for MANETs Based on Chaotic Map," in *IEEE Access*, vol. 7, pp. 95197-95211, 2019.

[7] R. Baiad, H. Otrok, S. Muhaidat and J. Bentahar, "Cooperative cross layer detection for blackhole attack in VANET-OLSR," *2014 International Wireless Communications and Mobile Computing Conference (IWCMC)*, 2014, pp. 863-868, doi: 10.1109/IWCMC.2014.6906469.

[8] S. Godse and P. Mahalle, "Secure & Efficient Routing Mechanisms in VANET Using CBDS," *2017 International Conference on Computing, Communication, Control and Automation (ICCUBEA)*, 2017, pp. 1-6, doi: 10.1109/ICCUBEA.2017.8463722.

[9] A. M. El-Semary and H. Diab, "BP-AODV: Blackhole Protected AODV Routing Protocol for MANETs Based on Chaotic Map," in *IEEE Access*, vol. 7, pp. 95197-95211, 2019, doi: 10.1109/ACCESS.2019.2928804.

[10] J. Chang, P. Tsou, I. Woungang, H. Chao and C. Lai, "Defending Against Collaborative Attacks by Malicious Nodes in MANETs: A Cooperative Bait Detection Approach," in *IEEE Systems Journal*, vol. 9, no. 1, pp. 65-75, March 2015, doi: 10.1109/JSYST.2013.2296197.

[11] A. P. Jadhao and D. N. Chaudhari, "Security aware routing scheme in Vehicular Adhoc Network," *2018 2nd International Conference on Inventive Systems and Control (ICISC)*, 2018, pp. 1374-1379, doi: 10.1109/ICISC.2018.8399033.

[12] U. Khan, S. Agrawal and S. Silakari, “Detection of malicious nodes (DMN) in vehicular ad-hoc networks,” Procedia Computer Science, vol. 46, pp. 965–972, 2015.