GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES

# A REVIEW ON NOVEL SCHEME FOR ISOLATION OF SYBIL ATTACK IN VANET

**Akanksha Kumari[1], Yogesh Arora[2] & Ritu Chahal[3]**
[1]M.Tech Scholar, Department Of Computer Science Engineering, SET,Soldha
[2]Assistant Professor Department Of Computer Science Engineering, SET,Soldha
[3]Assistant Professor Department Of Computer Science Engineering, SET,Soldha

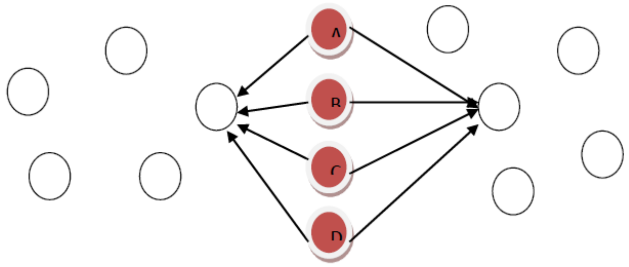
## ABSTRACT

Vehicular adhoc networks (VANETs) are classified as an application of mobile adhoc network (MANET) the primary advantages of VANETs are the doable in giving explorers alleviation and they enhance road protection and vehicle security while protecting drivers' privacy from attacks perpetrated by means of foes. As of late VANETs have emerged to turn the consideration of researchers in the area of wifi and cell communications. Due to self-configuring nature of the network, malicious nodes be part of the network which is responsible to trigger various kind of active and passive attacks. The Sybil attack is the active kind of assault in which malicious node spoof the identification of the legitimate node. The authentic node is not in a position to get the required statistics which leads to reduction in community throughput. In this work, technique is been proposed which will become aware of and isolate malicious nodes from the community which are accountable to trigger Sybil attack in the network. The proposed strategies is based totally based signal strength based technique and monitor mode techniques.

## I. INTRODUCTION

Vehicular adhoc community are wireless networks where each and every one of the automobiles from the nodes of the network. It is for the driver remedy and avenue safety, the inter- vehicle verbal exchange give them. Vehicular especially appointed network is subclass of mobile impromptu networks which offers a distinguished strategy to canny transport system. . It is self It is self sustaining and self-organizing wireless verbal exchange network, the place each one of the nodes in VANET includes themselves as servers or purchaser for replacing and sharing information. The community structure of VANET can be classified into three classes pure cellular, pure particularly appointed and hybrid.

Sybil Attack in VANET It involves of sending a couple of messages from one hub with a couple of identities. Sybil attack is continuously possible apart from the excessive conditions and assumptions of the possibility of resource parity and coordination amongst entities. At the point when any hub makes more than one copies of itself then it makes confusion in the network. Claim all the unlawful and pretend ID's and Authority. It can make collision in the network. This sort of state of affairs is acknowledged as Sybil attack in the network. This device can attack each internally and externally in which exterior attacks can be confined by way of authentication yet not inside attacks. There is balanced mapping amongst identity and substance in the network.



**Sybil Attack**

***A,B,C,D nodes are Sybil nodes which create fake or similar similar identity in network and collapse the network.***

ISSN 2348 – 8034
Impact Factor- 5.070

## II. LITERATURE REVIEW

Manuel Fogue et al. "On the use of a cooperative neighbour position verification scheme to secure warning message dissemination in VANETs" 2013, the author proposed a protocol named cooperative neighbour position and verification (CNPV) protocol which is based on proactive approach [1]. The scheme maximizes their performance when all the vehicles give correct information and when it gives position errors the performance gets reduced. The scheme detects the node that gives false location information. The result shows that UV-cast is a good mechanism to reach new areas of the roadmap while eMDR algorithm is more resistant.

**Claudia Campolo et al.** "Modeling broadcasting in IEEE 802.11p/WAVE vehicular Networks"2011, the author proposed a new analytical model which is intended for assessing the telecom execution on CCH in IEEE 802.11p/WAVE vehicular systems [2]. This model expressly represents the WAVE channel exchanging and processes bundle conveyance likelihood as an element of conflict window size and number of vehicles. The author validated the model by developing an event-driven custom simulation program in Matlab that follows the 802.11p EDCA protocol specifications. Results are carried out for certain set of parameter values and show the probability of successful broadcast delivery.

**Mervat Abu-Elkheir et al.** "Position Verification for Vehicular Networks via Analyzing Two-hop Neighbors Information"2011This paper proposes a position verification scheme that involves the collaborative exchange of one-hop neighbor information of vehicle position announcements to help make the decision [3]. Self-trust, honest majority, temporal behavior consistency is such conditions which should be there in vehicular environment. Results are carried out via simulation and future work would involve implementing a realistic VANET propagation model.
**Tim Leinmuller et al.** "Improved Security in Geographic Ad hoc routing through Autonomous Position Verification"2006, the author proposed a detection mechanism scheme that uses various different sensors to rapidly give an estimation of the dependability of other nodes position claims without utilizing specific equipment [4]. As a result, attackers have fewer possibilities for using fake positions. Results are carried out via simulation that shows how messages are delivered by Acceptance Range Threshold (ART) and Mobility Grade Threshold (MGT). It evaluates the detection capabilities of our decentralized position verification system.

**Soyoung Park et al**. "Defense against Sybil attack in Vehicular adhoc network based on road side unit support"2009, proposed a timestamp series approach to defend against Sybil attack in a vehicular adhoc network based on roadside unit support [5]. This approach is probably suitable for initial deployment of VANET where vehicles have network communication and have a basic infrastructure i.e. RSU. It uses digital certificates and do not use public key infrastructure though it is secured. Moreover, this timestamp series approach does not need internet accessibility. They analyzed their approach under various traffic situations i.e. traffic congestion, complex roadways.

**Tong Zhou et al**. "P2DAP – Sybil Attacks Detection in Vehicular Ad Hoc Networks"2011,the author proposed a lightweight and adaptable protocol whose main purpose is to identify Sybil assaults and deny malicious vehicles promptly after detection [6]. From the outcomes, it is shown that scheme having the capacity to identify Sybil assaults at low overhead and delay, while saving privacy of vehicles.

**Khaled Mohamed Rabieh et al.** "Combating Sybil Attacks in Vehicular Ad Hoc Networks" 2011, the author proposed a detection scheme whose idea is based on public key cryptography and aims to ensure security protection, confidentiality and non-repudiation [7]. However, he made utilization of the Online Certificate Status Protocol (OCSP), by incorporating it to his proposed plan, to ensure that the used certificates are fresh enough and avoid using already revoked ones.

**Shan Chang et al**. "Footprint: Detecting Sybil Attacks in Urban Vehicular Networks" 2012, the author proposed a novel Sybil assault discovery component, Footprint, utilizing the directions of vehicles for distinguishing while still preserving their location privacy [8]. When a vehicle methodologies a road side unit (RSU), it effectively requests an approved message from the RSU as the confirmation of the appearance time at this RSU. It is demonstrated by both analysis and extensive trace-driven simulations that Footprint can largely restrict Sybil attacks and can enormously reduce the impact of Sybil attacks in urban settings.

**Gang Liu et al** ," Some aspects of road sweeping vehicle automation ", they proposed some aspects of road sweeping vehicle automation a design of framework of intelligent transports system is proposed. The main task of the road condition information transferring module is deal with the information exchange of the car inside, car to car and car to road. They concern the security issues of VANETs from some aspects and provide the appropriate solving measures. To make sure the Its can be used under the security pattern [9].

**Kung,"** A survey of mobility models for ad hoc network research", *wireless communication & mobile computing (WCMC): special issue on mobile ad hoc networking: research, trends and applications*", proposed a survey of mobility models for ad hoc network research [3] they proposed security architecture for vehicular communication. The primary objectives of the architecture include the management of identities and cryptographic keys, the security of communications, and integration of privacy enhancing technologies. Their design approach aims at a system that relies on well-understood components which can be upgraded to provide enhanced security and privacy protection in the future [10].

**Hao Wu,"** An Empirical Study of Short Range Communications for Vehicles", they presented An Empirical Study of Short Range Communications for Vehicles a work on short range of communication over the vehicles. The work includes both V2V and V2I communication under highway scenario. The network characteristics in driving environment is been discussed in this work [11].

**Su-Jin Kwag**." Performance Evaluation of IEEE 802.11 Ad-hoc Network in Vehicle to Vehicle Communication" has propsed Performance Evaluation of IEEE 802.11 Ad-hoc Network in Vehicle to Vehicle Communication performed a work to analyzes the performance of the IEEE 802.11 Ad-hoc network for v2v communication under a vehicular environment, focusing on the fairness which very crucial to the safety related services, and the effect of mobility. Some suggestions for future researches are followed [12].

**JasonJ. Haan el al,"** Real-World VANET Security Protocol Performance" they represent a paper based on the performance measurements obtained from simulations of the (VANETs) vehicular ad-hoc networks. These simulations use as input traces of vehicle movements that have been generated

input traces of vehicle movements that have been generated by traffic simulators which is based on the traffic model theory. In this paper mainly work based on the actual large scale recordings of vehicle movements. In order to enable analysis on this scale, we have developed a new VANET simulator which handle more vehicle than ns2. To enable us simulator and present results of cross validation between ns2 and our simulator showing the both simulation produce result that are statistically the same. This simulator use to analyse the proposed authentication mechanism, which relies on ECDSA signatures comparing it to broadcast authentication using TESLA. In this paper perform our evaluations using real vehicle mobility. Our comparison shows its strength and weakness for each of these authentication schemes in terms of the resulting reception rates and latecyof broadcast packets [13].

**Josiane Nzouonta el al** ," VANET Routing on City Roads using Real-Time Vehicular Traffic Information" represented a paper based on routing protocols called RBVT, road based using vehicular traffic information routing which is based on the existing routing protocol in city based vehicular ad-hoc networks (VANETs). RBVT protocols leverage real time traffic information to create road based paths consisting of successions of road intersection and high probability, network connectivity among all the systems. In this paper use the geographical forwarding is used to sent the packets between intersection path, reducing the sensitivity within the paths to individual node movements. In the dense network high contention and optimize the forwarding using a distributed receiver based election of next hops, it is based on the multi-criteria prioritization function taking into account non-uniform radio propagation. This paper designs the reactive protocol RBVT-R and proactive protocol RBVT-P and compared them against MANETs protocols like AODV, OLSR, GPRS. Other protocol representative is like VANET. In the simulation result shows that in the urban settings shows that RBVT-R protocol best in term of delivery rate, with up to 40% increase compared to some existing protocols. In the protocol terms of average delay, RBVT-P performs best and 85% decreased as compared to other protocols [14].

## III. TECHNIQUES FOR ISOLATION OF SYBIL ATTACK

The proposed techniques is based on

- Signal strength based technique and
- Monitor mode techniques.

In the proposed technique, the road side units flood the ICMP messages in the network. The vehicle nodes when receive the ICMP messages will start sending its signal strength value to its nearest road side units. The road side units will gather all the information and exchange the information with each other. The vehicle node which has multiple signal strength values will be detected as the node which may cause the intrusion in the networks. To confirm that which node is the malicious node, the road side units send the control packets in the network and vehicle nodes when receive the control packets will go to monitor mode and start watching its adjacent nodes. The node which is malicious is detected a technique is multiple path routing is applied which isolate malicious nodes from the network. Signal strength and Monitor mode algorithm [15].

```
Input: vehicles, RSU, malicious vehicle
Output: Malicious vehicle
Apply information gathering process
{
Node send its credentials to road side units
If(Matched= true)
Assign identification
Else
Send not verified message
}
}
If (signal strength ==not matched )
Send ICMP messages in the network
Node receive the message go to monitor node
If(Node change id==true)
Node ==Malicious node
Else
Node=Legitimate node
}
End
```

## REFERENCES

1. *Manuel Fogue et al. “On the use of a cooperative neighbour position verification scheme to secure warning message dissemination in VANETs” 2013,*
2. *Claudia Campolo et al. “Modeling broadcasting in IEEE 802.11p/WAVE vehicular Networks”2011,*
3. *Mervat Abu-Elkheir, Sherin Abdel Hamid, Hossam S. Hassanein, Ibrahim M. Elhenawy, Samir Elmougy,“ Position Verification for Vehicular Networks via Analyzing Two-hop Neighbors Information”, 2011, IEEE, 978-1-61284-928-7*
4. *Tim Leinmuller, Christian Maihofer, Elmar Schoch and Frank Kargl,“Improved Security in Geographic Ad hoc routing through Autonomous Position Verification”2006, Elsevier, 2973023-3-4-454*
5. *eSoyoung Park, Baber Aslam, Damla Turgut, Cliff C. Zou,“ Defens against Sybil attack in Vehicular adhoc network based on road side unit support”2009, Research Pvt. Communications, 900042*
6. *Tong Zhou, Romit Roy Choudhury, Peng Ning, and Krishnendu Chakrabarty,“ P2DAP – Sybil Attacks Detection in Vehicular Ad Hoc Networks”2011, IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 29, NO. 3*

7. Khaled Mohamed Rabieh, Marianne Amir Azer,“ Combating Sybil Attacks in Vehicular Ad Hoc Networks” 2011, CCIS 162, pp. 65–72
8. Shan Chang, Shan Chang, Yong Qi, Hongzi Zhu, Jizhong Zhao, and Xuemin (Sherman) Shen,” Footprint: Detecting Sybil Attacks in Urban Vehicular Networks”, 2012, IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 23, NO. 6
9. Gang Liu and Han Guo, “ Some aspects of road sweeping vehicle automation”, IEEE lasme international conference on advanced intelligent mechatronics,2001
10. Kung et.al “A survey of mobility models for ad hoc network research”, wireless communication & mobile computing (WCMC): special issue on mobile ad hoc networking: research, trends and applications, vol. 2, no. 5, pp. 483-502, 2002.
11. Hao Wu "An Empirical Study of Short Range Communications for Vehicles", IJSER September 2, 2011, Cologne, Germany, pp 83-84
12. Su-Jin Kwag “Performance Evaluation of IEEE 802.11 Ad-hoc Network in Vehicle to Vehicle Communication ", Mobility 06, 1-59593-519-3
13. Michel Hugo "Self-Organized Traffic Control", VANET’10, September 24, o, Illinois, Reena Dadhich Department of MCA, Govt. College of Engineering, Ajmer, India,” Mobility Simulation of Reactive Routing Protocols for Vehicular Ad-hoc Networks”(2011)
14. Jason J. Haas and Yih-Chun Hu University of Illinois at Urbana-Champaign Urbana, Illinois, U.S.A,” Real-World VANET Security Protocol Performance” (2007) p1-7.[15] Josiane Nzouonta, Neeraj Rajgure, Guiling Wang, Member, IEEE, and Cr
15. Sybil Attack in VANETs Detection and Prevention Jyoti Grover, M.S. Gaur, and V. Laxmi