Towards an Optimized and Secure CASCADE for Data Aggregation in VANETs

Khaled Ibrahim and Michele C. Weigle
Old Dominion University

1) Motivation

CASCADE (*Cluster-based Accurate Syntactic Compression of Aggregated Data in VANETs*) is a data aggregation and dissemination technique for VANETs that we proposed in previous work. CASCADE is based on dividing the view in front of a vehicle into *clusters* (Figure 1). The information in each cluster is compressed and aggregated to provide more information to following vehicles. The length of a vehicle's *local view* is determined by how many clusters can fit into a single 802.11 frame.

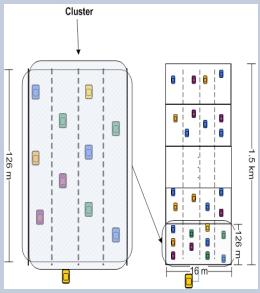

Figure 1. Vehicle's Local View

Originally, we suggested the cluster size to be 64 m long and 4 m wide, but is that the optimal cluster size? In this work, we present an analysis to determine the optimal cluster size to balance the trade-off between local view length and expected frame size. Also, we present a framework for a secure CASCADE by employing received signal strength and laser rangefinders for position verification.

2) Determining Optimal Cluster Size

In order to find the optimal cluster size that will maximize the local view length and at the same time minimize the aggregated frame size, we analyzed the relationship between the cluster size and both the local view length and the aggregated frame size. In our analysis we considered four different cluster lengths (62m, 126m, 254m, and 510m) and three different cluster widths (1 lane, 2 lanes, and 4 lanes). We found that the cluster size that maximizes the local view and minimizes the aggregated frame size is 126m long and 4 lanes wide as shown in Figures 2 and 3.

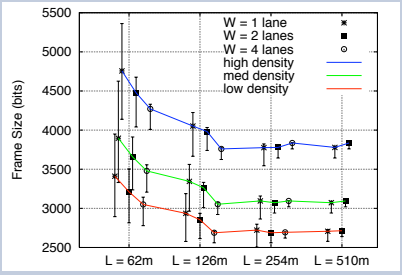

Figure 2. Minimum, Maximum and Expected Aggregated Frame Sizes as Cluster Dimensions and Traffic Density Change

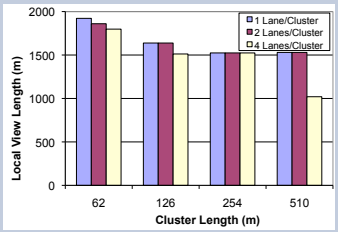

Figure 3. Local View Length as Cluster Dimensions Change

3) Position Verification in CASCADE

In CASCADE, each vehicle is responsible for reporting its information (location, speed, etc.). This may lead to several attacks, which we classify into four categories according to the false information source:

- **Unsynchronized Trace** – attacker reports position information from recorded trace, but the positions are *outside* the nominal transmission range from a potential receiver.
- **Synchronized Trace** – attacker reports position information from recorded trace, but positions are *within* the nominal transmission range of a potential receiver.
- **Primary Frame Replay** – attacker replays position information from recently received primary frames from other vehicles so that there will be a vehicle in the claimed position.
- **Malfunctioning GPS** – GPS device reports incorrect positions due to malfunction (*not an intentional attack*).

4) Defense Techniques

Detection Module

The detection module verifies that the location claimed in a received primary frame is consistent with the estimated location of the sending vehicle. This consistency check is performed on two levels:

1. using the signal strength (RSSI)
2. using the laser rangefinder, if the first check fails

Quarantine Module

The quarantine module function differs according to the vehicle's role:

- *vehicle detecting attacker* – form and broadcast a quarantine proposal
- *vehicle receiving quarantine proposal* – if the received proposal is regarding a suspected vehicle, form and broadcast a quarantine request
- *suspected vehicle receiving quarantine request* – if the count of received quarantine requests exceeds the threshold, suspend sending CASCADE reports for a certain time period

Figure 4 shows the average time before first quarantine for the different categories of attacks with different rates of CASCADE deployment.

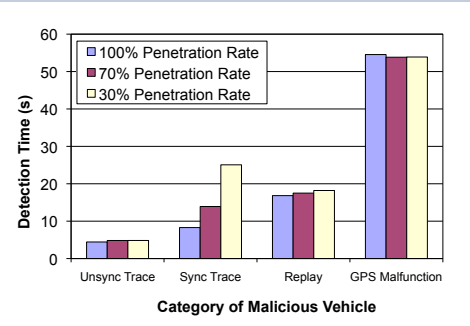

Figure 4. Effect of the Penetration Rate on The Average Time Before First Quarantine

Khaled Ibrahim and Michele C. Weigle { *ibrah_k, mweigle*} @cs.odu.edu *http://www.cs.odu.edu/vanet/*
Department of Computer Science, Old Dominion University, Norfolk, VA

ACM VANET, San Francisco, CA, September 2008