Revue d'Intelligence Artificielle
Vol. 33, No. 1, February, 2019, pp. 9-13
Journal homepage: http://iieta.org/journals/ria

Isolation of Wormhole Attackers in IOV Using WPWP Packet

Satya Sandeep Kanumalli[1,2*], Anuradha Chinta[3], Patanala Sri Rama Chandra Murty[1]

[1] CSE Department, Acharya Nagarjuna University, Guntur 522510, India
[2] CSE Department, Vignan's Nirula Institute of Technology & Science for Women, Guntur 522510, India
[3] CSE Department, Velagapudi Ramakrishna Sidhartha Engineering College, Vijayawada 52007, India

Corresponding Author Email: satyasandeepk@gmail.com

https://doi.org/10.18280/ria.330102

Received: 11 December 2018
Accepted: 20 January 2019

Keywords:
network, VANET, IOV, collision

ABSTRACT

IOV is a unique form of VANETS network with a special kind of remote system which is arranged with set of versatile vehicles that can be effortlessly included and expelled from the system with no incorporated organization where each node acts as both sender / receiver and a Hub which forwards the packets. Owing to absence of centralized administration, Nodes in IOV are exposed to various network layer attacks. Among them, the Wormhole attack is one of its kind of attack and must to be addressed with high attention. In this paper, we propose and implement a new algorithm to detect the tunneling attack. The performance of the proposed algorithm is evaluated against various existing algorithms and a comparison is made with our proposed Wormhole Path Watcher Packet (WPWP) technique using NS2 tool.

1. INTRODUCTION

Communication in IOV has got attention rapidly from last era due to advancement in transportation systems and its unique characters [1]. VANETS changing its face to IOV as the speculation for the future demand for fully autonomous cars have been increased as the whole system is fully dependent on wireless communication which leads to various advancements in production of the vehicles and various new applications can be developed in with different vehicles can form a social network by connecting and communicating different multimedia content, these nodes effortlessly included and expelled from the system with no incorporated organization where each node acts as both host and router.

These vehicles exposed to various types of security issues. Mostly, VANETS suffers from denial of service attack which a user is denied of the service of resource he would normally except to have [2, 3]. Generally, DOS attack is performed by the adversary at different layers of network stack which are physical, network and application layers. Apart from physical and application layers network layer attacks are easy to implement and difficult to detect. VANETs are exposed to various network layer attacks like black hole, wormhole [4, 5].

Particularly, wormhole intrusion is a most dangerous due to its special propertys with the help of tunnel rapidly guide the captured packets from one adversary node to its collaborative adversary. In this article we propose an efficient and reliable method to detect and isolate wormhole nodes in the network by hopcount, delay and a special packet wormhole path watcher packet. The rest of the paper is organized as follows section-II deals with various existing mechanisms to Detect wormhole attack, section-III deals with proposed algorithm to detect wormhole attack detection, section-IV deals with simulation results, section-V concludes the paper and section-VI gives future work.

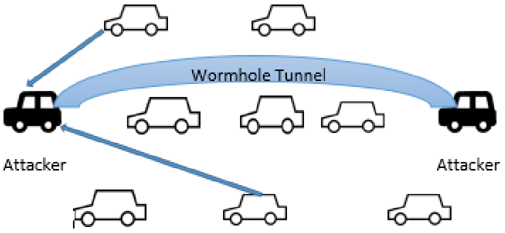


Figure 1. Wormhole attack

2. RELATED WORK

Juhi Biswas et al. propose a calculation to identify wormholes with no extraordinary hardware's. This work WADP is a change over beforehand given WAP in a way that WAP experienced false recognition where as WADP is free from false discovery when uncovered wormhole assault are propelled as it comprise of identification of noxious hubs through credibility test and further affirmation of wormhole presence by ascertaining delay per bounce if there should arise an occurrence of uncovered assaults and by neighbor hub checking in the event of shrouded assaults. Our system is executed in light of the changed AODV convention.

Aarfa Khan et al. [6] proposes NWLIDS calculation to alleviate the disadvantages in Local Intrusion Detection (LID) security directing instrument. Also, propose new component called Normalized Wormhole Detection System (NWLIDS) security directing instrument to permit the discovery of the aggressor to be locally; In this when the suspected middle of the road hub unicast the RREP towards the source hub the past hub to the transitional hub performs the procedure of location and not the source hub as appeared. In the first place, the past hub cushions the RREP parcel. Second, it utilizes another course to the following hub and sends FRREQ bundle to it. At the point when the past hub gets the FRREP parcel from the following jump hub, it extricates the data from the FRREP bundle and carries on as indicated by taking after tenets: If the following hub have a course to middle of the road hub and destination hub, the past bounce hub dispose of the FRREP, then unicast the RREP to the source hub. In the event that the following bounce has no course to the destination hub or the transitional hub or them two, the past hub disposes of the cushioned RREP and the FRREP also, in the meantime telecasts the alert message to report the wormhole vicinity.

Vasiliy Krundyshev, Maxim Kalinin et al. [14] have proposed Artificial Swan which is based on trust in which the whole work is divided in to building a path and maintenance of the existing paths and detection of the malicious nodes by comparing the trust values with a threshold.

Parmar Amisha et al. [15] have proposed a solution based on AMODV routing in which total roundtrip time is calculated and the malicious nodes are detected by comparing it with normal AMODV, it have shown a good result.

3. PROPOSED ALGORITHM

Wormhole attack is a more concentrating seeking attack in order to detect and isolate the wormhole nodes in IOV is a challenge issue. Here we propose WPWP algorithm, which is an efficient method to detect and isolate wormhole [6]. In this approach we don't require any special kind of hardware just by using one special packet (WPWP), hop-count and delay per hop to detect wormhole nodes.

- *Hop-count*: Number of intermediate nodes between source and target. Which is gets from RREQ packet [7].
- *Delay*: The amount of time taken for a packet to travel from source to destination is called delay.
- *WPWP packet*: Wormhole [8] Path Watcher Packet is a test packet it contains source ID, destination ID, sequence number and hop count field.

WPWP packet is a lightweight packet, which does not consume much bandwidth. Whenever a vehicle receives this WPWP packet the receiving vehicle must send acknowledgement packet back to the source vehicle. A brief description of the algorithm is shown in algorithm 1. In step1 we send RREQ packet and get hop-count, delay. From this if the path having very less or very large delay and hop-count less than or equals to 4 goto step 2 and send the WPWP packet for four times. If we get acknowledgement 3 or more times no wormhole otherwise paths suspected chance of wormholes [9], [10]. So go to step 3 and store all the intermediate Vehicle ids and go to step1 again takes a new path until and unless getting of reliable path. then go to step4 to isolate the wormhole nodes.

```
Step1:- Route Discovery
function ROUTE DISCOVERY(hc, Del) .
 Where hc – hop count, Del - delay from
  RREP packet
    count = 0
    Step2:- worm-path-watcher packet
  transmission
    if hc <= 4||Del > 100||Del < 10 then
    for i = 0 to 4 do
            Sender to WPWP Packet to reciever
                    if Ack >= 3 then
                    No wormhole
            Continue the data transfer
                    else
                    Warmhole
                     goto step3
                    end if
    end for
    end if
Step3:- storing Vehicle ID's in suspected
paths
for i = 0 to hc do
            Id[i] = vehicle id
            get(intermediateVehicle IDs)
            count = count + 1
            goto step1
end for
goto step4
Step4:- comparison of suspected lists
sortlists()  For comparison we use
sorting
counduplicates(ndup)
if ndup >= count-2 then
Detected wormhole Vehicle IDs
end if
end function
```

4. PERFORMANCE ANALYSIS

The recreations were performed utilizing Omnet++. With Veins communicating with SUMO with a traffic scenario containing (10, 30 and 50) number of vehicles moving in a region territory of 1024 x 1000 meters.

Hear we utilizes satisfactory parcel rate and unpredictable interruption times to reenactment and we actualize WPWP procedure to identify the wormhole Vehicles in the system, the execution is done by using AODV [11, 12] as routing protocol for the V2v communication, different comparisons are made with WPWP and without WPWP and calculations are done by shifting the quantity of wormhole vehicles in the system.

Also, we analyzed different execution measurements of parcel conveyance part, throughput and end to end delay. The reenactment parameters are outlined in Table 1.

Table 1. Simulation paramètres

Parameter	Values
Traffic type	CBR
Number of nodes	10, 20 and 30
Simulation time	1000 Sec.
Pause time	0, 1, 2, 3, 4 and 5
Simulation area	1024×800 mts
Mobility	0 to 20 mts/sec.

4.1 Performance metrics

- Packet Delivery Fraction: It is the proportion of aggregate number of parcels got to the aggregate number of bundles exchanged.
- Throughput: Number of packets transferred in unit time from source to target is called throughput.
- End To End Delay: The time taken by a packet exchanged from source to destination is called end to end delay

Here AODV routing protocol [13] is tested with wormhole nodes in the network and after initialization of WPWP technique in the routing, network performance is tested using various performance metrics and varying the number of vehicles in the network.

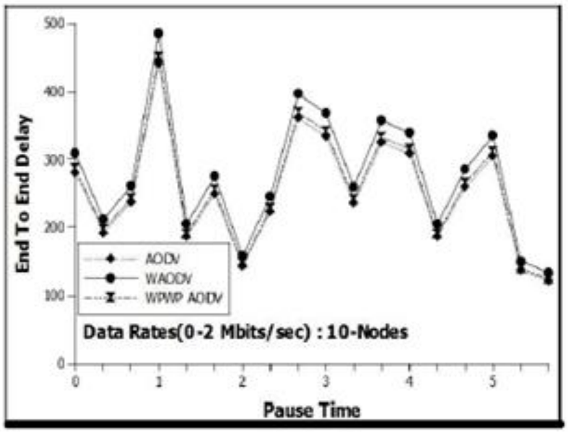


Figure 2. 10-nodes end to end delay

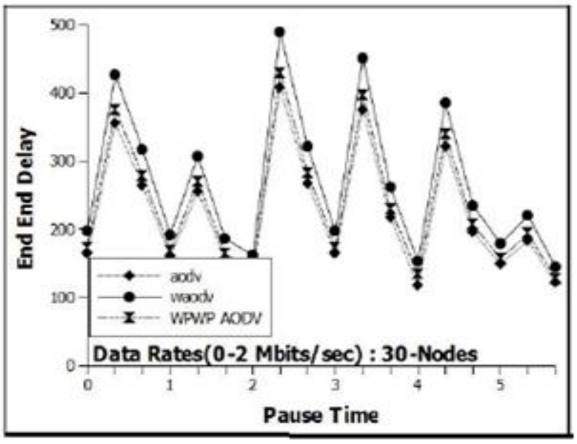


Figure 3. 30-nodes end to end delay

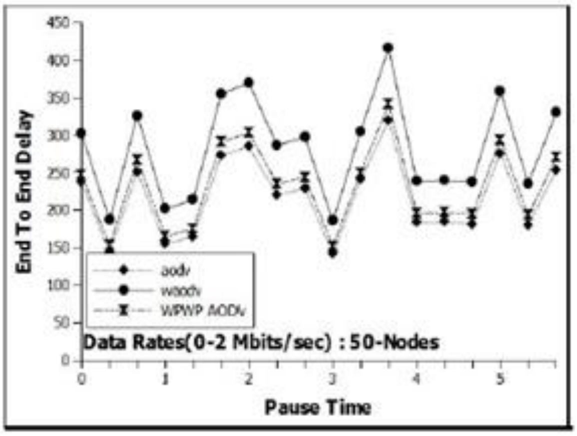


Figure 4. 50-nodes end to end delay

Figure 2, Figure 3, and Figure 4 show the end to end delay of 10, 30 and 50 nodes in normal situation, under wormhole attack and under WPWP. Under WPWP end to end delay is moderate with 10 nodes and for 30 and 50 decreases drastically compared to wormhole AODV, but it is greater than normal as it induces some computation which itself take some delay processing at the ends which can be ignored as it is so marginal but when some of the computation is shared with RSU it gives better results which brings down end to end delay significantly.

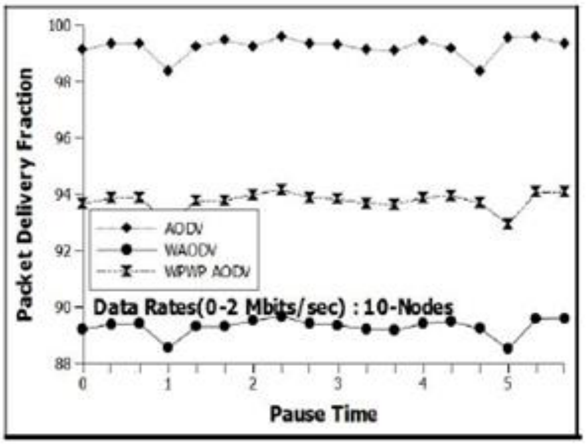


Figure 5. 10-nodes packet delivery fraction

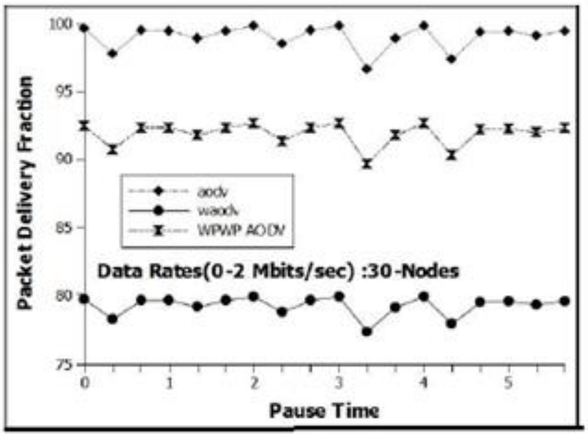


Figure 6. 30-nodes packet delivery fraction

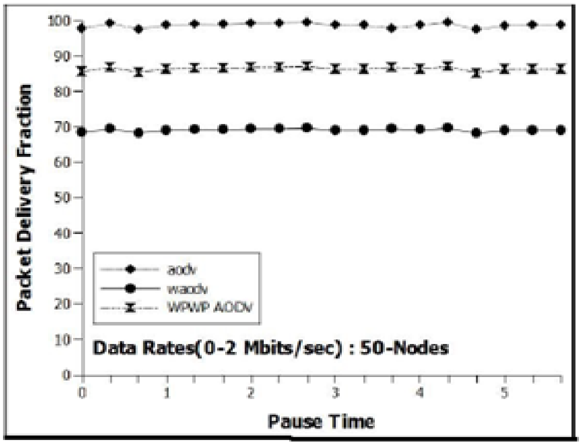


Figure 7. 50-nodes packet delivery fraction

Figure 5, Figure 6, and Figure 7 show the packet delivery fraction of 10, 30 and 50 nodes in normal situation, under wormhole attack and under WPWP. Under WPWP packet delivery fraction increases countably compared to wormhole AODV as the number of packet drops by the attackers reduces drastically as the attacking nodes are isolated which shows a significant improvement in the defense against wormhole attacks.

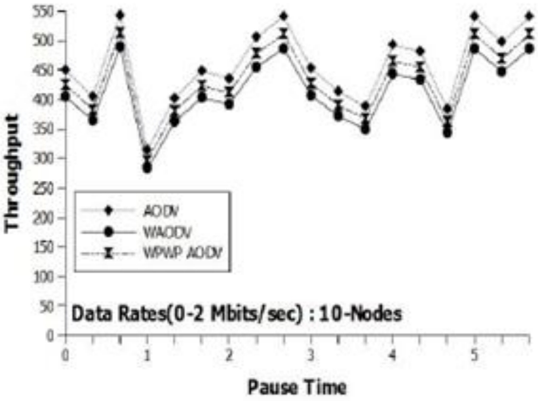


Figure 8. 10-nodes throughput

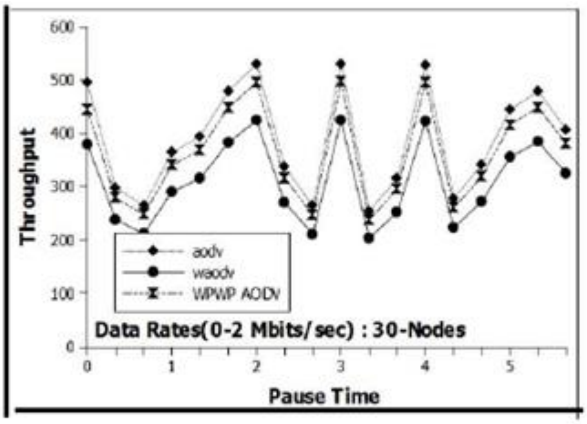


Figure 9. 30-nodes throughput

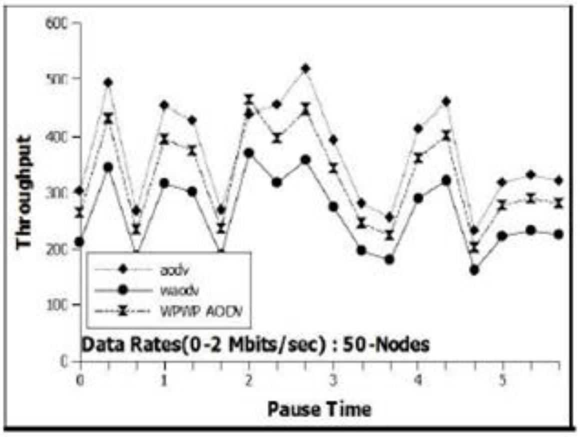
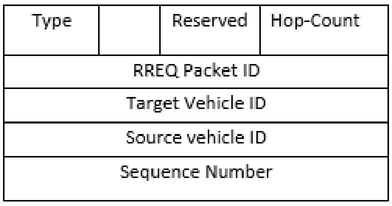


Figure 10. 50-nodes throughput



Type		Reserved	Hop-Count
RREQ Packet ID			
Target Vehicle ID			
Source vehicle ID			
Sequence Number			

Figure 11. Simple RREQ packet format

Figure 8, Figure 9 and Figure 10 show the Throughput of 10, 30 and 50 nodes in normal situation, under wormhole attack and under WPWP. Under WPWP throughput increases extremely compared to wormhole AODV as the number of packets exchanged over the network increases it shows consistency with the change in the number of vehicles but if they are too many wormhole attackers in the network the throughput may decrease due to not enough number of nodes can exchange messages it may also increase end to end delay as a packet may travel longer distance than usual as the shortest path contain the vehicle that may be identified as attacker and isolated. Figure 11 depicts a simple RREQ packet format.

5. CONCLUSION AND FUTURE WORK

In IOV for V2v communication with AODV routing protocol is tested with wormhole nodes in the network and after initialization of WPWP technique in the routing to detect and isolate wormhole is utilized. The network performance is tested using various performance metrics and varying the number of nodes, which showed a significant improvement as our future work, we would decrease the additional overhead caused by the WPWP test packet to test the path a greater number of times.

REFERENCES

[1] Belding-Royer, E.M., Perkins, C.E. (2003). Evolution and future directions of the Ad Hoc on-demand distance vector routing protocol. J. Ad Hoc Networks, 1(1): 125-150. https://doi.org/10.1016/s1570-8705(03)00016-7

[2] Johnson, D.B., Maltz, D.A., Hu, Y., Jetcheva, J.G. (2002). The dynamic source routing protocol for mobile Ad Hoc networks (DSR). The Dynamic Source Routing Protocol, Internet draft.

[3] Perkins, C.E. (2000). Ad Hoc Networking. 1st edition-Addison-Wesley Professional.

[4] Basagni, S., Conti, M., Giordano, S., Stojmenovic, I. (2004). Mobile Ad Hoc Networking. A John Wiley & Sons, Inc.

[5] Biswas, J., Gupta, A., Singh, D. (2012). WADP: A wormhole attack detection and prevention technique in MANET using modified AODV routing protocol. International Conference on Industrial & Information Systems, IEEE. https://doi.org/10.1109/ICIINFS.2014.7036535

[6] Khan, A., Shrivastava, S., Richariya, V. (2014). Normalized Worm-hole Local Intrusion Detection Algorithm (NWLIDA). Intern. Conf. on Computer Communication and Informatics (ICCCI), Coimbatore, pp. 1-6. https://doi.org/10.1109/ICCCI.2014.6921748

[7] Kanumalli, S.S., Anuradha, C., Murty, P.S.R.C. (2018). An efficient method for detection of Sybil attackers in IOV. Advances in Modelling and Analysis A, 61(1): 5-8. https://doi.org/10.18280/ama_b.610102

[8] Pathan, A.K. (2016). Security of self-organizing networks: MANET, WSN, WMN, VANET. CRC Press. https://doi.org/10.1201/EBK1439819197

[9] Contreras-Castillo, J., Zeadally, S., Guerrero-Ibañez, J.A. (2018). Internet of vehicles: Architecture, protocols, and security. IEEE Internet of Things Journal, 5(5): 3701-

3709. https://doi.org/10.1109/JIOT.2017.2690902

[10] Gopi, A.P., Babu, E.S., Raju, C.N., Kumar, S.A. (2015). Designing an adversarial model against reactive and proactive routing protocols in MANETS: A comparative performance study. Intern. J. of Electrical and Computer Engineering, 5(5): 1111-1118.

[11] Hayajneh, T., Krishnamurthy, P., Tipper, D. (2009). DeWorm: A simple protocol to detect wormhole attacks in wireless Ad Hoc networks. Third Intern. Conf. on Network and System Security, Gold Coast, QLD, pp. 73-80. https://doi.org/10.1109/NSS.2009.85

[12] Yang, F.C., Wang, S.G., Li, J.L., Liu, Z.H., Sun, Q.B. (2014). An overview of internet of vehicles. China Communications, 11(10): 1-15. https://doi.org/10.1109/cc.2014.6969789

[13] Cheng, J.J., Cheng, J.L, Zhou, M.C., Liu, F.Q., Gao S.C., Liu, C. (2015). Routing in internet of vehicles: A review. IEEE Transactions on Intelligent Transportation Systems 16(5): 1-14. https://doi.org/10.1109/TITS.2015.2423667

[14] Krundyshev, V., Kalinin, M., Zegzhda, P. (2018). Artificial swarm algorithm for VANET protection against routing attacks. 2018 IEEE Industrial Cyber-Physical Systems (ICPS), IEEE. https://doi.org/10.1109/ICPHYS.2018.8390808

[15] Amisha, P., Vaghelab, V.B. (2016). Detection and prevention of wormhole attack in wireless sensor network using AOMDV protocol. Procedia Computer Science, 79: 700-707. https://doi.org/10.1016/j.procs.2016.03.092