Secure Data Aggregation in Vehicular-Adhoc Networks: A Survey
Sagarika Mohantya\textsuperscript{a}, Debasish Jena\textsuperscript{b}
\textsuperscript{a,b}International Institute of Information Technology, Bhubaneswar, Odisha, India

Abstract

Vehicular ad hoc networks (VANETs) are an upcoming technology that is gaining momentum in recent years. That may be the reason that the network attracts more and more attention from both industry and academia. Due to the limited bandwidth of wireless communication medium, scalability is a major problem. Data aggregation is a solution to this. The goal of data aggregation is to combine the messages and disseminate this in larger region. While doing aggregation integrity of the information can not be easily verified and attacks may be possible. Hence aggregation must be secure. Although there are several surveys covering VANETs, they do not concentrate on security issues specifically on data aggregation. In this paper, we discuss and analyse various data aggregation techniques and their solutions.

1. Introduction

In recent years, with the advancement in network technologies and wireless communications vehicular ad-hoc network (VANET) is becoming a reality. The main goal of VANET is to provide safety and traffic information to its passengers, but due to the mobility of people and wide use of internet, now the aim is to provide commercial and infotainment information to its drivers and passengers. In the USA, the Dedicated Short Range Communications (DSRC) [1] standard is being developed to support vehicular communications while the same is being done in Europe by the Car2Car Communication Consortium [2]. Vehicular ad-hoc network (VANET), is a special form of mobile adhoc network(MANET) in which vehicles act as mobile nodes that aims to provide communications among nearby vehicles also known as inter vehicular communications(V2V or IVC) and between vehicles and nearby Roadside units or RSUs, referred to as vehicle to infrastructure communications (V2I or RVC). Besides this, there is hybrid communication including V2V and V2I [3].

E-mail address: sagarikam_23@yahoo.com\textsuperscript{a},debasish@iiit-bh.ac.in\textsuperscript{b}
Vehicles equip with devices called on-board unit (OBU) that can communicate with other vehicles using dedicated short range communication (DSRC). OBUs communicate with other OBUs or RSUs. Communication is done between roadside units either through wired or wireless networks to spread the messages to larger regions. The Trust authority (TA) is a trusted party responsible for authenticating vehicles and identifying a malicious identity if any dispute happens. The application server (Traffic Monitoring Center) is responsible for making further analysis and giving feedback to the RSUs after collecting the traffic related information. Some vehicles are equipped with a tamper proof device that carries certain secure operations. Applications are categorized as safety, transport efficiency and information/entertainment applications [4].

Research activities are going on in vehicular networks with the help of Government and automobile manufacturers. Still, many open research areas are available from which security is the most challenging part. The remainder of the paper is organized as follows. Section 2 describes secure data aggregation. Possible attacks or adversaries are discussed in section 3. Section 4 gives a detailed survey on the techniques of secure data aggregation schemes followed by concluding remarks in section 5.

2. Secure data aggregation

Secure data aggregation is a topic well studied in sensor networks. However, due to the mobility nature of vehicular adhoc networks and the fact that nodes move following specific paths, the reuse of wireless sensor network secure data aggregation (SDA) mechanism is not possible in VANET [5]. Data aggregation has been proposed in VANETs to solve the bandwidth utilization problem. Aggregation techniques can be classified as syntactic or semantic (Picconi et al.). Syntactic aggregation compress or encode the data from multiple vehicles in order to fit the data in a unique record or frame, e.g. an application that extracts a subset of each individual record and adds it to a single record is reducing the original information. Semantic aggregation means that data from individual vehicle is summarized, e.g. an application that instead of sending the location of each vehicle, only reports the number of vehicles in a given area. Besides this, some authors have done cryptographic aggregation on the signatures and certificates to reduce bandwidth. However, aggregation aggravates the security problem.

3. Possible attacks or adversaries

The major threat to VANET aggregation mechanism is false information dissemination [6]. Focusing only on the aggregation process, the following attacks may be possible [7, 8]:

![Fig 1. Vanet structure](image-url)
Forging of atomic reports: An attacker station may forge its own message and thus influence further aggregation.

Forging of aggregates: An attacker may directly create aggregates with arbitrary data and inject them into the network.

Suppression of aggregates: Because of the larger information value of aggregates, attacker stations may suppress aggregates, resulting in biased information dissemination.

Though suppression of aggregates and forging of atomic reports influence aggregation schemes, yet the most effective attack is the creation of an entirely fictitious aggregate, as such aggregates can carry information about arbitrary dimensions and values.

4. Techniques for secure data aggregation

Wischhof et al. [9,10] outline a (non-hierarchical) aggregation scheme, combining all the known information on each fixed-length road segment to one average value. Upon reception, a node considers an aggregate “better” if it has a newer timestamp.

Nadeem et al. [11] present the Traffic View system based on a fixed road segmentation, which uses semantic aggregation. The goal of TrafficView is to provide the driver of a vehicle with information about traffic and road conditions. The essence of the system is to gather and disseminate traffic information between the vehicles on the road. They present two techniques for aggregation: ratio-based and cost-based. In [12], they applied data aggregation based on the semantics of data using ratio based mechanism. They focus on data push communication model i.e. exchange information on a set of vehicles on a regular basis by flooding and disseminating.

In Caliskan et al. [13] work aggregation is performed over a hierarchical quad-tree. In their work, vehicles use periodic beacons to disseminate information about free parking slot.

The main focus of Raya et al. [6] paper is message aggregation and group communication. The group leader/cluster head is chosen dynamically as the one closet to the center of the cell. The group leader is in charge of aggregating and disseminating data. In their view, the major threat that can target specifically VANET aggregation mechanisms is that of false information dissemination. To crosscheck this, they have sought to combine the signatures generated by a group of vehicles reporting the same event. They proposed three types of combined signatures: concatenated signature, onion signature and hybrid signature. These schemes are in the realm of asymmetric cryptography which is expensive. That’s why they have designed a mechanism called overlapping groups which is based on symmetric cryptography. They have described another scheme called dynamic group key creation which is based on symmetric cryptography without losing the non-repudiation property of digital signatures.

In Eichler et al. [14] messages contain the node ID, message ID, and a street ID. Messages are aggregated if they have the same message and street ID. Aggregation depends on the timeliness of the message and the variability of the event.

Picconi et al. [15] propose a solution for validating aggregated data by taking speed and location information which is common to most vehicular applications. They focus on spoofing and bogus information attacks. Their solution is based on syntactic aggregation, though it is also applicable to certain cases of semantic aggregation. Their scheme is based on PKI based authentication and assume that every car has a tamper proof service that carries certain secure operations like signing, time stamping and random number generation. The main idea of their solution is to challenge the aggregator to provide a proof that can be used to probabilistically validate the aggregated record. An aggregated record is created by combining and compressing information contained inside several individual records. To validate the aggregated record the aggregator is asked to provide a randomly chosen original signed record.

Saleet et al. [16] present a location query protocol that aggregates data in VANETs. The protocol divides
the road into segments, and the node closest to the center of the segment plays the server role. Each vehicle periodically broadcasts its information, and the server node is responsible for storing this information, aggregating it, and then broadcasting it.

Lochert et al. [17] introduced a data aggregation mechanism for disseminating data in VANET applications. It is based on probabilistic data representation Flajolet-Martin sketch, which they extend to yield a soft-state variant of FM sketches in which previously inserted elements die after their TTL (Time to Live) has expired, unless they are refreshed by newer observation. In their scheme, multiple aggregates for the same area are merged, yielding a new one incorporating all the information in those aggregates. It also allows lower-level aggregates to be integrated into an already existing higher-level aggregate at any time.

In Catch-Up Yu et al. [18] developed a method that guarantees that reports are aggregated. The basic idea is to insert a delay before forwarding a report to the next hop. That's why the solution is unsuitable for safety messaging applications but perfectly valid for general traffic information. In their scheme, they divide the road into segments and time into frames, the intersection is called event frame. Reports are aggregated when they are from the same road section and within the same time frame. The objective is to generate an overview report by performing functions such as MAX, MIN, AVG etc. They design a model to define the benefits of different delay-control policies and then establish a decision tree to help vehicle choose an optimal policy from the perspective of long term rewards.

Zhang et al. [19] introduced an efficient identity based cryptography with batch signature verification scheme for communications between vehicles and RSUs (V2I). Here, an RSU can aggregate multiple signatures as one signature and perform the batch verification on the aggregate signature such that the total verification time can be reduced. The proposed scheme can achieve conditional privacy preservation due to the use of pseudo-identities and thus certificates are not needed and transmission overhead can be significantly reduced.

CASCADE, Ibrahim and Weigle [20] is a cluster-based accurate syntactic aggregation scheme. It has four major components, local view, extended view, data security and data dissemination which provide an efficient solution for the problem of scalability for VANET applications. Each vehicle periodically broadcasts its vehicular data which is called a primary record. The primary records representing vehicles ahead of the current vehicle comprise the local view and it is divided into clusters. The primary record is signed by the original vehicle using ECDSA. The certificate included in the frame contains the public key of the vehicle signed by the CA that’s why an attacker can be easily traced and replay attacks are nullified by the presence of the timestamp inside the signed primary record. Each vehicle periodically compresses and aggregates the primary records in its local view into an aggregated record and broadcast it to neighboring vehicles which provide information about vehicles beyond the local view, resulting in an extended view.

Zhu et al. [21] propose an aggregated emergency message authentication (AEMA) scheme to efficiently validate the emergency messages in VANETs. The basic idea is that during the emergency message data forwarding process, a vehicle can hold multiple messages, which can be aggregated into a single one before the vehicle transmit it in the network. The proposed AEMA scheme takes advantage of syntactic and cryptographic aggregation technique to reduce the transmission cost and adopt batch verification technique to reduce the computation cost. In their study, they aggregate the signatures and certificates and apply batch verification technique to verify this. They mainly consider the false data injection attack or collusion attack.

Zhang et al. [22] introduced a RSU-aided message authentication scheme named RAISE, which makes RSU responsible for message authentication and hash aggregation. Then the vehicle has to decide whether the result returned from the RSU is authentic or not. It adopts k-anonymity technique to preserve user privacy. They further proposed a supplementary scheme named COMET which will helpful in the absence of a RSU. The scheme achieves conditional privacy preservation due to the use of pseudo-identities and replay attack is prevented by the use of timestamping.

The main focus of Scheuermann et al. [23] is on the minimum aggregation requirements for scalable
dissemination applications, as the distribution of dynamic information from many sources to many destinations is a key challenge for VANET applications. They prove that any suitable aggregation scheme must reduce the bandwidth at which information about an area at distance \( d \) is provided to the cars asymptotically faster than \( (1/d^2) \). The sources of information, i.e. where aggregation and dissemination data comes from is called measurement points and goes to destinations (i.e., set of vehicles that are interested in information from a measurement point).

Dietzel et al. [24, 25] propose an information aggregation framework which is completely structure-free. Data aggregation is mostly used for fixed road segment, hierarchy of grids or group of nodes. They argue against such conditions as it contradicts the real situation. They explain all aggregation system has three main components: Decision (decide if two pieces of information are similar enough to be aggregated), Fusion (aggregation) and Dissemination, i.e, transmit the aggregated data into the network. The authors apply a fuzzy reasoning system to make aggregation decisions.

Wasef et al. [26] proposed an aggregate signatures and certificates (ASIC) verification scheme enabling each vehicle to simultaneously verify the signatures and certificates of the senders. Since each vehicle could receive a large number of messages from the neighboring vehicles, one of the inevitable VANET challenges is the ability for each vehicle to verify a large number of messages in a timely manner. ASIC significantly increases the vehicle capability to verify a large number of signatures and certificates in a timely manner.

Tsai et al. [3] proposed an aggregating data dissemination algorithm (ADD) in vehicular ad hoc networks to decrease the data dissemination cost. Their ADD algorithm is suitable for any scale network based on a hierarchical grid structure. In each level cell, a roadside unit is selected as the center unit that is responsible for collecting, aggregating and disseminating data to the center unit of higher level. Their ADD algorithm can offer the aggregated data of different enquiry range size for various enquiry demands. According to the algorithm the traffic information is aggregated and kept in the periphery of region and users can get the detailed data for a small area with higher accuracy and can get summary data for a large area with lower accuracy.

Viejo et al. [27] presented a scheme for trustworthy vehicle-generated announcements messages on VANETs that relies on a priori measures against internal attackers (vehicles in the VANET sending fake messages). They have used multisignatures over a Gap Diffie-Hellman group to aggregate announcements and thus reduced communication overhead. Their proposal is suitable for deployment in both deterministic (e.g. a highway) and non-deterministic (e.g.a city) scenarios. Regarding privacy, the proposed system uses a mechanism to provide unlinkability to the vehicles. Anonymity is achieved by using pseudonyms.

Dietzel et al. [7] introduce a generic model for aggregation that is applicable to wide range of applications. The structure is like this:

\[
A = \{ (\{a_1, b_1\}, \ldots, (a_n, b_n)) \mid (v_1, \ldots, v_p) \mid (m_1, \ldots, m_q) \}
\]

index dimensions    values        meta-information

The index dimensions indicate the area and time about which an aggregate contains information. The values are the actual information and the meta-information contains additional information used to verify aggregate’s correctness. In their security mechanism, they strategically chose a subset of all atomic reports to generate an aggregate report. They have identified three types of attacks: forging of atomic reports, forging of aggregates and suppression of aggregates of which the second one is the most significant one as the creation of entirely fictitious aggregates and the attacker pretends this fictitious aggregate is backed up by several other vehicles so the trustworthiness is high.

Lochert et al. [28] introduce the concept of soft-state sketches for probabilistic hierarchical data aggregation derived from Flajolet–Martin sketches (FM sketches). Locally stored sketches are periodically broadcasted to the vehicle’s one-hop neighbors, which upon reception merges them with its own. Previously inserted elements die out after their TTL has expired, unless they are refreshed by a newer observation.

Han et al. [29] present a secure probabilistic data aggregation scheme (SAS) for vehicular sensing networks, which is based on Flajolet-Martin sketch and a series of sketch proof techniques. They also discussed
the tradeoff between the bandwidth efficiency and the estimation accuracy.

Wu et al. [30] in their novel RSU-based message authentication scheme for VANET also use hash aggregation in intra RSU ranges.

The idea of Qin et al. [31] is to aggregate a large number of signatures as a single one without degrading security, hence much less bandwidth is consumed and storage capacity is saved. In their scheme, cryptographic witnesses of safety-related traffic messages are compressed so that they can be stored for a long period for liability investigation.

Molina et al. [8] address the security problem in VANETs that determines whether road traffic information available to a driver is trustful or not. They defined three geographic zones with respect to the reported event: Danger Zone, Uncertainty Zone and Security Zone. The main idea is that vehicles who agree with the generated information can sign the packet. Second, in order to avoid that the packet grow indefinitely, signatures are generated according to a granularity defined depending on the type of road and making it impossible for an attacker any packet modification. The aim is to select signatures that are evenly distributed throughout the aggregate area i.e, packets from borders and additional reports from other areas to provide reliability.

Tseng et al. [32] propose a secure aggregated message authentication (SAMA) scheme in certificateless public key settings to validate emergency messages in VANETS. In their scheme, the vehicle makes use of the partial private key generated by the KGC and the private key chosen by it to generate the signatures on the emergency messages. They claimed that compared to Zhu et al.’s scheme their scheme achieves more efficient authentication on emergency messages. They used Petrinet in the security analysis and showed that their proposed scheme can successfully defend forgery attacks and ensure the conditional privacy preservation and traceability of vehicles.

Dietzel et al. [33, 34] introduced a modeling approach for VANET aggregation to achieve comparability as it is essential to properly measure accuracy, performance and efficiency. Their model promises to reduce bandwidth requirements and enable scalability. The modeling approach consists of three models: the architecture model, the information flow model and the aggregation state graph model. They apply each modeling approach to some of the existing aggregation schemes and discuss its strengths and weaknesses that can be used for designing a more generic aggregation scheme.

5. Conclusion

In VANETS, vehicles produce an enormous amount of data. Each vehicle transmits this message to the approaching vehicles (e.g. Traffic jam). Now, instead of sending many similar messages which would congest the medium, summarized or aggregated information can be sent which will solve the purpose. Thus the need of aggregation i.e. instead of disseminating individual messages only the aggregated information is transmitted.

In this paper, we have discussed the major schemes available so far in data aggregation. However, as aggregation aggravates the security problem, different types of attacks may be possible. Most of the schemes agreed on three types of attacks i.e., forging of atomic reports, forging of aggregates and suppression of aggregates. From these, forging of aggregates is the more serious one as the creation of an entirely fictitious aggregates. Most of the authors use syntactic and cryptographic aggregation schemes to reduce bandwidth and achieves scalability. Some of them use semantic aggregation. To avoid replay attacks, timestamps are used.

Table 1 Taxonomy of secure data aggregation schemes:

| Authors | Aggregation Type | Aggregation structure/data structure | Aggregator | Fixed/dynamic areas | Application | Secure against Attacks |
|---------|-----------------|-------------------------------------|------------|---------------------|-------------|------------------------|

---
| Authors          | Approach                  | Technique               | V(cluster head) | F                     | Attack                          |
|------------------|---------------------------|-------------------------|-----------------|------------------------|---------------------------------|
| Raya et al.      | Semantic                  | Cluster-based           | V               | D                      | app. specific                   |
| Piccon et al.    | Synactic and semantic     |                         |                 |                        | Spoofing & bogus inf. attack    |
| Zhang et al.     | Cryptographic             |                         |                 |                        | Traffic inf.                    |
| Ibrahim et al.   | Syntactic                 | Cluster-based           | V               | F                      | All                             |
| Zhu et al.       | Syntactic & cryptographic | Cluster-based           | V               |                        | Emergency event                 |
| Scheuermann et al.| Hierarchical aggregation  | Soft-state variant of FM | V               |                        | Parking spaces                  |
| Dietzel et al.   | Semantic & cryptographic  |                         | V               | D                      | All                             |
| Lochert et al.   | semantic                  | Soft-state variant of FM | V               | D                      | 3 types of attacks discussed in sec.3 |
| Qin et al.       | Cryptographic             |                         | V               |                        | Safety messages                 |
| Tseng et al.     | Syntactic & cryptographic |                         | V               |                        | Existential forgery attack      |

References

[1] Dedicated Short Range Communications (DSRC). [Online]. Available: http://grouper.ieee.org/lgroups/scc32/dsrc/index.html
[2] Car 2 Car Communication Consortium. [Online]. Available: http://www.car-2-car.org/
[3] Wen TH., Tzung-Shi C., Sheng-Kai L., 2009. Dissemination of Data Aggregation in Vehicular Ad Hoc Networks, 10th International Symposium on Pervasive Systems, Algorithms, and Networks, IEEE, p. 625-630.
[4] Hartenstein H., Laberteaux KP., 2008. A Tutorial Survey on Vehicular Adhoc Networks. IEEE Communications Magazine, p. 164-171.
[5] Rivas AD., Barcelo’-Ordinas Jose M., Zapata MG., Morillo-Pozo Julia’n D., 2011. Security on VANETs: Privacy, misbehaving nodes, false information and secure data aggregation, Journal of Network and Computer Applications, ELSEVIER, 34 (2011) 1942–1955.
[6] Raya M., Aziz A., Hubaux J-P., 2006. Efficient secure aggregation in vanets, Proceedings of the 3rd international workshop on vehicular ad hoc networks, VANET, New York, NY, USA, p. 67–75.
[7] Dietzel S., Schoch E., Konigs B., Weber M., Karl F., 2010. Resilient secure aggregation for vehicular networks, IEEE Network 2010;24(1): p. 26–31.
[8] Molina-Gil J., Caballero-Gil P., Caballero-Gil C., 2010. Data Aggregation for Information Authentication in VANETs, Information Assurance and Security Letters, 1, p. 47-52.
[9] Wischhof L., Ebner A., Rohling H., Lott M., Halfmann R., 2003. SOTIS – a self-organizing traffic information system, Proceedings of the 57th IEEE Semi Annual Vehicular Technology Conference, p. 2442–2446.
[10] Wischhof L., Ebner A., Rohling H., 2005. Information dissemination in self-organizing intervehicle networks, IEEE Transactions on Intelligent Transportation Systems, 6(1), p. 90–101.
[11] Nadeem T., Dashtinezhad S., Liao C., Iftode L., 2004. Trafficview: traffic data dissemination using car-to-car communication, ACM SIGMOBILE Mobile Computing and Communications Review, 8(3), p. 6-19.
[12] Nadeem T., Shankar P., Iftode L., 2006. A Comparative Study of Data Dissemination Models for VANETs, University of Maryland Technical Report, CS-TR-4810, p. 2006.
[13] Caliskan M., Graupner D., Mauve M., 2006. Decentralized Discovery of Free Parking Places, Proceedings of the 3rd international workshop on Vehicular ad hoc networks, VANET, New York, NY, USA, p. 30–39.
[14] Eichler S., Merkle C., Strassberger M., 2006. Data aggregation system for distributing inter-vehicle warning messages, Proceedings of the 31st IEEE Conf. on Local Computer Networks, IEEE Computer Society, November 2006, p.543-544.

[15] Picconi F., Ravi N., Gruteser M., Iftode L., 2006. Probabilistic validation of aggregated data in vehicular ad-hoc networks, Proceedings of the 3rd international workshop on vehicular ad hoc networks, VANET, New York, NY, USA, p.76-85.

[16] Saleet H., Basir O., 2007. Location-based message aggregation in vehicular ad hoc networks, Proceedings of IEEE AutoNet, Washington DC, USA, p.1-7.

[17] Lochert C., Scheuermann B., Mauve M., 2007. Probabilistic aggregation for data dissemination in VANETs, Proceedings of the Fourth ACM International Workshop on Vehicular Ad Hoc Networks, VANET; 07:p.1-8.

[18] Yu B., Gong J., Xu CZ., 2008. Catch-up: a data aggregation scheme for vanets, Proceedings of the 5th ACM international workshop on Vehicular Inter-networking, VANET, New York, NY, USA, p.49-57.

[19] Zhang C., Lu R., Lin X., Ho PH., Shen X., 2008. An Efficient Identity based Batch Verification scheme for Vehicular Sensor Networks, Proceedings of IEEE INFOCOM, Phoenix, AZ, p.246 - 250.

[20] Ibrahim K., Weigle MC., 2008. CASCADE: Cluster-Based Accurate Syntactic Compression of Aggregated Data in VANETs, IEEE GLOBECOM Workshops, p.1-10.

[21] Zhu H., Lin X., Lu R., Ho PH., Sherman XS., 2008. AEMA: An Aggregated Emergency Message Authentication Scheme for Enhancing the Security of Vehicular Ad Hoc Networks, Proceedings of IEEE ICC, p.1436-1440.

[22] Zhang C., Lin X., Lu R., Ho PH., Shen X., 2008. An Efficient Message Authentication scheme for Vehicular Communications, IEEE Transactions on Vehicular Technology 57(6).

[23] Scheuermann B., Lochert C., Rybicki J., Mauve M., 2009. A fundamental scalability criterion for data aggregation in vanets, ACM Mobile Computing.

[24] Dietzel S., Schoch E., Bako B., Kargl F., 2009. A Structure-free Aggregation Framework for Vehicular Ad Hoc Networks, Proceedings of the 6th International Workshop on Intelligent Transportation, Hamburg, Germany, p.61-66.

[25] Dietzel S., Bako B., Schoch E., Kargl F., 2009. A fuzzy logic based approach for structure-free aggregation in vehicular ad-hoc networks, Proceedings of the sixth ACM international workshop on Vehicular Internetworking, VANET, New York, NY, USA, p.79-88.

[26] Wasef A., Shen X., ASIC: Aggregate signatures and certificates verification scheme for vehicular networks. Available at: http://www.engine.lib.uwaterloo.ca.

[27] Viejo A., Sebe F., Domingo-Ferrer J., 2009. Aggregation of Trustworthy Announcement Messages in Vehicular Ad Hoc Networks, IEEE 69th Vehicular Technology Conference, VTC 2009.

[28] Lochert C., Scheuermann B., Mauve M., 2010. A probabilistic method for cooperative hierarchical aggregation of data in vanets, AdHoc Networks, Journal of Vehicular Networks, 8(5), p.518-30.

[29] Qi H., Suguo D., Dandan R., Haojin Z., 2010. SAS: A Secure Data Aggregation Scheme in Vehicular Sensing Networks, Proceedings of IEEE ICC.

[30] Wu HT., Wei-Shuo L., Tung-Shih S., Wen-Shyong H., 2010. A Novel RSU-based Message Authentication Scheme for VANET, Fifth International Conference on Systems and Networks Communications, IEEE, p.111-116.

[31] Qin B., Wu Q., Zhang L., Domingo-Ferrer J., 2010. Secure Compression of Privacy-Preserving Witnesses in Vehicular Ad Hoc Networks, First International Workshop on Vehicular Communications and Networking, IEEE, p.541-547.

[32] Tseng HR., Jan RH., Yang W., Jou E., 2011. A Secure Aggregated message authentication scheme for Vehicular Ad-Hoc Networks, 18th World congress on Intelligent Transportation systems.

[33] Dietzel S., Kargl F., Heijenk G., Schaub F., 2010. On the potential of generic modeling for VANET data aggregation protocols, Proceedings of the 2nd IEEE Vehicular Networking Conference, IEEE, p.78-85.

[34] Dietzel S., Kargl F., Heijenk G., 2011. Modeling In-Network Aggregation in VANETs, IEEE Communications Magazine, 49(11).