ISSN: 0975-766X
CODEN: IJPTFI
Available Online through *Research Article*
www.ijptonline.com

IDENTIFICATION OF MALICIOUS VEHICLES IN VEHICULAR ADHOC NETWORKS USING PRIME PRODUCT CALCULATION

[1]P.Saravanan and [2]T.Arunkumar
[1]School of Computing, SASTRA University, India.
[2]School of Computing Science and Engineering, VIT University, India.
Email: sharan.doit@gmail.com

Received on: 18.10.2016 *Accepted on: 11.11.2016*

Abstract

Vehicular Adhoc Network is the key component of Intelligent Transport System (ITS) and Internet Of Things (IOT). The promising technology of VANET attracts the researchers towards safety applications. VANET is the subset of Mobile Adhoc Network, created using anonymous vehicles for routing and communication. Hence VANET security got much interest while transmitting life critical information. Malicious vehicle can insert or modify this critical information and mislead the driver to a wrong decision. In this proposed work, a mathematical approach has been implemented to detect the malicious vehicle and the malicious route in the VANET using prime product approach. Simulations are carried out with 50 nodes scattered around 5 square kilometers. The Prime Product Number (PPN) method has been implemented to calculate the trust of vehicle using masking scheme. This method outperforms in detection and removal of the particular malicious node and route. Thereby the throughput wastage of using malicious route can be avoided.

Keywords: VANET, Critical information, VANET Attack, Malicious vehicle, Prime product, Masking scheme, Malicious route.

1. Introduction

Vehicular Ad hoc Networks (VANETs) is the self organizing networks of vehicles on the road. Each vehicle on the road can act as router or end nodes. VANET communications can be classified into Vehicle to Vehicle (V2V) Communication and Infra to Vehicle (I2V) Communication. The promising applications [1] of VANET are collision warning, location tracking, emergency brake notification, signal violation notification, parking lot availability, weather information and major information services on the road. Since, the VANET on the road is been created using passing away vehicles

which are anonymous, the VANET data is most vulnerable for various attacks. The attacks are due to lack of centralization and limited resources. These attacks can be either active or passive. In passive attacks, the data to be forwarded is not modified whereas active attacks alter the original data and destination receives modified data. In active attacks one node affects the other nodes in the network whereas in passive a node becomes selfish by acquiring all the resources. Active attacks are further classified as external and internal. External attacks are caused by the nodes that are present outside the network, whereas internal attacks are due to the nodes that are related to network. Internal attacks are difficult to be identified than external attacks.

The presence of various attacks like black hole attack where the attacker modifies data and generates some other data that affects traffic in network, gray hole attack that selectively drops packets causing network distraction, spoofing where one node pretends to be the other node etc., affect this security issue. There are attacks that involve the alteration of data to be transmitted. Threshold cryptography is one of the methods which can transfer the information via multiple routes in a very secure manner. Similarly, many methods are available that detect the attacks and thus provide security. The Novel Security Scheme is such a secret sharing scheme which detects the attacks and avoids high computational complexity.

Various attacks [2] may occur specifically at different layers of network. Jamming attack will mainly occur at MAC layer .Similarly Session hijacking attack at transport layer, Repudiation attack at application layer, Black Hole Attack, Sinkhole Attack, Gray Hole Attack, Information Disclosure Attack, Byzantine Attack, Resource Consumption Attack, Wormhole Attack, Neighbor Attack, Routing Attack, Stealth Attack, Man- in- the- Middle Attack at network layer.

The main objective of the proposed work is to find the malicious vehicle in the VANET, identify the malicious route from source to destination to avoid emergency message transmission using the same. Prime Product Number (PPN). The rest of the manuscript has organized as follows. Section 2 reviews the related works that have been used for the malicious node detection and security solutions. Section 3 details the proposed architecture and its implementation. Section 4 reveals the experimental setup and the results achieved. Conclusion and future work have been given section 5.

2. Related Work

Many different schemes have been proposed to detect the malicious routes or nodes and to provide security in wireless ad hoc networks. Some schemes [3] follow approach with scanning procedure and security measures for the abnormal behavior of the malicious nodes and verify the presence of attacks. Another method used in cooperative wireless network

[4] is based on local decisions taken at each node, which are then merged at a fusion centre having the authority to block node's activity. Intrusion is an external attack. Collision, packet drop, misdirection are the different types of intrusion attacks. In the paper [3], a cross-layer design approach is followed. A detailed analysis of the collision detection algorithm, the detection procedure for packet drop and the misdirection attack is discussed. ADCLI algorithm proposed in [5], involves a technique in which the malicious nodes are detected. It uses message passing between each pair of nodes present in a particular radio range. From the messages received during the detection phase which is initiated by monitor node, each node sends votes to monitor node about the nodes it suspects. The monitor node finally determines the malicious nodes by inspecting the suspected nodes. These methods may not be efficient in case of a large network with many nodes. Using Naïve-Bayesian classification [6] another approach has been proposed for fraud detection in telecommunication sector. K-L divergence method has been adopted to find the fraudulent customer.

In networks, various attacks like black hole, worm hole etc. makes the transfer of information through one path insecure. Threshold cryptography is one of the methods to transfer data through multiple paths in a secure manner. In this method, the message is encrypted into n parts. The decryption process involves the usage of only threshold (t) number of parts to generate the original information. Even if some parts (< (n-t)) are modified, original information can be generated. In the paper [7], an extended threshold cryptography scheme is proposed for MANETs to sustain the service availability in localized schemes when the number of local shareholders available is below the threshold. Generally, this cryptography demands significant computational and communicational resources at the nodes. But in [8], proposes a fully-distributed threshold cryptography based scheme which reduces the computational complexity.

The Novel Security Scheme [9] uses the concept of Threshold Cryptography. In this, any information is divided into multiple shares and they are transmitted via multiple disjoint paths between communicating nodes. The receiving end reconstructs the original information by combining the received shares. The earlier schemes lead to high computational complexity during both sharing and reconstructing. But this reduces the complexity, as it employs elementary graphical masking method, done by simple ANDing for share generation and reconstruction is done by simple ORing the received shares.

Prime Product Number (PPN) scheme [10] is mathematical approach for the detecting malicious node in wireless communication networks. The promising features of prime number have been used for identifying the unwanted nodes.

3. Proposed Scheme for Detection of Malicious Node

3.1 System Architecture

In this methodology, each new vehicle entering to the network is assigned with a distinct prime number. This prime number can also be acting as address or identification number of the node. The vehicle on the road can be clustered and the road side unit is considered as cluster head which will care about prime products. PPN is the product of all prime numbers from source to destination. At destination node received PPN will be checked whether it is divisible by all the prime numbers that are assigned to nodes in that route.

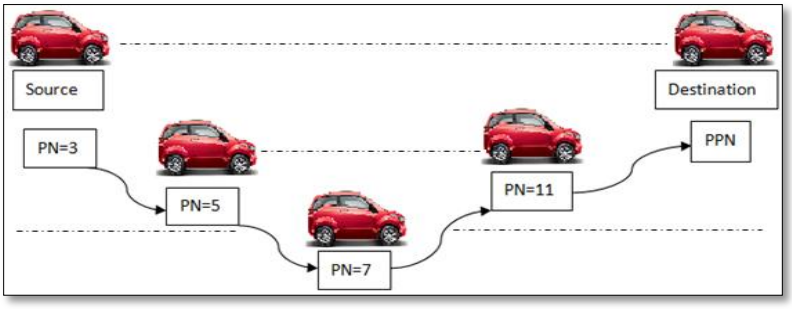

Fig. 1 VANET Packet transmission with Prime Products.

Each prime number will be divisible by itself and 1 only. But a composite number will be divisible by other numbers also. Here PPN will be checked for divisibility with each prime number that is pre-assigned to the nodes. If PPN is not divisible by any of the assigned prime numbers, then the respective node will be identified as malicious. Fig. 1 shows the sample scenario of VANET communications with the prime number as identity for each vehicle.

Each vehicle has a prime number as identity the actual data has been using this prime number. The list of the prime numbers assigned to each vehicle has been maintained by cluster head. When any packet transmission has been taken from source to destination, the prime numbers on the route have been multiplied the final product result has been calculated by destination which referred as Prime Product number (PPN). The calculated PPN has been compared for any changes by any of the malicious node. The checking process will be the division process. The PPN has been divided by the list prime number as crossed in reverse order. If the PPN is divided by all the prime numbers then it is assumed that there is no malicious vehicle on the path form source to destination. Otherwise the first vehicle from the destination whose prime number is not a divisor has been declared as malicious vehicle. That malicious route has been avoided for further packet transmission from the same source and destination. The proposed method for malicious vehicle detection in VANET environment has been depicted in Fig 2.

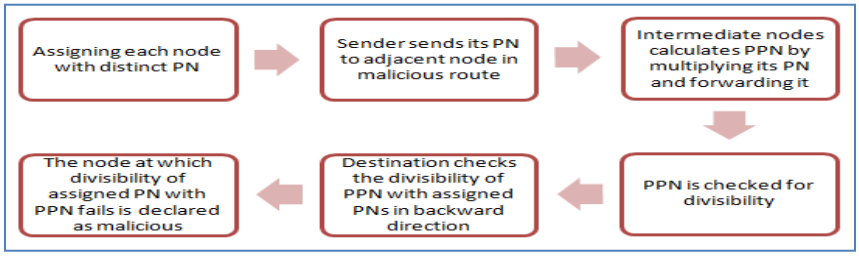

Fig. 2 Proposed Architecture for Malicious Vehicle detection.

3.2 Algorithm for Malicious Vehicle detection in VANET

Step 1: Assign new prime number for the vehicle entering to the cluster by cluster head.

Step 2: Send source prime number to its next node in the route towards destination.

Step 3: At intermediate node, calculate PPN by multiplying its PN and forward it.

Step 4: Repeat Step 3 until reaching destination.

Step 5: At destination, calculate the final PPN.

Step 6: Check final PPN using divisibility of PPN with assigned PNs in backward direction.

Step 7: The node at which divisibility of assigned PN with PPN fails is declared as malicious

3.3 Methodology illustration: In fig 1, the path between source and destination vehicles with three intermediate routing vehicles is depicted. The unique prime numbers have been assigned to source and intermediate nodes as given in the table 1.

Table 1: Unique identification of Vehicles using Prime Numbers.

Node	Source Vehicle	Routing Vehicle 1	Routing Vehicle 2	Routing Vehicle 3	Destination Vehicle
Prime Numbers Assigned	3	5	7	11	13
PPN Calculated	3	15	105	1155	15015

Table 2 shows the method of malicious vehicle detection on the path between source vehicle and destination vehicle. The final PPN is received by the destination vehicle and the received PPN has been checked with list prime numbers for division. The list of prime numbers has been referred from the cluster head by sending the addresses of various nodes crossed while transmission.

Table 2: Malicious Vehicle node detection using PPN.

Node	Destination Vehicle	Routing Vehicle 3	Routing Vehicle 2	Routing Vehicle 1	Source Vehicle

Prime Numbers Assigned	13	11	7	5	3
PPN Calculated	15015	1155	105	15	3
If No malicious vehicle on the path	13 is a divisor of PPN	11 is a divisor of PPN	7 is a divisor of PPN	5 is a divisor of PPN	3 is a divisor of PPN
If Routing Vehicle is malicious node		11 is not a divisor of PPN	7 is not a divisor of PPN	5 is not a divisor of PPN	

The PPN is divided by the prime numbers from destination to source direction. If the final prime number is equal to prime number of source then, it is declared as no malicious vehicle has been found on the path. Otherwise, the routing vehicle whose prime number is not a divisor of PPN has been declared as malicious node. The path via this particular vehicle has been declared as malicious route no further transmission will be carried out using this malicious path.

Case 1: If no node is malicious

PPN= 3 * 5 * 7 * 11 = 1155

Here PPN, 1155 is divisible by all assigned PN's.

Case 2: If there is a malicious node in a route

Assume node 2 is malicious. Source node sends PN as 3 to node1. Node1 multiplies its own PN 5 to received number 3 and sends 3 * 5 to node 2. As node 2 is malicious, instead of performing correct work it sends modified number, say 32 to node 3. Node 3 multiplies its own PN 11 to the received number 32 and sends the PPN 32*11=352 to destination node.

Destination node checks for divisibility of PPN with prime numbers assigned to each node starting from its previous node. The first node at which divisibility fails will be detected as malicious. First PPN, 352 is checked for divisibility by 11, as it is divisible node 3 is declared as non malicious node. Next, 352 is checked for divisibility by 7. As divisibility fails, node 2 is declared as malicious.

4. Experimental Results and Discussion:

NS2 simulations are carried out with 50 nodes scattered around 5 square kilometers. The Prime Product Number (PPN) method has been implemented to calculate the trust of vehicle using masking scheme. Various paths have been considered have been used for packet transmission using Geographic Routing Protocol (GRP). In the selected path

random vehicle has been selected for malicious activities. One base station has been used as Road Side Unit (RSU) and also as cluster head to assign prime number to each new vehicle. For vehicle mobility random waypoint model has been used with the mobility of 10 meters/second. Number-of-retransmission attempts and throughput have been used to check the performance of proposed methodology.

Table 3: Simulation Parameters.

Parameters	Values
Number of Nodes	50
Routing Protocols used	GRP
Simulation area	5 sqkm
Base Station used	Single
Performance factors	Throughput, transmission attempts, control overheads
Mobility	10 m/s
Mobility Model	Random Way point

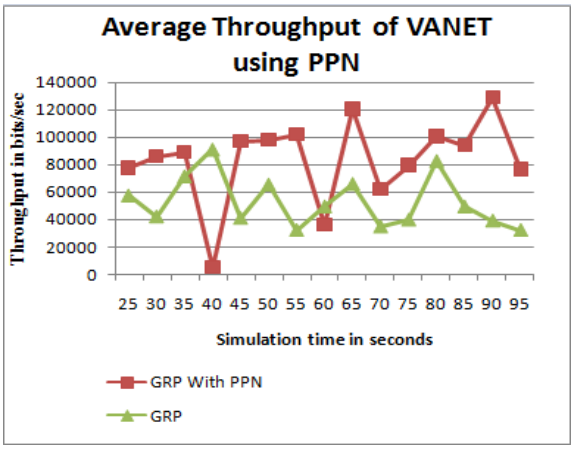

Fig3: Throughput VANET.

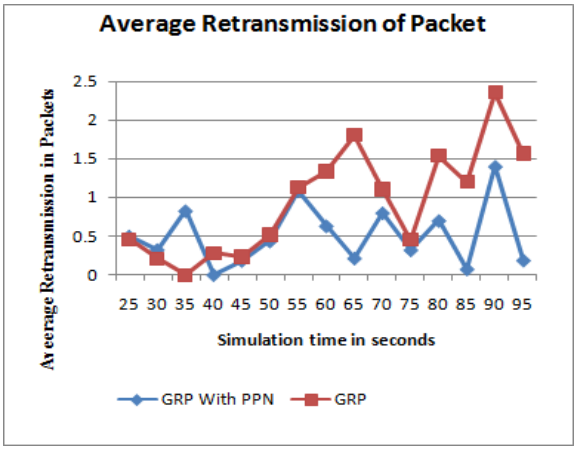

Fig 4: Average retransmission of Packets.

The simulation results are shown in Fig 3 and Fig 4. Figure 3 shows the throughput performance of VANET with GRP routing with and without PPN method. Figure 4 show the number of retransmission attempts made by the source,

because of malicious attacks. The traditional GRP protocol attempts many retransmissions because of attacks by malicious node and malicious route. In the case of GRP with PPN the malicious node has been detected using prime product number and the particular route has been avoided. Hence the number of packet drops has been reduced enormously and hence the least number of retransmission. The proposed architecture for malicious node and route detection outperformed in-terms of throughput and number of retransmission attempts for vehicular ad hoc environment.

5. Conclusion

VANET may offer various applications in safety level, comfort level and communication level. Since the VANET may use malicious anonymous vehicles for routing the data from one end to other end of geographically scattered area. The proposed work, identification of malicious node in vehicular adhoc has been aimed to provide security to the data transmitted. A mathematical approach has been implemented to detect the malicious vehicle and the malicious route in the VANET using prime product approach. Simulations are carried out with 50 nodes scattered around 5 square kilometers. The Prime Product Number (PPN) method has been implemented to calculate the trust of vehicle using masking scheme. This method outperformed in detection and removal of the particular malicious node and route. Thereby the throughput wastage of using malicious route can be avoided.

References

1. Saravanan, P., & Arunkumar, T. (2014). Fuzzy Enabled Geographic Routing Protocol for Vehicular Ad hoc Networks. *International Review on Computers and Software (IRECOS)*, *9*(6), 1101-1107.
2. Isaac, J. T., Zeadally, S., & Camara, J. S. (2010). Security attacks and solutions for vehicular ad hoc networks. *IET communications*, *4*(7), 894-903.
3. Thamilarasu, G., Balasubramanian, A., Mishra, S., & Sridhar, R. (2005, November). A cross-layer based intrusion detection approach for wireless ad hoc networks. In *IEEE International Conference on Mobile Adhoc and Sensor Systems Conference, 2005.* (pp. 7-pp). IEEE.
4. Manikandan, T., & Sathyasheela, K. B. (2010, October). Detection of malicious nodes in MANETs. In *Communication Control and Computing Technologies (ICCCCT), 2010 IEEE International Conference on* (pp. 788-793). IEEE.

5. Saravanan, P., Subramaniyaswamy, V., Sivaramakrishnan, N., Prakash, M. A., & Arunkumar, T. (2014). Data Mining Approach For Subscription-Fraud Detection in Telecommunication Sector. *Contemporary Engineering Sciences, 7(15), 515-522.*
6. Tarmizi, S., Veeraraghavan, P., & Ghosh, S. (2009, December). Extending the collaboration boundary in localized threshold cryptography-based schemes for MANETs. In *Communications (MICC), 2009 IEEE 9th Malaysia International Conference on* (pp. 290-294). IEEE.
7. Tomasin, S. (2011). Consensus-based detection of malicious nodes in cooperative wireless networks. *IEEE communications letters*, *15*(4), 404-406.
8. Dey, H., & Datta, R. (2012, December). Monitoring threshold cryptography based wireless sensor networks with projective plane. In *Computers and Devices for Communication (CODEC), 2012 5th International Conference on*(pp. 1-4). IEEE.
9. Das, A., Basu, S. S., & Chaudhuri, A. (2011, February). A novel security scheme for wireless adhoc network. In *Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE), 2011 2nd International Conference on* (pp. 1-4). IEEE.
10. Gambhir, S., & Sharma, S. (2013, February). PPN: Prime product number based malicious node detection scheme for MANETs. In *Advance Computing Conference (IACC), 2013 IEEE 3rd International* (pp. 335-340). IEEE.