Towards an Optimized and Secure CASCADE for Data Aggregation in VANETs

Khaled Ibrahim and Michele C. Weigle
Department of Computer Science,Old Dominion University
Norfolk, VA 23529-0162, USA
{ibrah_k, mweigle}@cs.odu.edu

ABSTRACT

We present an analysis of and security extensions to the CASCADE (Cluster-based Accurate Syntactic Compression of Aggregated Data in VANETs) data aggregation technique. CASCADE organizes known vehicles into clusters, the size of which determines both the frame size used to distribute aggregated data and the distance ahead that vehicles are aware of (*local view*). We determine the optimal cluster size to balance the trade-off between local view length and expected frame size. The original CASCADE description does not consider security issues, so we present our framework for a secure CASCADE by employing received signal strength and laser rangefinders for position verification.

Categories and Subject Descriptors

C.2.0 [**Computer-Communication Networks**]: General; E.4 [**Coding and Information Theory**]: Data compaction and compression

General Terms

Algorithms, Design, Security

Keywords

Aggregation, Data Compaction, VANETs, Security

1. OVERVIEW OF CASCADE

CASCADE [1,2] aims to provide vehicles with an accurate view of traffic conditions ahead. Each vehicle participating in CASCADE broadcasts a primary frame that contains its position information (including location, speed, acceleration, and heading) every 300-400 ms. A receiving vehicle extracts the information from the received primary frames and use to form and updates its local view. A vehicle's local view comprises the vehicles described by received primary frames. The length of the local view is determined based on certain parameters used in the aggregation phase, as all the aggregated local view information must fit in a single frame (2312 bytes for IEEE 802.11). As the vehicles's transmission range is limited to 300 m, primary frame re-broadcast is need to send it further.

Every 4 sec, each vehicle aggregates, compresses and broadcasts the information in its local view. The local view is divided into fixed-size clusters. The originally suggested cluster size was 4 m x 62 m, assuming a 4 m lane width, which resulted in local view with length 1.9 km. The aggregating vehicle compresses each vehicle's information in the local view by replacing its absolute attribute values with values relative to its containing cluster center. Then the vehicles' compressed data is concatenated to form a frame containing all the local view information and is broadcasted.

VANET'08, September 15, 2008, San Francisco, California, USA.
ACM 978-1-60558-191-0/08/09.

2. DETERMINING OPTIMAL CLUSTER SIZE

In CASCADE, driver information about the traffic ahead has two sources. The first is the individual vehicle data that has been collected locally. This is limited by the local view length, so it is better to have longer local view. The second source is the aggregated frame that contains the other vehicles' local views in a compact format and is used to build the vehicle's extended view. As the local view length increases, the extended view grows quickly using few aggregated frames.

The aggregated frame is an important component in the CASCADE system, as it represents the building block for the vehicles' extended view. Based on the CASCADE design, the size of the aggregated frame is limited to the maximum IEEE 802.11 frame size of 2312 bytes. Even so, it is still better to minimize the size of the aggregated frame to minimize the bandwidth consumption and allow more vehicular applications to share the bandwidth with CASCADE.

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 (62 m, 126 m, 254 m, and 510 m) 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 126 m long and 4 lanes wide. More details can be found in our technical report [3].

3. POSITION VERIFICATION IN CASCADE

In CASCADE, each vehicle periodically broadcasts a primary frame that contains its information. As vehicles are responsible for reporting their own information, malicious vehicles have a chance to attack by reporting false information. These attacks can be classified into four categories according to the false information source:

- *Unsynchronized Trace:* The attacker could record a

trace of position information during a previous trip on the same road and then substitute these recorded positions for the vehicle's actual current GPS coordinates. An unsynchronized trace is one where the positions being sent to CASCADE are outside the nominal transmission range from a potential receiver.

- *Synchronized Trace:* This attack is similar to the unsynchronized trace, but the claimed position is within the nominal transmission range of a potential receiver.
- *Primary Frame Replay:* The attacker could record the position information from recently received primary frames from other vehicles and then substitute these positions for its actual GPS coordinates. The difference between this attack and the previous two is that the attacker will be sure of having a vehicle in the claimed position which will harden the detection.
- *Malfunctioning GPS:* If the GPS device is malfunctioning, it will not be able to translate the received signal into the correct coordinates and will report incorrect location coordinates to CASCADE.

The proposed defense technique requires each vehicle to be equipped with a GPS receiver, a communications device using DSRC [4], a scanning laser rangefinder, and the CASCADE application. The defense technique consists of two modules: a detection module and a quarantine module.

The detection module verifies that the location claimed in a received primary frame is consistent with the estimated location of the sending vehicle. The consistency check is performed in two levels: first using the signal strength (RSSI), and then using the laser rangefinder, if needed. The first level consistency check is executed by each vehicle in the system when it receives a primary frame. In this check, the location claimed by the sending vehicle is extracted from the received primary frame and compared with the estimated location using the RSSI technique. If they match, the primary frame passes to the CASCADE application for normal processing. Otherwise, the second level consistency check is executed only by vehicles neighboring the claimed location. During this check, the neighboring vehicles will try to detect the sending vehicle using the laser rangefinder. If there is a vehicle existing in the claimed location and this location is not claimed by any other vehicle in the local view, the primary frame is passed to CASCADE for normal processing. Otherwise, the check is considered to be failed, and the quarantine module is called.

The quarantine module function differs according to the vehicle's role. For example, the quarantine module in the vehicle that first detects a malicious vehicle is responsible for forming a quarantine proposal and broadcasting it. While the quarantine module in a vehicle receiving a quarantine proposal is responsible for checking if this quarantine proposal is regarding one of the suspect vehicles. If so, it will form a quarantine request and broadcast it. Otherwise, it will discard the received quarantine proposal. When the quarantine module in the suspected vehicle receives a quarantine request, it accumulates them until their count exceeds a specific threshold. Then it forces the sending module in CASCADE to stop sending any data for a specific time period. The suspect vehicle has no control on its quarantine module because it exists with the CASCADE application in a tamper-proof device, and any tampering with it will force the CASCADE application to stop functioning and the vehicle will not be able to send any data.

4. EVALUATION

We evaluated our security extensions for CASCADE using ASH (Application-aware SWANS with Highway mobility) [5], which is an extension of the SWANS network simulator [6]. We found that the proposed technique is able to detect any malicious vehicle in less than one minute under different penetration rates. Also, the technique had a false positive rate under 5%. More details are found in our technical report [3].

5. CONCLUSION AND FUTURE WORK

We have presented an analysis of and security extensions to the CASCADE (Cluster-based Accurate Syntactic Compression of Aggregated Data in VANETs) data aggregation technique. In our analysis, we determined that a cluster size 16 m wide and 126 m long would provide the best trade-off between frame size and local view length. To improve the security in CASCADE, we have used received signal strength (RSSI) and laser rangefinders for position verification. Our defense techniques can quickly detect false inputs given to the system and quarantine those responsible vehicles with very low rates of false positives.

In future work, we plan to incorporate the aggregated frames data into an additional consistency check to reduce the false positives rate. We also plan to take advantage of vehicles traveling in the opposite direction for position verification.

6. ACKNOWLEDGMENTS

This work was supported by the National Science Foundation under Grant CNS-0721586.

7. REFERENCES

[1] K. Ibrahim and M. C. Weigle, "Accurate data aggregation for VANETs (poster)," in *Proceedings of the ACM International Workshop on Vehicular Ad Hoc Networks (VANET)*, Montreal, Canada, Sep. 2007, pp. 71–72.

[2] ——, "CASCADE: Cluster-based accurate syntactic compression of aggregated data in VANETs," in submission, available at http://www.cs.odu.edu/vanet/papers/ibrahim-cascade-submitted08.pdf, Mar. 2008.

[3] ——, "Towards an optimized and secure cascade for data aggregation in VANETs," Technical Report, available at http://www.cs.odu.edu/vanet/papers/ibrahim-TR-2008.pdf, 2008.

[4] ASTM E2213-03, "Standard Specification for Telecommunications and Information Exchange Between Road-side and Vehicle Systems - 5GHz Band Dedicated Short-Range Communications (DSRC) Medium Access Control (MAC) and Physical Layer (PHY) Specifications," ASTM International, Jul. 2003.

[5] K. Ibrahim and M. C. Weigle, "ASH: Application-aware SWANS with highway mobility," in *Proceedings of IEEE INFOCOM Workshop on MObile Networking for Vehicular Environments (MOVE)*, Apr. 2008.

[6] "JiST/SWANS," http://jist.ece.cornell.edu, 2004.