Localization of Sybil Nodes and Detection of Malicious Node in VANETs

K.Murugan[1], R.Nandhakumar[3], Dr.P.Varalakshmi[2],
[1,3]Teaching Fellow, Department of computer Technology,
[2]Assistant professor, Department of Information Technology,
Anna University
[1]Krishna.muruga@gmail.com [2]varanip@gmail.com [3]nandhakumarr03@gmail.com

Abstract ---- The Sybil attack is a significant attack in Vehicular Ad Hoc Networks, because it causes security threats in VANETs and, even leads to a threat to lives of drivers and passengers. In this paper, we address the attack in two phases. Sybil attack is where one malicious node pretends to be several non-existent nodes by stealing or borrowing identities of physical nodes. The objective is to first identify the Sybil nodes and then identify the malicious node generating the Sybil nodes. In order to do this, we make use of a suspicion factor. The node with the highest suspicion number is identified as the malicious node. Our proposal shows a better performance than the existing methods by making use of the range and suspicion factor which makes it easier for identifying and recognizing all the Sybil nodes even when the number of vehicles keeps increasing.

***Keywords*—VANET, MANET, C2CC, IVC, RSU**

I. INTRODUCTION

Recent year's rapid development in wireless Communication networks has made Inter-Vehicular Communications (IVC) and Road-Vehicle Communications (RVC) possible in Mobile Ad Hoc Networks (MANETs), this has given birth to a new type of MANET known as the Vehicular Ad Hoc Network (VANET), aiming to enable road safety, efficient driving, and infotainment.

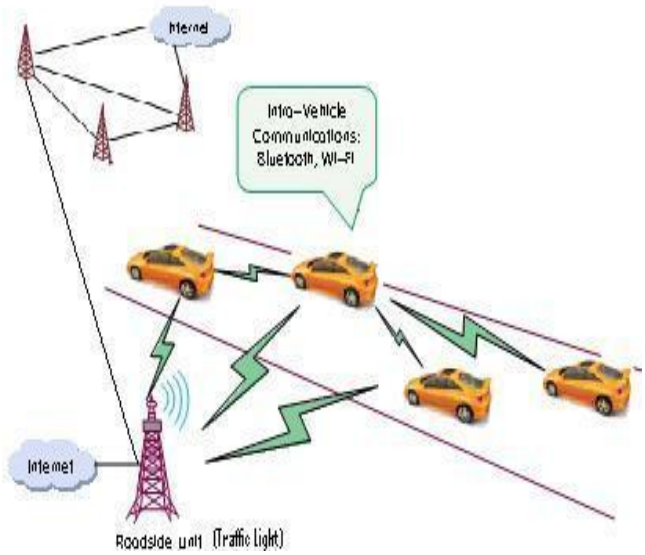

Fig. 1 Car to Car Communication.

Sybil attack happens when an attacker creates large number of pseudonymous, and claims or acts like it is more than a hundred vehicles, to tell other vehicles that there is jam ahead, and force them to take alternate route. This is depicted in Figure 2. Sybil attack depends on how cheaply identities can be generated, the degree to which the system accepts inputs from entities that do not have a chain of trust linking them to a trusted entity, and whether the system treats all entities identically. For instance an attacker can pretend and act like a hundred vehicle to convince the other vehicles in the road that there is congestion, go to another rout, so the road will be clear.

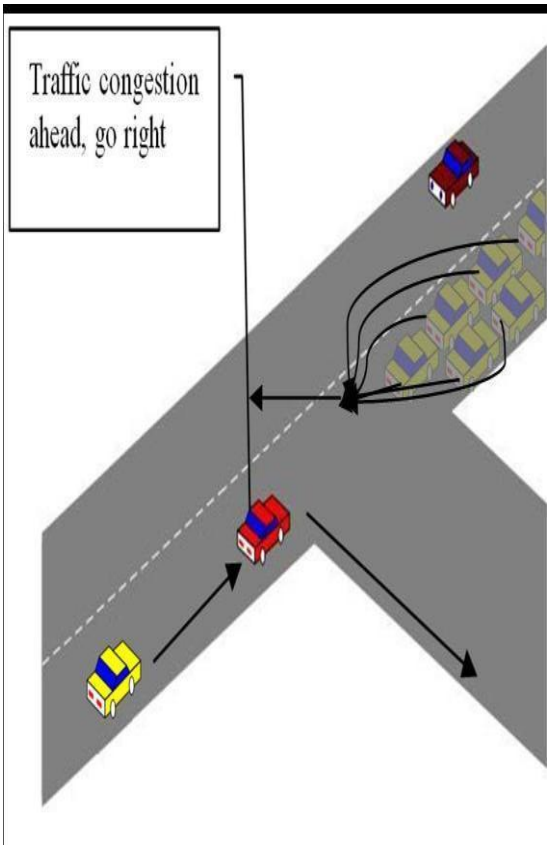

Fig. 2 Sybil attack scenario

The following are the challenges in VANET when there is a Sybil attack: In the application of deceleration warning systems [3], if a vehicle reduces its speed notably, it will broadcast a warning message to the surrounding vehicles. The receiver vehicles will relay this message to vehicles further behind. However, this sending process can be interceded by a large number of malicious Sybil nodes. In this way, the malicious adversary vehicle can create a huge collision and traffic on the highway, possibly causing great loss of life and wealth. The Sybil attack should thus be addressed in order to provide a safe journey for the vehicles on a highway. The rest of this paper is organized as follows: we discuss previous research work in Sybil detection in Section 2; Section 3 describes our proposed Sybil attack detection approach in detail; Section 4 presents the simulation and evaluation results of our proposed approach. Finally, we present our conclusions and ideas for future work in Section 5.

II. RELATED WORK

Considerable devotion from the research community has been given by emerging vehicular networks. There have been several proposals pointing out the importance of security in vehicular networks which are discussed below. Sybil attack, in which a malicious node creates an illusion of traffic congestion by claiming multiple identities, is a serious threat and needs attention in VANETs.

A. Sybil Attack: The Sybil attack was first described and formalized by Douceur in [4]. It this attack, an entity sends multiple messages from one node with multiple identities which may be stolen or borrowed. Applications of the Sybil attack in Vehicular Ad-Hoc Networks have been discussed in [1], and show the importance of Sybil nodes detection in VANET. One important result shown in [4] which is without a logically centralized authority, Sybil attacks are always possible (*i.e.* may remain undetected) except under extreme and unrealistic assumption of resource equality and coordination among entities.

B. Resources testing: [4] and [8] propose resources testing as a defense against Sybil attack. This resource testing is based on the assumption that each physical entity is limited in some resource. The method described in [4] uses computational puzzles [7] to test nodes computational resources. In [8], the authors show that this approach is not suitable to ad-hoc networks, and hence typically VANET, because the attacker can have more computational resources than an *honest* node. Hence, they propose a radio resource testing.

C. Use of public key cryptography: In [11], the authors try to solve the security problem of the Sybil attack with public key cryptography. The authors propose the use of a PKI for VANET and termed it VPKI. They describe a feasible solution to provide security of communications and they address the problem of key distribution in VANET. In addition, they propose a mechanism for key revocation. Each vehicle may be authenticated with its public key, and hence the Sybil attack is always detected. Nevertheless, deploying PKI for VANET is heavy and a difficult solution that must be tested to analyze its possible use in a real world.

D. Assuming a given propagation model: Some of the papers dealing with detection of Sybil attack in wireless networks assume a predefined propagation model [9]. They use the received signal power to deduce some discrepancies between the received power of the signal and the claimed position. In a node collects signal strength measurement from other nodes and estimates their new position according to a given propagation model. A node is considered suspect if its claimed position varies by a large margin from the evaluated one.

E. Secure positioning: Another possibility to defeat Sybil attack is to provide a secure positioning system and the reliability of the position claimed by vehicles. In [2], the authors propose methods for determining a transmitting peer's node location using signal properties and trusted peers collaboration for identification and authentication purposes. The method uses characteristics such as signal strength and direction. In [3], the authors present a novel approach called *verifiable multil ateration*, using distance bounding protocol [2] and base stations to provide secure positioning. They also assume that all network nodes can establish pair wise secret keys.

F. Distinguish ability: In [5], the authors propose an approach to analyze the validity of VANET data. Data are correlated and scored; data with the higher score will be accepted. The proposed model notably relies on the fact that nodes are associated with specific devices allowing tying a message with physical sources.

III. PROPOSED WORK

A. Assumptions:

We consider the initial deployment stage of VANET where:

1. There is sufficiently large number of road side units

2. All vehicles are equipped with equal number of resources which are same. The basic assumptions on vehicles and RSUs are as follows:

• Vehicle: It has an on-board unit (OBU) for networking and computing messages, GPS for location detection, and digital map including geographical road information.

• Roadside Unit (RSU): It has a transmitter for sending and receiving messages from the vehicles regarding their locations. In addition, it has a tamper-proof device for storing secure information.

Sybil attacks can incur great security threats to VANETs. First, Sybil nodes may cause an illusion of

traffic congestion. A greedy driver may convince the neighboring vehicles that there is considerable congestion ahead, so that they will choose alternate routes and allow the greedy driver a clear path to his/her destination [4]. Second, Sybil nodes may directly or indirectly inject false data into the networks, greatly impacting on the data consistency of the system. For example, VANETs may rely on multiple vehicles voting to generate a traffic status report. Thus it is very important to localize and detect the Sybil attacks in VANET.

B. SCENARIO

Each node would periodically play two roles, that is, each node is a claimer and a verifier but at various moments and for various purposes.

Claimer phase:

Here, all the vehicles broadcast their identity and position. This includes the Sybil nodes as well. The malicious node pretends to be several Sybil nodes.

1. Each node stored the claimed identity and position in its memory. Every node in the network exchanges the location of all the nodes.

Verifier phase:

Here, the claimed and estimated position of the vehicle is measured.

1. The RSU requests all the nodes for a certificate.
2. If that node is a Sybil node, it won't possess a certificate as it in nonexistent.
3. All physical nodes in the range of that Sybil node is marked with a suspicion factor. This is done because the Sybil nodes might have stolen identity. The position of the Sybil node is calculated using mean estimation position.

D. Using this method, the suspicion factor is increased for nodes under suspicion. The node with the highest suspicion factor is identified as the malicious node.

The next step is to identify the malicious node that caused the Sybil attack. It has to be removed from the network as it may further cause many damages to the other vehicles. The RSUs use the positions of the Sybil nodes and also collect the estimated positions of the Sybil nodes for calculating the mean estimated positions of the Sybil nodes.

The node having the maximum suspicion count will be recognized as the malicious node. If more than two nodes have the same suspicion count, then the energy of the nodes are checked. The malicious node will possess less energy as it acts as many Sybil nodes. Hence the energy of the two nodes are compared with the energy at their initial stages and thus identified.

```
detect_malicious()
{
        RSU sends certificates to all the physical
        nodes for (i= 0 to n) //n is the no of nodes
        within the
transmission range of RSU
    {
```

The algorithm is as follows:

The malicious node can generate Sybil nodes only in its transmission range [3]. Hence by having the estimated positions of the Sybil nodes, the vehicles around the Sybil nodes can be identified. We require this information because the malicious node will be in the range of all the Sybil nodes. We maintain a factor called suspicion factor which keeps incrementing whenever the node comes under the range of the Sybil nodes.

```
        set certificate 0 or 1          //Sybil nodes
    }
        RSU validates the nodes by checking
        certificates
     if {$certificate == 0 }                  //Sybil  nodes
                                                 donot
have certificates
        {
        print "This is a sybil node"
        }
        if {$certificate == 1 }Normal    nodes  have
certificates
        {
        print "This is a normal node"
        }
        RSU finds the claimed and estimated
positions of sybil nodes
        Claimed=(x1,y1)
        Mean Estimated position = (x2,y2)
        Using Mean Estimated position neighbour list of
sybil nodes are generated
        Sybil_node_1 list [Node_1 Node_2 ....
        Node_n]....
        Sybil_node_n list [Node_1 Node_2 ....
        Node_n]....
            for {j = 0 to l} //l is the length of the list
        {
        set l($j) [lindex $mylist $j]
          for (i = 0 to len) //len is the length of
          the inner list
          {
           set m($i) [lindex $l($j) $i]
           set count($m($i)) [expr
           {$count($m($i))+1} ]}
        print "Suspicion factor of $i is $count($
        i)" Find the node with Maximum suspicion
        factor
        print "The node with Maximum
        suspicion factor is
Node_x"
If two nodes have same suspicion factor
        check energy if(energy(Node_x) !=
```

```
        Energy_max))
        {
          Print "Node_x is the Malicious node"
        }
}
```

The algorithm first checks for the certificates from the vehicle nodes if there are any discrepancies in their claimed positions. If the RSUs possess more than one identity for the same node it checks for the certificates and then detects the Sybil nodes. Finally the malicious node has to be detected so that it does not further affect the environment.

A. ALGORITHM

The proposed algorithm works as follows. The vehicles periodically broadcast their positions to the other vehicles and also to the RSUs. The RSUs maintain a database wherein it stores all information about the vehicles regarding their positions. The Sybil nodes also send their positions to others using identity stealing approach.

The RSUs now have ambiguous data in the database as they have more than one entry for the same vehicle because of the Sybil attack. Now the RSUs in their transmission range check for these discrepancies and request for certificates from the vehicles both legitimate and Sybil nodes which have the same identity. The nodes which do not possess certificates can be identified as Sybil nodes. In such a manner all Sybil nodes can be identified. Red circles indicate Sybil nodes and brown indicates the identified malicious node. Fig. 4 shows the suspicion factor of node 5 is 9 and hence is identified as malicious node.

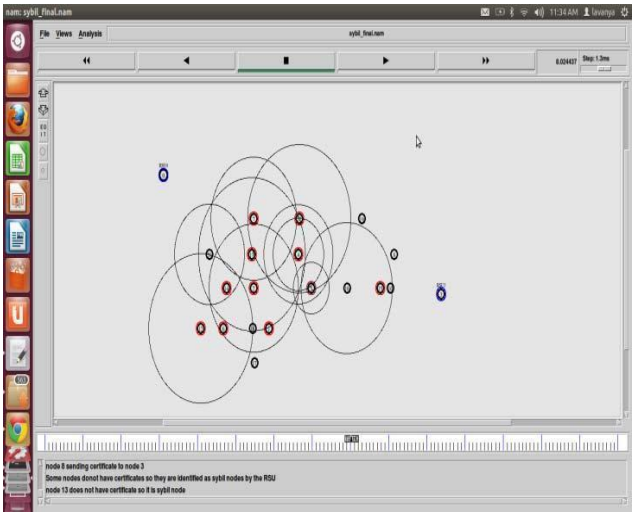

Fig. 3 Sybil nodes and their positions are identified

VI. IMPLEMENTATION AND RESULTS

A. IMPLEMENTATION

The scenario is simulated in NS2 and the algorithm runs with the simulation. Sybil nodes and malicious nodes are identified. Snapshots figure 3 and 4 are given below. Fig. 3 indicates the identified Sybil and malicious nodes.

B. CHALLENGES ADDRESSED

Our algorithm assumes that the highway has a large number of RSUs. This is because the RSU acts as a verifier to check all the nodes with proper certificates and also detects the Sybil and malicious nodes. In contrast, if a vehicle does all the verifications instead of the RSU it works for some cases where the verifier node is not a malicious node. If the verifier node happens to be a malicious node then this node does not check for certificates from the Sybil nodes as it has only caused the attack. This type of node is referred to as a selfish node. To avoid this problem we make the RSU to be the verifier of all nodes which is assumed to be the Trusted Authority (TA). Another problem in making a vehicle to be a verifier is the dynamics of the traffic. A vehicular node keeps moving and thus cannot maintain an up-to-date status of the other nodes. The RSUs are fixed and have higher processing and storage capability thus reducing the problem. This is our novel approach.

C. RESULTS AND COMPARATIVE ANALYSIS

The results thus obtained are compared in the fig. 5 represents the detection accuracy versus number of nodes when suspicion factor is taken into account.

X axis:Number of nodes
Y axis: Detection Accuracy

The comparison is made based on the fact that the verifier node is not a malicious node. In this paper we have assumed the verifier node to be an RSU which is a trusted authority.

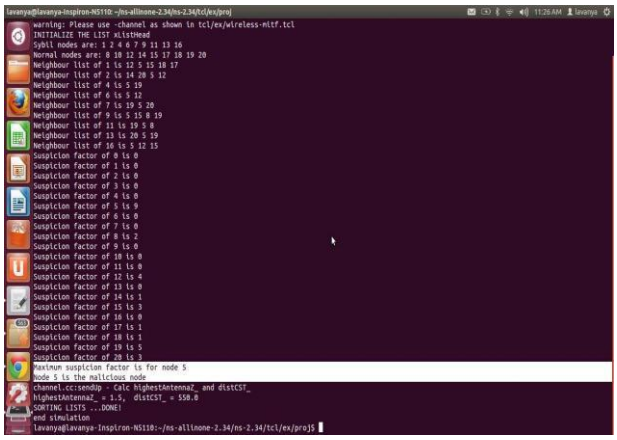

Fig. 4 Malicious node is identified

If the verifier node is a malicious node, then the attack will not at all be determined and the effect may be severe.

Detection Accuracy = (No of Sybil nodes / Total number of nodes) *100

The formula used to compare the values is:

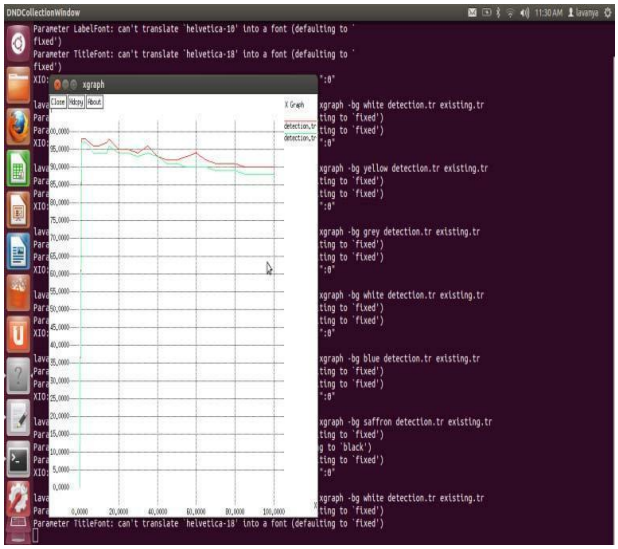

Fig 5: Detection Accuracy

The graph shows that our algorithm holds good even when the number of nodes keeps increasing and is also accurate. Here the green line indicates the accuracy of the existing protocol which does not take into account the fact that the verifier node is a malicious node. The red line which is the performance of the proposed work shows that detection accuracy is much better than the existing ones.

V. CONCLUSION

In our paper, we propose a method to efficiently detect the Sybil nodes and identify the malicious node that generates them. We do this in two phases – claimer and verifier phase. All the Sybil nodes are identified initially and their location is used to increase the suspicion count which identifies the malicious node. The results show that our proposal gives a better performance than the existing methods in identifying and recognizing all the Sybil nodes even when the number of vehicles keeps increasing. In cases where a normal node lies too close to a malicious node, there might be false results which will be worked with in the future.

References

[1] Bin Xiao, Bo Yu, Chuanshan Gao, "Detection and Localization of Sybil Nodes in VANETs" , *ACM, DIWANS'06, Sep 26, Los Angeles, California, USA. 2006.*

[2] Chen Chen, Xin Wang, Weili Han, Binyu Zang "Robust Detection of the Sybil Attack in Urban VANETs*", 29th IEEE International Conference on Distributed Computing Systems Workshops 2009.*

[3] Chen Chen; Xin Wang; Weili Han; Binyu Zang, "Robust Detection of the Sybil Attack in Urban VANETs", *Distributed Computing Systems Workshops,. ICDCS Workshops '09. 29th IEEE International Conference 2009.*

[4] Gilles Guette and Bertrand Ducourthial, "On the Sybil attack detectionin VANET",*IEEE, Laboratoire Heudiasyc UMR CNRS 6599 Universite de Technologie de Compiegne, France 2007.*

[5] Nizar Alsharif, Albert Wasef, and Xuemin (Sherman) Shen "Mitigating the Effects of Position-Based Routing Attacks in Vehicular Ad Hoc Networks", *IEEE Communications Society subject matter experts for publication in the IEEE ICC proceedings 2011.*

[6] Parastoo Kafil, Mahmoud Fathy, Mina Zolfy Lighvan, "Modeling Sybil Attacker Behavior in VANETs",*9th International ISC Conference on Information Security and Cryptology 2012*

[7] ShanshanChen , GengYang , ShengshouChen ,"A Security Routing Mechanism Against Sybil Attack for Wireless Sensor networks",*Communications and Mobile Computing(CMC), International Conference 2010.*

[8] Shaohe Lv ; Xiaodong Wang ; Xin Zhao ; Xingming Zhou Detecting the Sybil Attack Cooperatively in Wireless Sensor Networks",*Computational Intelligence and Security,. CIS '08. International Conference 2008.*

[9] Soyoung Park; Aslam, B.; Turgut, D.; Zou, C.C, "Defense against Sybil attack in vehicular ad hoc network based on roadside unit support",*Military Communications Conference,. MILCOM IEEE 2009.*

[10 Wei Wei, Fengyuan Xu, Chiu C. Tan, Qun Li, "Sybil Defender: A] Defense Mechanism for Sybil Attacks in Large Social Networks"*IEEE Transactions On Parallel And Distributed Systems, IEEE 2013.*

[11] Nai-Wei Lo, Hsiao-Chien Tsai, "Illusion Attack on VANET Applications A Message Plausibility Problem",*National Taiwan University of Science and Technology, Taipei.*