ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

Sybil Attack in Vanet by Neighbourhood Information Passing

Mr. Pankaj Kumar [1], Mr. Vikas Kumar[2] , Dr. Jagjit Singh[3]
[1] Department of ECE, Samalkha Group of Institutions, Samalkha, India
[2]Assistant Professor ,Department of ECE, Samalkha Group of Institutions, Samalkha, India
[3]Associate Professor ,Department of ECE, DAVIET Jalandhar, India
pnkjkakkar5@gmail.com

Abstract

In this paper, we will present one of the most applicable forms of Ad-Hoc networks; the Vehicular Ad-Hoc Networks (VANETs). VANET is the technology of building a robust Ad-Hoc network between mobile vehicles and each other, besides, between mobile vehicles and roadside units. It also demystifies some excerpts from the IEEE 802.11 standard that are related to the operation in the Ad-Hoc mode and illustrates the main points of its amendment in vehicular environments (IEEE 802.11p). Communications in wireless sensor networks are usually based on a unique identity that represents a network entity i.e. a node. Identities are used as an address to communicate with a network entity. In a Sybil attack a malicious node can generate and control a large number of logical identities on a single physical device. This gives the illusion to the network as if it were different legitimate nodes. A malicious device's additional identities are known as Sybil nodes. This proposed work presents an algorithm to detect Sybil nodes having fabricated identities in a vehicular ad hoc network. Vehicular ad hoc network have many applications and if it is attacked by Sybil node then harmful situation can be created. To avoid this we have proposed a modified neighborhood algorithm for a city. The proposed algorithm checks the results for different sizes of blocks in the city and different number of Sybil nodes. For simulation purpose MATLAB has been used as a tool and inclusion of Sybil nodes number in the city is purely based on user's desire. Results for different number of Sybil nodes will be checked for different block sizes of city.

Keywords: Sybil Attack, Network Entity,Ad-Hoc Network, Wireless Sensor Networks

Introduction

Wireless research field is growing faster than any other one. It serves a wide range of applications under different topologies every one of which comes with some new specialized protocols. In this research, we will present an introduction to a wireless technology that is expected to be adopted by both governments and manufacturers in the very near future. It directly affects car accidents which is the first cause of death in the age group 1 - 44 years and the sales of one of the largest markets. It is the technology of building a robust network between mobile vehicles; i.e. let vehicles talk to each other. This promising technology is literally called Vehicular Ad-Hoc Networks (VANETs). VANET is the technology of building a robust Ad-Hoc network between mobile vehicles and each other, besides, between mobile vehicles and roadside units. There are two types of nodes in VANETs; mobile nodes as On Board Units (OBUs) and static nodes as Road Side Units (RSUs). This work addresses a critical and emerging security problem in vehicular networks, namely detecting the presence of Sybil attacks. Sybil attacks are classified as an attack on the trust of a peer-to-peer system by an attacker assuming many pseudonymous identities. Using these identities, the attacker can gain a disproportionately large influence on system functionality. In vehicular networks, the presence of a Sybil attack can have negative consequences. For instance, in an application like road safety, consider a single malicious vehicle, *VM*, assuming a large number of fake identities incorrectly reporting road conditions. Other benign vehicles will tend to believe such a message, since it appears to be coming from multiple vehicles, and may adjust their routes. In such a case *VM* can potentially obtain exclusive access to the road, which it otherwise could not. A number of other applications like content exchange, intelligent traffic signaling, and ramp metering can all be compromised in the presence of Sybil attacks. Unlike static networks like the Internet, vehicular motilities make Sybil detection very difficult with the added spatio-temporal constraints.

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

In this research, an introduction to the technology of VANETs will be presented as well as a new contribution with a novel broadcasting protocol

Classification of Sybil Attack & Sybil Defences

In order to detect the Sybil attack it is necessary to understand the different forms in which the network is attacked .

(a) Direct and Indirect Communication

In direct attack, the legitimate nodes communicate directly with Sybil nodes whereas in indirect attack, the communication is done through malicious node.

(b) Fabricated and stolen identities:

It creates a new identity for itself based on the identities of the legitimate nodes, that is, if legitimate nodes have an ID with length 32 bit integer, it randomly creates ID of 32 bit integer. These nodes have fabricated identities.

In stolen identities, attacker identifies legitimate identities and then uses it. The attack may go unidentified if the node whose identity has been stolen is destroyed. Identity replication is when the same identities are used many times in the same places.

(c)Simultaneous and non simultaneous attack

In simultaneous, all the Sybil identities participate in the network at the same time. Since only one identity appears at a time, practically cycling through identities will make it appear simultaneous.

The number of identities the attacker uses is equal to the number of physical devices; each device presents different identities at different times

Besides the broad classification of Sybil defenses into centralized and decentralized defenses, as described in above section, the defenses we survey in this thesis include two major and broad categories of techniques: trusted certification and resource testing categories, as shown in Figure 1. Among the schemes in the trusted certification category, we survey works that use a centralized certification authority (CCA), decentralized cryptographic primitives, or trusted devices. Among works that use resource testing, we are particularly interested in works that use IP testing, cost recurrence, and social graphs. While a broad survey is provided for these techniques, detailed descriptions are provided for cryptographic primitives and social graph–based techniques.

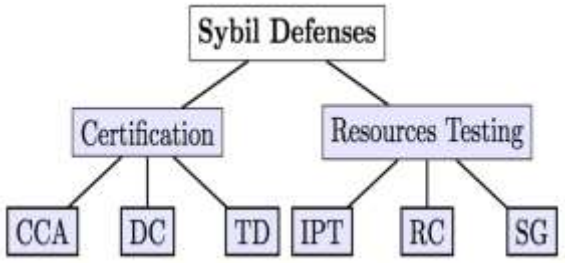


Figure 1: An illustration of the different types of defenses against Sybil attacks in P2P overlays.

Proposed Algorithm

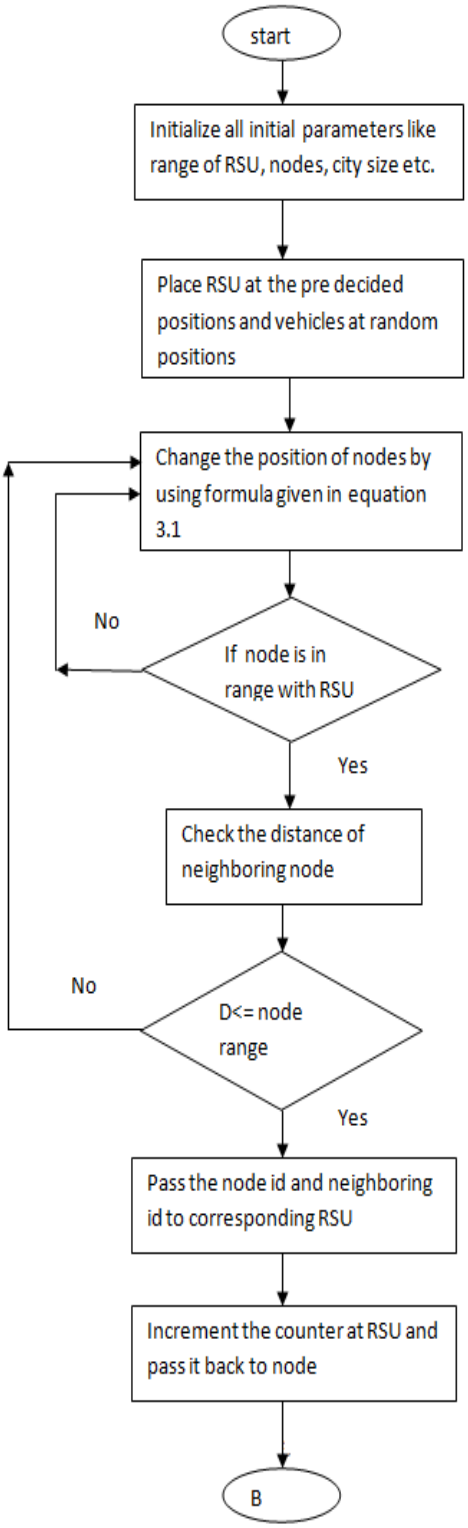
In this work we have developed VANET for a small city which is spread in 100*100 km^2 area. RSU's are placed at certain distance in the city with equal range. Whenever any vehicle comes into range of RSU, then information transfer is done between vehicle and RSU and RSU maintain a table for the data of vehicle. Every vehicle transfers the information of each neighbor into its range to RSU. As discussed in previous chapter, Sybil attack is the problem in VANET which can transfer wrong information to RSU, so it is required to detect the Sybil node and to remove it. For this purpose we have modified neighborhood detection method by disrupting the communication only in between neighbors. This method doesn't require any centralize unit to issue authentication certificates to vehicles and vehicle is only registered with the RSU by which it is passing. It reduces the overhead cost of certificated carrying by each vehicle.

In our proposed work each vehicle is considered as a node and flexibility in simulation has been provided to change the number of nodes. Theses nodes move randomly in the prescribed geographical region. As discussed earlier these nodes continuously keep an eye over their neighbors and pass the neighbor ID to RSU in contact with the node. We have customized our simulation with the facility to change the number of Sybil nodes and to their positions also. Sybil nodes are placed to chase the nodes. Since all Sybil nodes have same IDs, so we have also assigned same ID to each Sybil node. It has been assumed here in our work that no node can chase any other node for a long distance in any city. This gives us the principle of protocol designed to detect Sybil nodes. Whenever RSU will see any ID is chasing any node for a long distance as per mentioned in the protocol, then that node will be declared as Sybil node. Every Sybil node is provided ID other than all other nodes have. Here algorithm is divided into three steps mainly:

- Nodes and RSUs placement

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

- Sybil nodes position assignment
- Sybil node detection



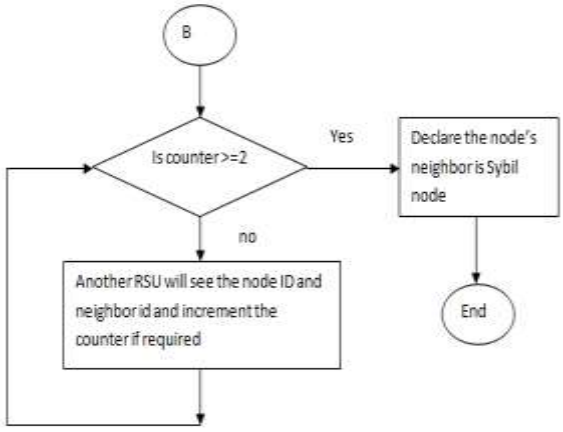


Figure 2: Flow chart of proposed algorithm

Results and discussion

As discussed in proposed work our work detects the node which is followed by Sybil node. We have considered some assumptions which are:

- Vehicles don't move outside the geographical area defined
- Range of every RSU and every vehicle for communication is assumed to be same
- Transmission power is same for Sybil node and authentic node
- No collision of message and vehicle is considered

Case: A city, which is spread into an area of 100 *100 square kilometer, is designed first in MATLAB which is shown in figure 3 below.

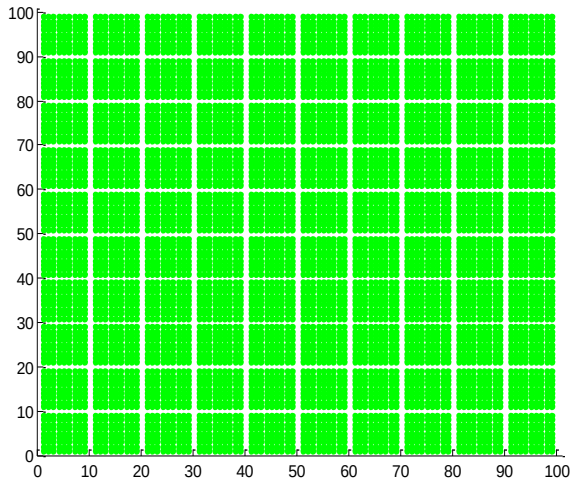


Figure 3: city designed in MATLAB

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

Table 1. Initial Parameters considered for simulation

RSU range	7.7 km
Node range	3 km
Number of vehicles	100
Number of Sybil nodes	5
RSU id	1472014-1472063
Node id	1-100

Here initially 5 sybil nodes are considered which can be altered and their position is selected randomly or their positions can be manually decided. Here we are considering the case of random position. Initial position of authentic nodes and Sybil nodes in the city is shown in figure 5. The black points in the figure represent the authentic nodes and points in magenta color represent Sybil nodes. Whenever any node comes in range of any of RSU then communication starts between node and RSU as shown by blue lines in the figure which shows the node in range of RSU. Figure 5 shows the position of nodes and Sybil nodes at different simulation time. Here the id of every Sybil node is kept same as this is the property of Sybil node that their id will be same irrespective of the number of Sybil nodes.

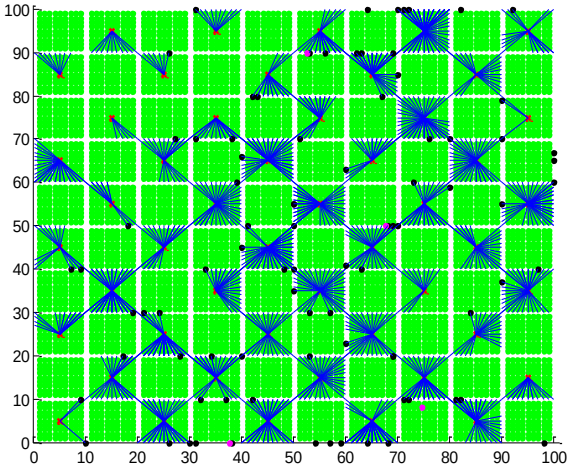


Figure : 4 Authantic Node moving in city

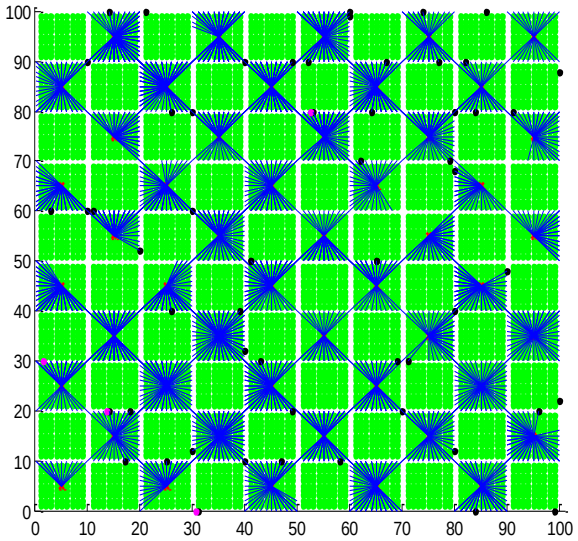


Figure 5 Sybil nodes moving in the city

These nodes keep on moving in the city till all nodes move out of geographical area which is shown in figure 5.

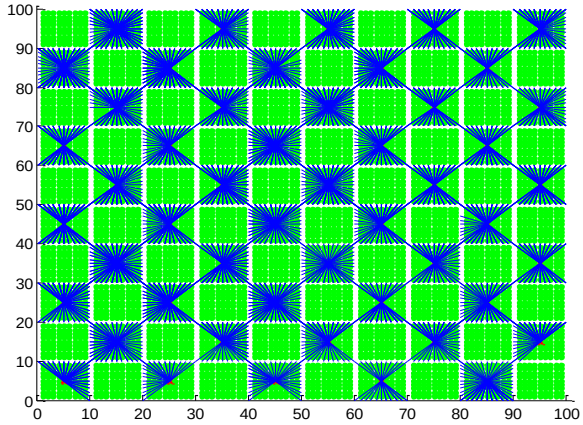


Figure 6: All nodes move out of city

If number of Sybil nodes is changed then also our algorithm is able to detect nodes. Figure 7 shows that into graphical representation for more insight understanding. Figure 7 compares the correct recognition rate with the number of actual Sybil nodes in the network and figure 8 shows the comparison of percentage of correct Sybil node detection with the number of nodes. Form bar graph it is clear that when Sybil nodes were 5, then correct detection percentage is highest. The statistics may change in next time simulation as random positions of nodes are used every time.

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

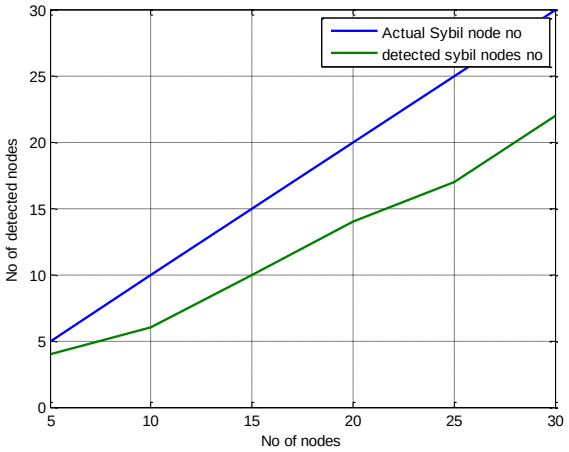


Figure 7: Comparison of correct detection of Sybil nodes with total Sybil nodes

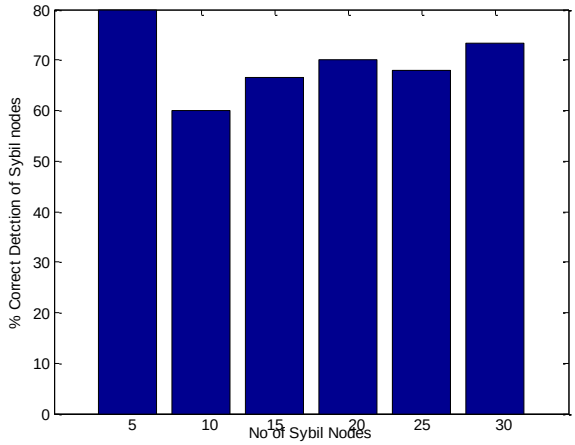


Figure 8: bar chart for % correct detection of sybil nodes

Conclusion

In this paper we focused on the development of security mechanisms to thwart the Sybil attack in wireless ad hoc networks. The cornerstone of our work are resource tests, a promising technique that allows the mitigation of sybil identities, without requiring any pre-configuration of the nodes, being thus able of improving the scalability of the network. In this neighboring information by vehicles is transferred to road side units at a cost very less overhead in transmission and rest work lies with RSU not with vehicle. RSU adds a counter to information traversed back to vehicle so that other RSU can check the previous information of vehicle. This information helps RSU to identify the Sybil node.

References

[1] Ali Akbar Pouyan, Mahdiyeh Alimohammadi," Sybil Attack Detection In Vehicular Networks" Computer Science And Information Technology 2(4): 197-202, 2014.

[2] Roopali Garg, Himika Sharma," Comparison between Sybil Attack Detection Techniques: Lightweight and Robust" International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, Vol. 3, Issue 2, February 2014.

[3] D. R. Bild, Y. Liu, R. P. Dick, Z. M. Mao, and D. S. Wallach, "The Mason test: A defense against Sybil attacks in wireless networks without trusted authorities," IEEE Trans. Mobile Computing, under review, Mar 2014.

[4] K. Kayalvizhi, N. Senthil kumar, G. Arulkumaran," Detecting Sybil Attack by Using Received Signal Strength in Manets" International Journal of Innovative Research in Science & Engineering, March 14.

[5] Sohail Abbas, Madjid Merabti, David Llewellyn-Jones, and Kashif Kifayat," Lightweight Sybil Attack Detection in MANETs" IEEE Systems Journal, Vol. 7, No. 2, June 2013.

[6] Mina Rahbari1 and Mohammad Ali Jabreil Jamali," Efficient Detection Of Sybil Attack Based On Cryptography In Vanet" International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.6, November 2011.

[7] Himadri Nath Saha , Dr. Debika Bhattacharyya , Dr. P. K.Banerjee," Semi-Centralized Multi-Authenticated RSSI Based Solution to Sybil Attack" International Journal of Computer Science & Emerging Technologies, Volume 1, Issue 4, December 2010.

[8] 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, 2009. MILCOM 2009. IEEE , vol., no., pp.1,7, 18-21 Oct. 2009.

[9] Piro, C.; Shields, C.; Levine, B.N., "Detecting the Sybil Attack in Mobile Ad hoc Networks," Securecomm and Workshops, 2006 , vol., no., pp.1,11, Aug. 28 2006.

[10]James Newsome, Elaine Shi, Dawn Song," The Sybil Attack in Sensor Networks: Analysis & Defenses" IPSN'04, April 26–27, 2004, Berkeley, California, USA.