A Secure Model for Prevention of Sybil Attack in Vehicular Ad Hoc Networks

Azita Soltanian Bojnord
Dept. Software Engineering
Payame Noor University
Tehran, Iran

Hoda Soltanian Bojnord
Dept. Information Security
University of Technology Malaysia
Kuala Lumpur, Malaysia

Abstract:
Recent technology known as Vehicular Ad Hoc Network (VANET) is invited to serve new vehicle driving experience. It is very useful to mitigate collision and utilizes traffic. Even though, VANET seems to be a promising technology, its drawbacks are inadequate with the security for a public accessible technology. VANET security is essential because a badly designed VANET is vulnerable to network attacks, and this may danger the safety of drivers, and As long as VANETs are the wireless network, there are different kinds of attacks and threats can happen in VANETs. Sybil attack is one of the most important attacks in VANETs. This thesis deals with the problem of the security in VANET especially in Sybil attack. In this research, a robust detection mechanism against Sybil attack in VANET is addressed based on fuzzy detection mechanism. Our contribution behind the implementation of proposed approach is that each vehicle has different set of neighbors providing sufficiently high density in VANET.

Key-Words:
Vehicular Ad hoc Networks, Sybil attack, Security, Fuzzy logic

1. Introduction

Vehicular Ad Hoc Network (VANET) is a subcategory of Mobile Ad hoc Networks (MANET). The main intention of VANET is to provide passengers' comfort and safety by broadcasting traffic, road and weather conditions among a group of neighboring vehicles. VANET consists of a number of On Board Units (OBU) which are located inside the vehicles and a number of Road Side Units (RSU) which form the infrastructure of the network. VANET is providing vehicle to vehicle and vehicle to Road Side Units (RSU) communication; hence, Communication in VANET is divided into two different categories: Vehicle-to-Vehicle (V2V) Communication and Vehicle-to-Infrastructure (V2I) Communication (Wang and Li 2009). Integrating vehicles with fixed position infrastructures in a communicating model produces complexity which is raised by unique mobility model (routes, speed and contiguous nodes), highly dynamic network topology, short-lived communication link, rich network nodes resources (e.g., high computing ability, unlimited power supply), and scattered authorized infrastructures to provide extra services in some intersections and hot spots (Manvi and Kakkasageri 2008). Maintaining Security in VANETs is a crucial issue to be discussed by experts. In this paper a secure model against Sybil attack is proposed and discussed. Sybil attack is a serious threat able to paralyze the VANET. This attack is working by broadcasting huge amount of messages in the network by simulating multiple identities which is duplicated from other nodes. The node which own the identity named Sybil nodes, and the node which spoof the identity is called malicious node/Sybil attacker (Douceur 2002). Sybil attack is important to be prevented in VANET as it enable other attacks to be taken into place. One possibility could be creating an illusion of a traffic jam or accident so that other vehicles change their routing path or leave the road for the benefit of the attacker. Sybil attacker can also inject false information in the networks via some fabricated non existing nodes.

2. Related Works

Douceur introduced the Sybil attack in a peer to peer network in 2002. In (Douceur 2002), one of the possible solution for preventing this attack is proposed in a way that all physical entities should be equipped with limited computational resource, bandwidth and storage; hence, these limitations is preventing Sybil node to lunch any attack as the simulating multiple identities requires more computational resource than usual. Aforementioned solution may suitable for peer to peer network, but Ad hoc Network's has access to higher resources than peer to peer networks. Another drawback of using limited resources is the possibility of creating network congestion in instances when the number of request/reply to a node is increased.

One efficient approach to protect network is to use Cryptographic-based methods which increase the reliability of receiving position and identities requested by vehicles. Many great works (Golle, Greene et al. 2004, Hubaux, Capkun et al. 2004, Kuhn 2005, Raya, Aziz et al. 2006, Raya and Hubaux 2007) has been done on position security by PKI method. Digital signatures are discussed in (Parno and Perrig 2005, Choi, Golle et al. 2006,

Manuscript received January 5, 2017
Manuscript revised January 20, 2017

Armknecht, Festag et al. 2007, Chen, Wang et al. 2009, Chen, Han et al. 2011). Apart from many advantages of using cryptography, a barrier on the road to apply it is that due to the variety of models and manufacturer of vehicles, it needs huge effort to setup a global cryptographic method.

An innovative validation approach for using in sensor networks -called Radio Resource testing- has been proposed by Newsome et al. In this method each physical device is assumed to have only one radio and the radio is capable of sending and receiving message only in one channel simultaneously. One major security drawback of this approach is that the security cannot be guaranteed if the radio transmitter/receiver is customized. Also, high energy consumption is another obstacle in using this method (Newsome, Shi et al. 2004). The resource testing method is not applicable in Analyzing the signal strength for position verification is employed to detect and locating the Sybil node in VANETs. This lightweight security method was proposed by Xiao et al. It begins with feasibility assessment of the location detection of vehicles by using signal strength. Each node is playing three roles in this scheme. Claimer is the node that broadcast a bacon message which contain the identity and its GPS position, in order to find its neighbors. Second possible role is Witness who is the contiguous nodes within the signal range and saves the corresponding information in their memory. Last role is the Verifier who confirms the position of the claimer vehicle by matching the information of witness and claimer (Xiao, Yu et al. 2006).

Zhou et al. was proposed a Privacy preserving scheme to detect Sybil attacks in VANETs. Based on this method, a set of predefined pseudonyms is stored in Department of Motor Vehicle (DMV) and RSU. Vehicles randomly pick one pseudonym which is hashed to specific common value, in order to hide their unique identity and communicate in the network by their new identity. The Sybil node is detected while pseudonyms used to communicate to RSU is different from the pseudonym sets or is previously picked with other entity. The suspected node information will be sent to DMV for getting its hashed identity and putting the identity in the black list. In this scheme the privacy of the vehicles are preserved, but the vehicle should be registered in DMV. This method has lack of feasibility because of the huge number of vehicles and producing large number of pseudonyms (Zhou, Choudhury et al. 2011). Position Based Application method is a position based protocol for privacy preserved VANET to detect Sybil attack proposed by Hao et al. This protocol works based on geographic information of vehicles and has three phases. Probing, confirmation and quarantine. The information contained indices of M nearest front and behind vehicles along with its geographical information broadcasts in the network during probing phase. In the confirmation phase, these indices are compared by vehicles, if any anomaly position is detected, the index of the suspect vehicle is signed by a private key and broadcast it as a warning message with the corresponding partial signature periodically in the control channel periodically. In the quarantine phase, it will quarantine the Sybil node by piggybacking of the latest geographical information and the corresponding complete signature in their own safety related messages. The efficiency of this method is proved by simulation but it works only for one Sybil node and one malicious vehicle (Hao, Tang et al. 2011).

3. Proposed Model

In the previous scheme, this localizes the fake identities of malicious vehicles by analyzing the consistent similarity in neighborhood information of neighbors of these fake identities. Beacon packets are exchanged periodically by all the vehicles to announce their presence and get aware of neighboring nodes. Each node periodically keeps a record of its neighboring nodes. In proposed approach, each node exchange groups of its neighboring nodes periodically and perform the intersection of these groups. If some nodes observe that they have similar neighbors for significant duration of time, these similar neighbors are identified as Sybil nodes. Proposed approach is able to locate Sybil nodes quickly without the requirement of secret information exchange and special hardware support. But, in the real network this method has very low accuracy in true detection rate. In the proposed method, we try to improve this method with considering global information called as network opinion and local information including neighborhood duration (the previous method) and the received power strength. Moreover, to make high accurate decision about miss-behaving of one neighbor, we use a fuzzy logic controller.

The proposed system is based upon fuzzy logic. Fuzzy logic is a form of multi valued logic derived from fuzzy set theory to deal with reasoning that is approximate rather than precise. In contrast with “crisp logic”, where binary sets have binary logic, fuzzy logic variables may have a truth value that ranges between 0 and 1 and is not constrained to the truth values of classic propositional logic. The fuzzy model is integrated with neighbor discovery mechanism as shown in figure 1. It consists of following two components namely neighborhood manager module and Fuzzy decision maker. During fuzzy parameter extraction, the system extracts the parameters required for analysis from network traffic by using the periodic hello messages. These parameters are passed to neighbor manager list and then to fuzzy decision maker module, which applies various fuzzy rules and membership functions to calculate malicious level of the neighbor nodes. This malicious level is compared with threshold value in fuzzy verification module to check the behavior of node and if, malicious level is less than threshold level, an alarm packet with the IP address of detected malicious node is broadcasted in the network. Every node has a list of neighbor nodes and their related parameters (e.g. the received power level and global opinion). Every node periodically send hello message (beacon) to inform neighbor nodes the last update about malicious level of nodes. Upon one node receive a hello message, it update the list and make a fuzzy decision for each entry to determine the new level of malicious for neighbor nodes. Node sends the new updated information to its neighbors in the next hello message.

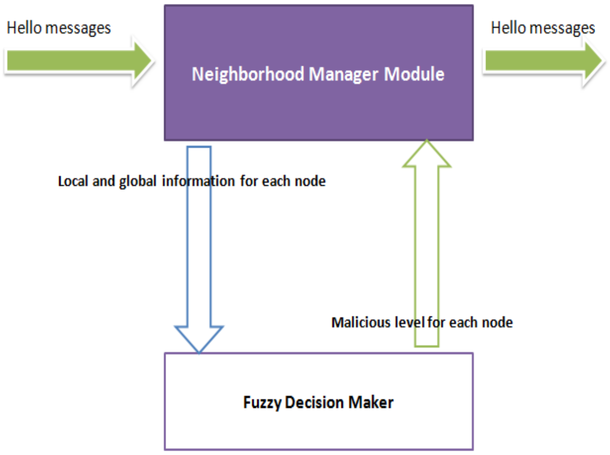
Hello messages
Neighborhood Manager Module
Hello messages
Local and global information for each node
Malicious level for each node
Fuzzy Decision Maker

Figure 1. Different modules of the proposed scheme in every for detecting Sybil attacks

In fact, one node makes a decision based on local information in neighborhood and other node's opinions. Hello message has different information shown in table 1.

Table 1: Structure of hello message

Source ID
Malicious id list
Malicious level list

Every node maintains a table including neighborhood information. The following table 2 presents the structure of this table.

Table 2: Structure of table

Neighbor node
Malicious list
Malicious level
The received power
Node opinion
Network opinion

The values of node opinion and network opinions are computed by using the following equations. In the first equation, the malicious level of one node is computed by the previous node and network opinion. In the second equation, network opinion is updated based on the previous value of network opinion and sum of opinion of neighbor nodes.

$$malicious_{level_t}(i,j) = fuzzy\_module\_output(node_{opinion_{t-1}}(i,j), network\_opinion_t(i,j))$$

$$\underset{j \epsilon \text{ neighbors}}{\text{network\_opinion}_t(\text{current node}, j)} = \propto \text{ network\_opinion}_{t-1}(i,j) + (1- \propto) \sum_{k=1}^{|\text{Neighbor}|} \text{node\_opinion}_{t-1}(k,j)$$

To define node opinion how is determine by each node, notice to following figure 2:

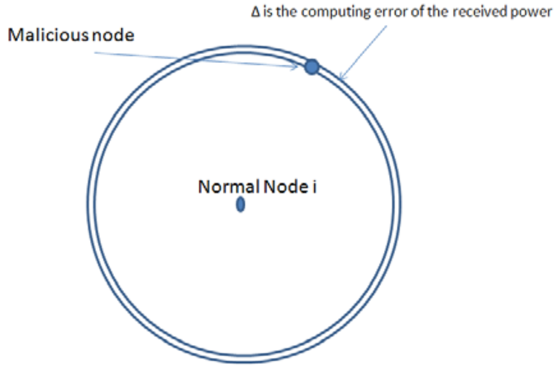

Figure 2. Source area of possible attacks

$$\underset{\text{i} \epsilon \text{ neighbors}}{\text{node\_opinion}_t(\text{current node, i})} = \{node\_opinion_t(current\ node, i) - \delta||P_i - P_j| \leq \Delta\}$$

We apply an aging mechanism to node opinion, to improve the level of well behavior nodes. Each node in a periodic time runs fuzzy decision making process to determine malicious level of neighbor nodes, notice to the following figure 3 and 4.

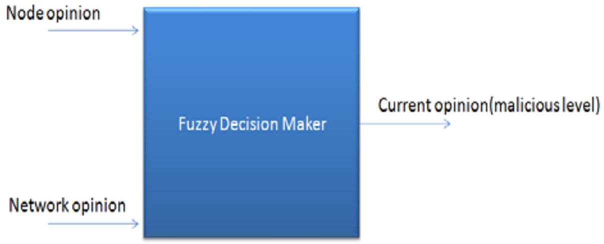

Figure 3. Fuzzy decision maker

```
                    Handle function(EVENT)
{
  If (EVENT== Hello_Message_Arrival )
  {
    gather information( malicious list, ..)
    compute the received power and update malicious node list
    update information table
  }
  Else if(EVENT==FUZZY_DECISION_MAKING)
  {
    For all nodes in table
    {
       Extract network and node opinion
       Make a fuzzy decision and  compare its result with threshold
       update malicious level
    }
  }
  Else if (EVENT==AGING_TIME)
  {
    Decrease malicious level of nodes, which are in sections with
    no abnormality
  }
}
```

Figure 4. pseudo code of the proposed scheme

3.1 Fuzzy Decision Maker

To fuzzily the input variables in fuzzy decision maker, we use the following membership functions:

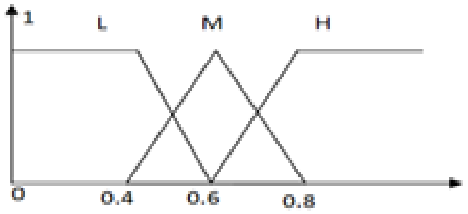

Figure 5. Membership function of fuzzy decision maker

The membership function of figure 5 is applied to the both of input variables in the fuzzy decision maker module.

3.2 Value of malicious level

We use table 3 to judge about the value of malicious level of node.

Table 3 : Value of Malicious Level

	Network Opinion is LOW	Network Opinion is MEDIUM	Network Opinion is HIGH
Node Opinion is LOW	Normal	Normal	Suspicious
Node Opinion is MEDIUM	Normal	Suspicious	Malicious
Node Opinion is HIGH	Suspicious	Malicious	Malicious

4. Conclusion and future work

Our contribution behind the implementation of proposed approach is that each vehicle has different set of neighbors providing sufficiently high density in VANET. These neighbors can provide helpful information and participate in detection mechanism to improve the precision of algorithms. One attacker tries to send different beacon packets with different source ID. So, the neighbors can watch this event with tracking the received powers. This feature of Sybil attacker is exploited in our research by creating groups of neighboring nodes at discrete time intervals and comparing the neighbor information collected from neighboring nodes. After gathering the neighborhood information, we use an efficient fuzzy decision maker to decide about level of malicious of attacker. If malicious level of one attacker is greater than a threshold, it will be considered as a malicious node. Our scheme is simple and efficient as compared to existing detection approaches because it does not require secret information exchange and special hardware support. As a part of future work, we would like to perform the experiments with different heuristic methods like as genetic and neural networks.

References

[1] Armknecht, F., et al. (2007). Cross-layer privacy enhancement and non-repudiation in vehicular communication. Communication in Distributed Systems (KiVS), 2007 ITG-GI Conference, VDE.

[2] Chen, C., et al. (2011). "Sybil attack detection based on signature vectors in VANETs." International Journal of Critical Computer-Based Systems 2(1): 25-37.

[3] Chen, C., et al. (2009). A robust detection of the sybil attack in urban vanets. Distributed Computing Systems Workshops, 2009. ICDCS Workshops' 09. 29th IEEE International Conference on, IEEE.

[4] Choi, J. Y., et al. (2006). Tamper-evident digital signature protecting certification authorities against malware. Dependable, Autonomic and Secure Computing, 2nd IEEE International Symposium on, IEEE.

[5] Douceur, J. R. (2002). The sybil attack. Peer-to-peer Systems, Springer: 251-260.

[6] Golle, P., et al. (2004). Detecting and correcting malicious data in VANETs. VANET '04 Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks, ACM.

[7] Hao, Y., et al. (2011). Cooperative sybil attack detection for position based applications in privacy preserved VANETs. Global Telecommunications Conference (GLOBECOM 2011), 2011 IEEE, IEEE.

[8] Hubaux, J. P., et al. (2004). "The security and privacy of smart vehicles." Security & Privacy, IEEE 2(3): 49-55.

[9] Kuhn, M. (2005). An asymmetric security mechanism for navigation signals. Information Hiding, Springer.

[10] Manvi, S. and M. Kakkasageri (2008). "Issues in mobile ad hoc networks for vehicular communication." IETE Technical Review 25(2): 59-72.

[11] Newsome, J., et al. (2004). The sybil attack in sensor networks: analysis & defenses. Proceedings of the 3rd international symposium on Information processing in sensor networks, ACM.

[12] Parno, B. and A. Perrig (2005). Challenges in securing vehicular networks. Workshop on Hot Topics in Networks (HotNets-IV).

[13] Raya, M., et al. (2006). Efficient secure aggregation in VANETs. Proceedings of the 3rd international workshop on Vehicular ad hoc networks, ACM.

[14] Raya, M. and J. P. Hubaux (2007). "Securing vehicular ad hoc networks." Journal of Computer Security 15(1): 39-68.

[15] Wang, Y. and F. Li (2009). Vehicular ad hoc networks. Guide to wireless ad hoc networks, Springer: 503-525.

[16] Xiao, B., et al. (2006). Detection and localization of sybil nodes in VANETs. Proceedings of the 2006 workshop on Dependability issues in wireless ad hoc networks and sensor networks, ACM.

[17] Zhou, T., et al. (2011). "P2DAP—Sybil attacks detection in vehicular ad hoc networks." Selected Areas in Communications, IEEE Journal on 29(3): 582-594.