International Journal of Advanced Research in Engineering and Technology (IJARET)
Volume 10, Issue 3, May-June 2019, pp. 217-224, Article ID: IJARET_10_03_022
Available online at http://www.iaeme.com/ijaret/issues.asp?JType=IJARET&VType=10&IType=3
ISSN Print: 0976-6480 and ISSN Online: 0976-6499
© **IAEME** Publication

PAODV_RTPSN- A HYBRID APPROACH FOR BLACKHOLE ATTACK PREVENTION IN VANET

Dr. Ajay N. Upadhyaya
Computer Engineering Department,
Ahmedabad Institute of Technology, Ahmedabad, India

Dr. J.S. Shah
Computer Engineering Department, Ex. Principal,
Government Engineering College, Patan, India

ABSTRACT

For secure VANET communication first system has to discover who the attackers are and how they can damage the VANET communication. Attackers disturb the communication by getting full or partial access in communication of network. Based on the participation nature of attackers we can detect the different attackers. VANET communication must be secure and must having surety that transmitted message is not inserted, deleted or modified by any attackers. Detection of such attackers will only give improvement up to some extent, but there is a need to identify a method which prevents such attackers before spreading attack in other VANET communication areas. In this paper we presented the analysis of hybrid preventive approach PAODV_RTPSN (Preventive AODV - Reactive Trusted Path based on Sequence Number). We presented the improvement of hybrid method under blackhole routing attack with the detail comparative analysis of different parameters like Packet Drop Rate, Throughput, Average End to End Delay, Jitter and Network Routing Load.

Key words: VANET, Security, AODV, Routing Attack, Blackhole Routing Attack, AODV_RTPSN.

Cite this Article: Dr. Ajay N. Upadhyaya, Dr. J.S. Shah, PAODV_RTPSN- A Hybrid Approach for Blackhole Attack Prevention in VANET, *International Journal of Advanced Research in Engineering and Technology*, 10 (3), 2019, pp 217-224.
http://www.iaeme.com/ijaret/issues.asp?JType=IJARET&VType=10&IType=3

1. INTRODUCTION

In VANET, communication is done between V2V (Vehicle to Vehicle) and V2I (Vehicle to Infrastructure). In VANET each vehicle is equipped with OBU (On Board Unit) and each cross road enabled with RSU (Road Side Unit). VANETs is having different security requirement for governing proper vehicular communication. For secure VANET communication there is a need to find the advance methods which can detect such malicious attackers without adding extra burden on network. Here we will discuss hybrid approach which is actually based on two different methods. In first part first method is activated which is based on detection of higher Sequence Number in a transmitted data. Initially every node will maintain the list of Trusted nodes and Non-trusted nodes. If source node will receive reply from any node with largest sequence number then it will be considered as a possibility of Routing attack. After detection of such malicious behavior second method activated, we named it as trusted path method. In said approach RSU is having a responsibility to detect malicious node. RSU will manage List of Trusted node and Non-Trusted node. In this mode transmission done only through trusted path which is identified based on repeated entry of common path.

2. RELETED WORK

VANETs are particularly prone to malicious behaviour. Due to the lack of any centralized authority VANETs becomes very vulnerable to eavesdropping and infiltration. Loopholes in security are the major barrier in adoption of VANET in commercial application. Only detection of routing attack like blackhole is not enough there is a need to find the preventive methods which breaks the spreading of such attacks. The recent research work different researcher had proposed different solutions for the domain of blackhole attack prevention.

In [1-5,10-11] the different solutions are proposed by authors for establishing trust management in VANETs. In trust management trust level can be establishing by nodes on other car nodes by their OBU or by RSU-Infrastructure Nodes. Trust is a very difficult task to achieve in VANETs because it is decentralized in nature. The movement of any car nodes in the range of RSU is unpredictable. In this solution need to build trust table based on the trust values given by other vehicle which they collected from their neighbouring vehicles. In [6], author discussed about cryptographic methods and with the help of key exchange mechanism neighbour node authentication is done. In [7], author presented the effects of blackhole attack with routing protocols AODV and DOV. In paper they proposed a hybrid protocol which is having benefits of AODV and DSR. In [8], author presented performance analysis of DOA and AODV Routing Protocols with Black Hole Attack. In [9], author discussed about cooperative cross layer detection for blackhole attack by improving the watchdog detection method.

3. PERFORMANCE MEASUREMENT PARAMETERS

For measuring the performance here, we taken five different parameters: Packet Drop Rate (PDR), Average End-to-End Delay (E2ED), Network Throughput, Jitter and Normalized routing load (NRL).

Packet Drop Rate defines the total number of packets drop over total number of transmitted packets. Average End-to-End Delay is based on total average transmission time of each packet from source to destination. Throughput defines the success rate of message transmission over a particular communication medium. Average Jitter is the variation in the delay introduced by the vehicle components along the communication path in VANET. Every protocol is adding routing information for managing packet transmission smoothly. The addition of this packet is considered as an extra load or Routing Overhead for data packet transmission which specifies the stress level added by particular protocol.

4. PAODV_RTPSN - HYBRID APPROACH FOR BLACKHOLE ATTACK PREVENTION

This hybrid concept of trusted path and sequence number named as a "Preventive AODV - Reactive Trusted Path based on Sequence Number (PAODV_RTPSN)". This method is having a two level of security with the reduction mechanism in total load on network which generally we have to face in simple preventive methods. In first level of this method if source node will receive reply from any node with largest sequence number then it will be considered as a malicious node detection who want to impose blackhole attack on network and particular node will enable level-2 security which is based on establishment and following of trusted path mode for transmission. As advancement it will inform all other nodes with the help of RSU for follow Trusted path.

Algorithm:

Step 1: Initially source node, which is unaware about the position of destination node broadcast Route Request Message (RREQ).

SN → RREQ [SN_ID, DN_ID, SN_SEQ_NO, BROD_ID]

Step 2: Different nodes will receive RREQ broadcasted by Source Node and based on it different node will send Route Reply Message (RREP) to Source Node.

SN ← RREP [DN_ID, SN_ID, DN_SEQ_NO, HOP_COUNT, LIFE_TIME]

Step 3: Initially all neighbour nodes will be considered as a Trusted Nodes, List_Trusted_Node will store Node_Id of its neighbours.

```
Create Trust_Node_List ( )
{
SN [List_Trusted_Node] ← NN[N_ID]
SN [List_Non_Trusted_Node] ← null
}
```

Step 4: If source node receives any route reply with very larger Sequence Number, which is having difference with source sequence number more than 2^{16} then particular node, will be treated as malicious node.

```
RREP_CHECK ()
{
For each (NN (RREP))
{   If (Diff(DN_SEQ,SN_SEQ) > $2^{16}$ then
        DN = MN
        Update_Trust__Node_List ()
        {
        SN [List_Trusted_Node] ← Remove (DN[N_ID])
  SN [List_Non_Trusted_Node] ← Add (DN[N_ID])}
       End if
    }
}
```

Step 5: Now there is a need to activate the trusted path mode. It will be very helpful in collaborative blackhole attack. Now source node will transmit data only through the node which is having entries in trusted path. As well as node will send non trusted node list to respective RSU.

```
Enable Trusted Path ()
{
Create Trusted Path List ()
{
TPL ← Repeat_Entry(Routing Table) && In( SN [List_Trusted_Node])
}
Route_Selection()
{
   If found (TPL) then
Select_Route ← TPL (Min (Hop_Count))
   Else
Select_Route ← RT (Min (Hop_Count))
  End If;
}
}
```

Step 6: RSU will collect list of all Non-trusted node list from each node inside the range and based on that prepare the block node list. This block node list will be forwarded to each node in the range of RSU. As well as RSU inform other nodes to enable trusted path based transmission.

```
Manage Block_node_List ()
{
RSU [Block_Node_List] ← SN [SN_ID, List_Non_Trusted_Node]  }
EN ← RSU [Enable Trusted Path]
EN ← RSU [Block_Node_List]
}
```

Step 7: All Nodes will Enable the Trusted path mode for a random period of time and update Trusted and non-trusted Node list based on the updates given by RSU.

```
Update_Trust_Node_List ()
{
   SN [List_Trusted_Node] ← Remove (MN[MN_ID])
   SN [List_Non_Trusted_Node] ← Add (MN[MN_ID])
}
```

5. IMPROVEMENT ANALYSIS OF PAODV_RTPSN IN VANET

Here we considered some of the parameters as a performance Metrics like Packet Drop Rate (PDR), Network Throughput and Average End-to-End Delay. We simulated scenario in NS2 for 500 numbers of nodes for the 1000 second. We will analyze the parameters as per the discussion in section-4 using AODV protocol. Here we will do the analysis for three different methods and to get accurate the result we run the simulation five times for each method and presented result in following tables. Firstly we simply run the simulation for AODV protocol and received the result as per Table-I. After that we imposed blackhole attack and received the result as per Table-II. We clearly identify the degradation in various parameters. After that we run the simulation with hybrid method PAODV_RTPSN and received the result as per Table-III. Table-IV is presenting the average result of each parameter for each method.

Table 1 Result for AODV Protocol

	AODV				
	PDR (%)	**Th (kbps)**	**E2ED (ms)**	**Jitter (ms)**	**NRL (%)**
Observation-1	3.93	552.70	84.17	0.0445	6.1761

Observation-2	3.96	545.84	89.11	0.0450	6.1780
Observation-3	3.87	541.65	88.36	0.0454	6.1722
Observation-4	3.82	550.49	87.04	0.0446	6.1690
Observation-5	3.94	551.77	83.57	0.0445	6.1767

Table 2 Result for AODV Protocol Under Blackhole Attack

	AODV Under Blackhole Attack				
	PDR (%)	**Th (kbps)**	**E2ED (ms)**	**Jitter (ms)**	**NRL (%)**
Observation-1	89.62	59.72	483.01	0.1999	5.1237
Observation-2	88.64	64.56	467.08	0.1849	5.1221
Observation-3	87.67	69.47	427.13	0.1718	5.1269
Observation-4	88.92	63.42	468.44	0.1882	5.1296
Observation-5	88.66	65.14	438.92	0.1832	5.1232

Table 3 Result for PAODV_RTPSN Protocol Under Blackhole Attack

	PAODV_RTPSN				
	PDR (%)	**Th (kbps)**	**E2ED (ms)**	**Jitter (ms)**	**NRL (%)**
Observation-1	15.38	486.8289	90.1522	0.0989	6.7314
Observation-2	14.87	483.8317	95.6222	0.0995	6.7054
Observation-3	15.08	478.4886	95.4638	0.1006	6.7051
Observation-4	14.85	487.3634	93.6890	0.0988	6.7084
Observation-5	15.22	486.9750	90.2340	0.0988	6.7049

Table 4 Average Result for Different Protocol

Sr. No.	**Protocol**	**PDR (%)**	**Th (kbps)**	**E2ED (ms)**	**Jitter (ms)**	**NRL (%)**
1	AODV	3.90	548.49	86.45	0.0448	6.1744
2	AODV Under Blackhole Attack	88.70	64.46	456.92	0.1856	5.1251
3	PAODV_RTPSN	15.08	484.70	93.03	0.0993	6.7110

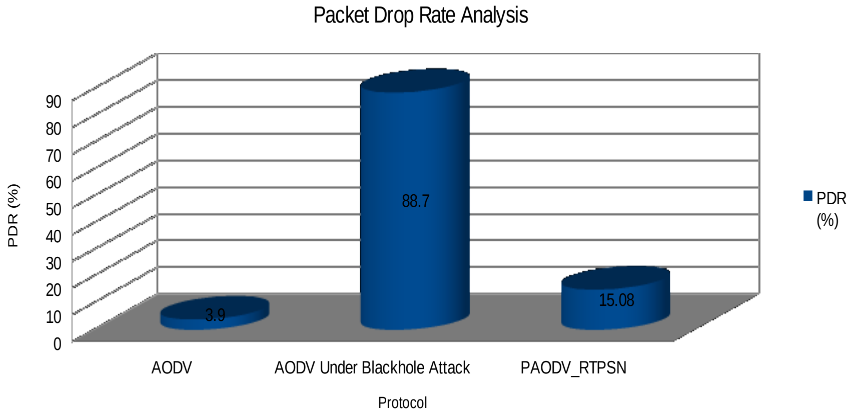

Figure 1 PDR Analysis

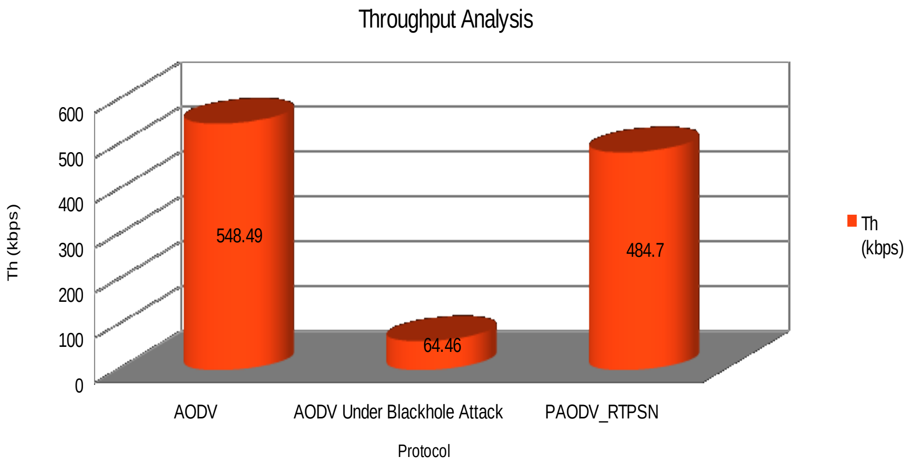

Figure 2 Throughput Analysis

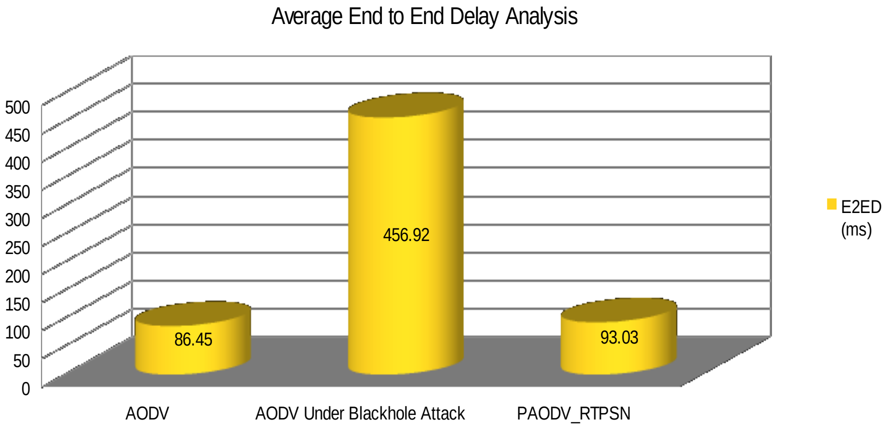

Figure 3 End to End Delay Analysis

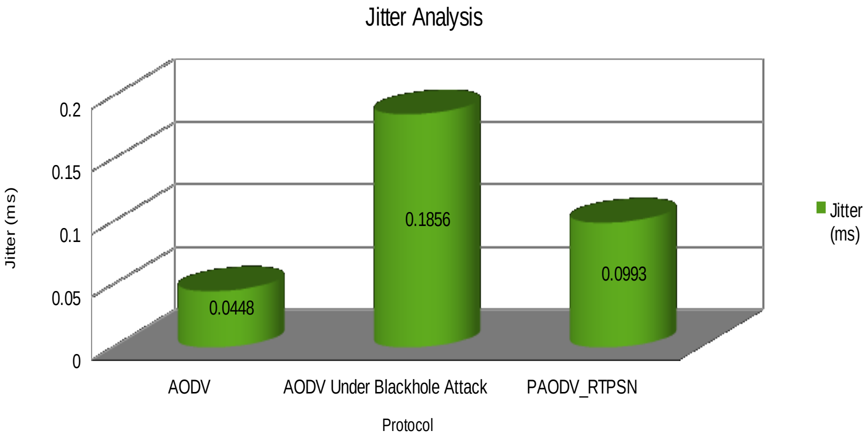

Figure 4 Jitter Analysis

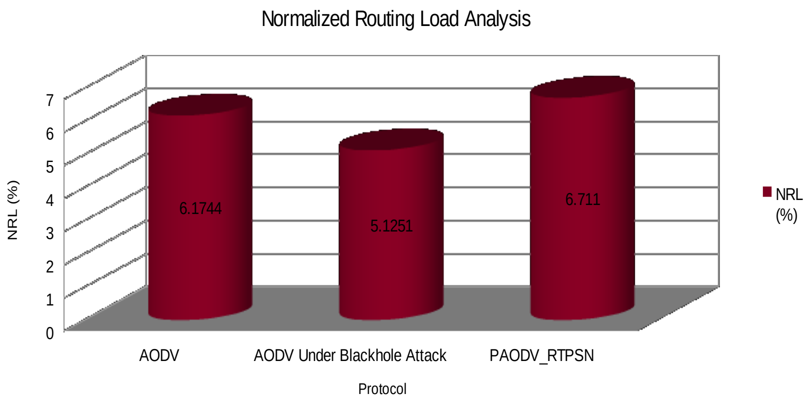

Figure 5 Network Routing Load Analysis

Figure 1 is presenting Packet Drop Rate Analysis, Figure 2 is presenting Throughput Analysis, Figure 3 is presenting Average End to End Delay Analysis, Figure 4 is presenting Jitter Analysis and Figure 5 is presenting Network Routing Load Analysis for AODV Protocol, AODV Protocol under Blackhole Attack and Preventive AODV Protocol with reactive trusted path based on sequence Number. Initially we received Packet Drop Rate 3.90% in AODV and after Blackhole Routing Attack we received very high average Packet Drop Rate 88.70%. After adopting Hybrid approach PAODV_RTPSN, we received good improvement and received packet loss 15.08%.

We received Throughput 548.49 kbps in AODV and after Blackhole Routing Attack we received Throughput 64.46 kbps. After adopting Hybrid approach PAODV_RTPSN, we received good improvement and received Throughput 484.70 kbps. Initially we received Average End to End Delay 86.45 ms in AODV and after Blackhole Routing Attack we received Average End to End Delay 456.92 ms. After adopting Hybrid approach PAODV_RTPSN, we received Average End to End Delay 93.03 ms. We received Average Jitter 0.0448 ms in AODV and after Blackhole Routing Attack we received Average Jitter 0.1856 ms. after adopting Hybrid approach PAODV_RTPSN, we received Average Jitter 0.0993 ms. Initially we received Average Network Routing Load 6.1744 % in AODV and after Blackhole Routing Attack we received Average Network Routing Load 5.1251% and in Hybrid approach PAODV_RTPS we received Average Network Routing Load 6.7110%. Result is presenting all over good improvement in all the parameters in hybrid method.

6. CONCLUSIONS

In this paper we presented the effect of blackhole attack in VANETs and proposed hybrid prevention approach AODV_RTPSN to reduce the effects of such routing attack in VANET. We presented the effects on different parameters in different methods with detail analysis. Only detection of malicious node is not sufficient there is a need to find different methods which prevent network from similar attacks in future. Here we presented hybrid method for blackhole routing attack prevention in which we received good improvement in packet drop rate, throughput, Average end to end delay, jitter and Network Routing Load.

REFERENCES

[1] Irshad Ahmed Sumra, Halabi Hasbullah, Iftikhar Ahmad, Jamalul-lail bin Ab Manan "Forming Vehicular Web of Trust in VANET" in 978-1-4577-0069-9/11/2011 IEEE

[2] Vani A. Hiremani , Manisha Madhukar Jadhao “Eliminating Co-operative Blackhole and Grayhole Attacks Using Modified EDRI Table in MANET”, 978-1-4673-6126-2/13/2013 IEEE

[3] Raghad Baiad, Hadi Otrok, Sami Muhaidat, Jamal Bentahar “Cooperative Cross Layer Detection for Blackhole Attack in VANET-OLSR” , 978-1-4799-0959-9/14/2014 IEEE

[4] Shiang-Feng Tzeng, Shi-Jinn Horng, Tianrui Li, Xian Wang, Po-Hsian Huang, and Muhmmad Khurram Khan “Enhancing Security and Privacy for Identity-based Batch Verification Scheme in VANET”, VT-2014-00658, 10.1109/TVT.2015 .2406877, IEEE Transactions on Vehicular Technology 0018-9545 (c) 2015 IEEE.

[5] Prathima P, Kishore Rajendiran, Shri Ranjani G, Preethi Kurian, Swarupa S “Simple and Flexible Authentication Framework for Vehicular Ad hoc Networks”, IEEE ICCSP 2015 conference, 978-1-4799-8081-9/15/2015 IEEE

[6] Saurabh Gupta, Subrat Kar , S Dharmaraja "BAAP: Blackhole Attack Avoidance Protocol for Wireless Network " in International Conference on Computer & Communication Technology (ICCCT)-2011, 978-1-4577-1386-611, 2011 IEEE

[7] Sisily Sibichen, Sreela Sreedhar, “ An Efficient AODV Protocol and Encryption Mechanism for Security Issues in Adhoc Networks” in International Conference on Microelectronics, Communication and Renewable Energy (ICMiCR-2013) 978-1-4673-5149-2/13/2013 IEEE

[8] P. R. Jasmine Jeni , A. V imala Juliet , R.Parthasarath, A.Messiah Bose, “Performance Analysis of DOA and AODV Routing Protocols with Black Hole Attack in MANET” in 2013 International Conference on Smart Structures & Systems (JCSSS-20 13), March 28 - 29, 2013, Chennai, INDIA, 978-1-4673-6240-5/32/2013 IEEE

[9] Hichem Sedjelmaci and Sidi Mohammed Senouci, “A New Intrusion Detection Framework for Vehicular Networks”, IEEE ICC 2014 - Ad-hoc and Sensor Networking Symposium, 978-1-4799-2003-7/14/2014 IEEE

[10] Wenjia Li, and Houbing Song, “ART: An Attack-Resistant Trust Management Scheme for Securing Vehicular Ad Hoc Networks”, IEEE Transactions on Intelligent Transportation Systems, VOL. 17, NO. 4, APRIL 2016, 1524-9050

[11] Yu-Chih Wei & Yi-Ming Chen “Adaptive Decision Making for Improving Trust Establishment in VANET”, IEICE - Asia-Pacific Network Operation and Management Symposium (APNOMS) 2014

[12] Shalu Malik and Dr. Anil Kumar Sharma, Detection and Isolation Technique for Blackhole Attack in Wireless Sensor Network, International Journal of Computer Engineering & Technology, 9(1), 2018, pp. 66–73.

[13] Dr. Ajay N. Upadhyaya, Dr. J.S. Shah, Effect on AODV Routing Protocol Under Blackhole Attack in VANET, International Journal of Computer Engineering and Technology 10(3), 2019, pp. 166-174.

[14] Kavitha T, Muthaiah R, Mitigation of Blackhole Attack using Neighbor Coverage, International Journal of Mechanical Engineering and Technology, 8(8), 2017, pp. 423–427.

[15] Muthaiah R, Kavitha T, Review on Adaptations to AODV Routing Protocol to Mitigate Blackhole Attacks in Mobile Ad hoc Networks, International Journal of Mechanical Engineering and Technology, 8(8), 2017, pp. 406–410.