VANET'07 Poster: Providing VANET Security Through Active Position Detection

Gongjun Yan, Gyanesh Choudhary, Michele C. Weigle, Stephan Olariu
Department of Computer Science,Old Dominion University,
Norfolk, VA 23529-0162, USA
{ygongjun, gchoudha, mweigle, olariu}@cs.odu.edu

ABSTRACT

Our main contribution is a novel approach to enhancing position security in VANET. We achieve *local* and *global* position security by using the on-board radar to detect neighboring vehicles and to confirm their announced coordinates. We compute cosine similarity among data collected by radar and neighbors' reports to filter the forged data from the truthful data. Based on filtered data, we create a history of vehicle movement. By checking the history and computing similarity, we can prevent a large number of Sybil attacks and some combinations of Sybil and position-based attacks.

Categories and Subject Descriptors: C.20[Computer-Communication Network]: General-Security and protections

General Terms: Design, Security

Keywords: Vehicular ad hoc networks, security, radar

1. INTRODUCTION

Vehicle position is one of the most valuable pieces of information in a Vehicular Ad-hoc NETwork (VANET). Adversaries, such as pranksters and malicious attackers [1], may harm the VANET by modifying existing packets or inserting bogus packets. Specially, an attacker may create the illusion of a traffic jam before selecting an alternate route to his advantage. The attacker could also replay packets, pretending to be at a fake position to create the illusion of a bona-fide vehicle. Another well-known attack is the Sybil attack [2] which is launched by forging multiple identities. This attack gives the illusion of numerous cars in the traffic and may have a serious effect on VANET, such as network connection, bandwidth consumption, and even a threat of life.

Interestingly, on-board radar is already used in advanced cruise control systems [3]. It is natural, therefore, to enlist the help of these devices for the purpose of enhancing the security of the information flow in VANET. A classic example of "anti-social" behavior in VANET is for malicious cars to fake their true position. Our main contribution is to show that by using GPS and radar-provided information one can ensure the validity of position information in the VANET by detecting and isolating malicious. Underlying our solution is the famous adage: "*Seeing is believing*". We use on-board radar as the virtual "eye" of a vehicle. Although the "eyesight" is limited due to modest radar transmission range, a vehicle can "see" surrounding vehicles and hear reports of their GPS coordinates. By comparing what is heard and seen to what has been reported, a vehicle can corroborate the real position of neighbors and isolate malicious vehicles to achieve local security. Due to the inherent limitation of radar spatial penetration, we need to combine local security with global security. We use preset position-based cells (through which we achieve local security) to create a communication network by exchanging messages among cells and verifying vehicles' position using the oncoming traffic's on-board radar. In this way, we achieve global security. An observer vehicle stores position data in a time series to form a movement history of the observed vehicles. The movement history can help determine whether new received data is valid or not. We isolate vehicles which send invalid data. This isolation can help to prevent a large number of position-based attacks, Sybil attacks, and some combinations of position and Sybil attacks.

2. THE SYSTEM MODEL

Vehicles represented in this paper are assumed to have following features: 1) A GPS navigation system including a GPS receiver and GPS maps; 2) A front and a rear radar. We assume that the omni-directional front radar can detect neighboring cars within line of sight in a radius of 200 meters. 3) A computer center, which will provide data processing, computing and storage; 4) A wireless transceiver, using Dedicated Short Range Communications (DSRC) for communications; 5) A unique ID, such as an electronic license plate which is issued by a registration authority. We assume that vehicles can lie about their GPS positions and their unique IDs. If an attacker changes its GPS position, a position attack is launched. If an attacker forges a vehicle's ID, a Sybil attack is launched. In some cases, a combination of these two attacks can be launched.

3. LOCAL AND GLOBAL SECURITY

We combine proactive and reactive corroboration using radar to get the relative velocity, angle and position to the target object. When an observer vehicle does not receive any packets from a observed vehicle in a certain period of time, a timeout counter will increase by one. If the timeout counter increases beyond a threshold, the observer vehicle will transmit a radar signal to test the observed vehicle's position. Radar detection will also be triggered at a random time during the on-going communication with a vehicle. The rationale for this latter strategy is to ensure that a trusted vehicle remains trustworthy.

VANET'07, September 10, 2007, Montréal, Québec, Canada.
ACM 978-1-59593-739-1/07/0009.

Since GPS has precision tolerance, there is a region of possible values for the real GPS position as shown in Figure 1. Similarly, there has a possible region for data detected by radar. If there is an intersection between the GPS position dark shadow and radar light position shadow, this means the actual GPS position is very close the value which is detected by radar. Therefore, we claim that we can accept the GPS position.

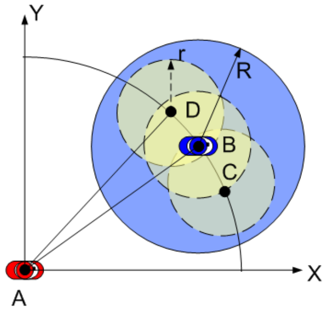

Figure 1: ***Confirming GPS coordinates with GPS and radar position***

Vehicles are grouped into preset cells based on their GPS location. Global security is based on the fact that vehicles in the same cell see and hear almost the same traffic and road situation, so any modification done by malicious nodes can be detected by other honest vehicles. These honest vehicles then broadcast the correct record and isolate the malicious vehicle. Locally secured position and speed information needs to be propagated so that other vehicles approaching the cell can benefit from it. We have chosen a cell router for each direction, which is responsible for forwarding this information, to minimize collisions and bandwidth usage. When a remote vehicle's position needs to be verified, a request can be propagated to a position where radar can be used. The result is propagated back the requester.

4. MAP HISTORY

Each vehicle in a cell knows the exact position of all the remaining vehicles in a cell by exchanging packets. Vehicles in a cell can query the position of a specified vehicle among the neighbors in the cell. When receiving responses from neighbors and computing these positions, the requester comes to an agreement about all the neighbors' position. With locally radar-detected data, oncoming traffic's radar detected data, and trusted neighbors's data in hand, we apply cosine similarity to these data. If the similarity value is above a threshold, we accept the data, otherwise it is dropped. With the accepted data, we build a history of vehicle movements, or a Map History. The Map History of a remote vehicle is built in the observer vehicle's memory. The basic idea is that a vehicle without position history is not trustable, just like a person without credit history can not obtain a loan. When receiving a position announcement, the observer checks the Map History to verify the position based on movement consistency. For example, if a computed position is outside of the road (position A in Figure 2), then based on the Map History, it is rejected. If the position is supposed to be between $t_0 - t_1$, but it reports position B in Figure 2, then it is rejected.

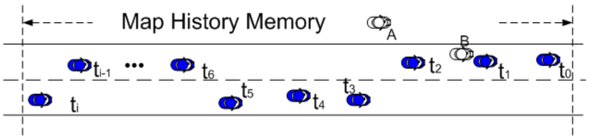

Figure 2: ***Map history examples***

5. SIMULATION RESULTS

We developed a microscopic traffic simulator based on a Java-based microscopic transport simulator from the Dresden University of Technology [4], which features a realistic traffic model. We simulated a 3000 meter highway. We can investigate the number of compromised vehicles to be detected and the time to find these compromised vehicles. The total road length is 3 Km with 2 lanes in 2 directions. The cell radius is 100 meters, traffic arrival rate is 1800 vehicles/hour, mean velocity is 33.3 m/s, and transmission radius is 100 meters. We studied the time to detect 20 compromised vehicles with 60%, 80% and 90% of the total vehicles being compromised. Compromised vehicles are randomly distributed in the system. When there are fewer than 16 compromised vehicles, the time required to detect them does not change with their percentage of the traffic. If there are more than 16 compromised vehicles, the lower the percentage is, the longer it takes to find them because they are more sparsely distributed and need more hops to be detected.

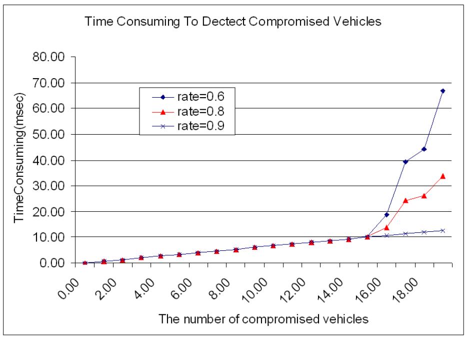

Figure 3: ***Time to detect compromised vehicles.***

6. FUTURE WORK

We are working on increasing the precision of our system to detect all the compromised vehicles and on simulating the Sybil attack and some combination of Sybil attacks and position attacks.

7. REFERENCES

[1] B. Parno and A. Perrig,Challenges in securing vehicular networks,Proceedings of HotNets-IV, 2005.

[2] John R. DouceurThe, Sybil attack, In First International Workshop on Peer-to-Peer Systems (IPTPS), March 2002.

[3] R. Moebus, A. Joos, and M. Morari, Multi-Object Adaptive Cruise Control, Proc. Hybrid Systems: Computation and Control, LNCS vol. 2623, 2003, 359-76.

[4] M. Treiber, Microsimulation of road traffic, http://www.traffic-simulation.de/, July 2005.