REST-Net: A dynamic rule-based IDS for VANETs

Andreas Tomandl, Karl-Peter Fuchs, Hannes Federrath
University of Hamburg
Germany

***Abstract*—In this paper we introduce REST-Net, a novel Intrusion Detection System for Vehicular Ad Hoc Networks (VANETs) that helps to mitigate the integrity and authenticity challenges introduced by VANETs. At its core, REST-Net uses a dynamic detection engine that monitors and analyzes data sent in VANETs through plausibility checks to detect attacks in form of fake *Messages*. Unlike previous solutions REST-Net offers high detection rates, adaptive warning levels to prevent interruptions of drivers and a concept for the revocation of fake *Messages* once an attacker is detected. We present the design and components of REST-Net, discuss its security properties and provide results from an initial feasibility study with a micro-traffic simulator.**

I. Introduction

Vehicular Ad Hoc Networks (VANETs) are an upcoming technology that enables communications between vehicles via Wi-Fi based on IEEE 802.11p [1], IEEE 1609 [2] and related standards. Communications between vehicles is an important perquisite for a new generation of Advanced Driver Assistance Systems (ADAS) that are supposed to increase road safety in the future. ADAS monitor data from various sensors of a vehicle (e. g., temperature, light, distance, speed, break, acceleration and impact sensors) to warn the driver about dangerous situations or perform automatic actions (e. g., a breaking maneuver) to prevent accidents or at least minimize the consequences of accidents.

With VANETs, vehicles are no longer limited to the data provided by their own sensors: According to various architecture proposals (cf. [3], [4] and [5]) vehicles exchange so-called *Beacons*[1] and *Messages*[2]. *Beacons* are broadcast frequently (i. e., *several times per second*) by every vehicle to its neighbors and contain information such as the current location, speed and acceleration of the vehicle and thus enable ADAS to create and analyze a virtual representation of the current traffic situation. In contrast, *Messages* contain warnings about events like slick or icy roads, traffic jams, accidents or approaching emergency vehicles. Thus, *Messages* allow a wider propagation of warnings compared to *Beacons*.

Besides obvious benefits for safety, VANETs introduce new *security challenges*, especially for privacy (cf. [9]–[15]), integrity and authenticity (cf. [16] and [3]). In this work, we focus on the integrity and authenticity aspects of *Messages*. While practical solutions for the detection of fake *Beacons* exist (cf. [17]–[23] and Sect. II), only few proposals (cf. [24]–[27]) address the detection of fake *Messages*. Further, these proposals are subject to considerable limitations, as we will show in Sect. II and V.

In contrast, with **REST-Net** (*Rule-Enforced Security Technique for VANETs*), we propose a novel Intrusion Detection System (IDS) that enables ADAS to detect fake *Messages* by monitoring and analyzing *Beacon* data. REST-Net extends ideas from previous solutions and, at its core, consists of a dynamic detection engine with the following main features:

REST-Net uses **plausibility checks** to verify the validity of *Messages*. Its detection engine validates both *Beacons* broadcast before a particular *warning Message* (**pre-validation**) as well as *Beacons* sent by the initiator of the *Warning Message* after he sent the *Message* (**post-validation**). The plausibility checks are modeled as sets of **dynamic rules**. A rule might for example contain the propositions Q ("Vehicle slowed down less than $n\,\%$ in period $[t_{min},\, t_{max}]$") and P ("Vehicle was standing before t_0") to detect wether an *Emergency Electronic Brake Lights* (EEBL)-*Message* is valid or not. Both rules and propositions are **adaptive**, i. e., may contain flexible thresholds (like $n\,\%$ and t_x in the previous two examples) to assert stable detection rates in different environments (e. g., on one lane roads with low speed limit as well as on multilane highways). Further, REST-Net uses **adaptive warning levels** to keep interruptions of drivers to a minimum while still detecting most attacks and enables the **revocation of an attacker's *Messages*** after his detection.

To demonstrate the feasibility of REST-Net, we perform an initial simulation-based evaluation with a micro-traffic simulator and maps of Berlin, New York and Puebla (three cities with highly diverse road structure). The simulation results suggest that REST-Net's detection rates are feasible for practical use and outperform a previous proposal by Ruj et. al. [27] in terms of detection rate as well as true/false positives and negatives.

The rest of this paper is structured as follows. In Sect. II, we outline fundamentals and related work. After a short characterization of the attacker model in Sect. III, we introduce REST-Net, our novel IDS tailored to VANETs in Sect. IV. Finally, we present and discuss results of an initial simulation-based feasibility study of REST-Net, before we conclude in Sect. VI.

II. Fundamentals and Related Work

To solve the challenges regarding data integrity and authenticity in VANETs, **proactive** and **reactive concepts** were proposed (cf. [28] for a detailed overview).

Proactive concepts typically include a (global) Public Key Infrastructure (PKI) and tamper-proof hardware (inside vehicles) to provide message authenticity and integrity as well as non-repudiation, accountability and access control. While proactive concepts (e. g., [3] and [5]) offer an important basic level of protection, relying solely on their security can be problematic since several attack vectors exist. First of all, assuring

[1] also known as *Co-operative Awareness Messages* [6] or *Basic Safety Messages* [7]

[2] also known as *Decentralized Environmental Notification Messages* [8] or *Roadside Alerts* [7]

the integrity of a global PKI is a challenging *technical* and *organizational* problem as demonstrated by several successful attacks on the X.509 PKI infrastructure of the Internet (for the SSL/TLS protocol suite): *Technical* problems include security flaws in the protocols, implementation errors or weaknesses in the construction of the cryptographic primitives used. Two side channel attacks, the *BEAST attack* [29] and the *Lucky Thirteen attack* [30], are well known examples (cf. [31] and [30] for a comprehensive overview). Secondly, *organizational* problems arise in global PKIs since authentication must be delegated to a large number of Certification Authorities (e. g., for different countries and organizations). Recently, these problems became apparent with security incidents involving the Certification Authorities Comodo and DigiNotar [32]. Generally, it only takes a single Certification Authority to misbehave (by being hacked, tricked, bribed or legally forced) to enable an attacker to send fake messages in any part of the world. While on the Internet (for the TLS case), these attacks typically lead to financial losses only, they might result in fatal accidents for VANETs. Further, even if all Certification Authorities are trustworthy, sensor manipulation (i. e., attacks on a physical level, that can hardly be prevented) are still applicable and attacks on the (assumed) tamper-proof hardware may be feasible as well.

As a result, relying solely on proactive concepts should be avoided. To this end, **reactive concepts** in the area of VANETs were introduced. Reactive concepts try to *detect* fake information transmitted between vehicles and can be classified into *signature based detection*, *anomaly detection* and *context verification* (cf. [28] for concrete examples). *Signature based detection* systems monitor the network traffic and compare it to previously defined signatures of attacks. In contrast, *anomaly detection* systems operate with the opposite technique: Instead of defining signatures for attacks, *statistical anomalies* of *normal* communication behavior is detected. While we want to point out that both concepts (which operate on the network layer) can be used in conjunction with the application-level concept REST-Net, in our view, face considerable limitations as the definition of reasonable signatures (i. e., reasonable *normal* and *abnormal* behavior) in VANETs is very challenging based on information gathered on the network layer only.

To overcome these problems, *context verification* (the third category of reactive concepts) was introduced. The term *context verification* summarizes application-level concepts that use information provided inside VANETs (like position, time and application-specific information) as input to detect attacks. REST-Net falls into this category and extends some of the previous proposals that will be explained more detailed in the remainder of this section.

As mentioned in Sect. I, in VANETs, application-level messages can be classified into *Beacons* and *Messages*. Like [24]–[26] and [27], REST-Net addresses the detection of fake *Messages* and requires an additional scheme for the detection of fake *Beacons*, i. e., REST-Net is built atop of schemes for the protection of *Beacons* like [17]–[22], [33] and [23]. These schemes use different techniques, like signal strength analysis [21]–[23], radar-based-positioning [17], infrastructure supported positioning [18] and trusted third party concepts [19], [20] to verify the position information contained in *Beacons*. Generally, those schemes offer a high level of protection, since they rely on physical observations (like signal strength) which are difficult to fake. To this end, we chose to focus on the detection of fake *Messages* (instead of fake *Beacons*) with REST-Net. To the best of our knowledge, only [24]–[26] and [27] are concepts with (in part) similar goals.

In [24], VANET participants use a so-called *model of the VANET* that specifies sets of *allowed* and *disallowed* events to detect attacks. The basic idea is that vehicles share sensor data with neighboring vehicles. Each vehicle analyses the redundantly received data for inconsistencies. When an inconsistency is detected, a heuristic is used to find the most likely sources of the attack. While the *model of the VANET* is based on the same ideas as the *plausibility checks* and *dynamic rules* of REST-Net, [24] is a high-level concept as the authors only provide a formal description of the model (a framework) and (apart from rather general statements) do not specify how the *model of the VANET* can be populated (however, it is mentioned that the model can be based on *rules* or *statistical properties* and might be *constructed when manufacturing the vehicles* [24]).

In contrast, we suggest (and evaluate) concrete rules and our approach does not require vehicles to send data redundantly, since attacks are detected through inconsistencies in the faked data itself, i. e., inconsistencies between *Beacons* and *Messages* of the same (potentially attacking) participant.

The concept introduced in [25] determines the plausibility of a *Post Crash Notification* by analyzing the reaction of the originator of a *Message*. By comparing the movement of the vehicle through its *Beacon* information and the expected trajectory calculated by a mobility model, a deviation from a normal behavior on a crash sight can be determined. However, the concept focuses on a single type of *Message* only (*Post Crash Notifications*) and thus, its applicability to other contexts is questionable. Further, it neglects all data sent before the *Message* in question, i. e., performs post-validation only.

[26] consist of a *malicious data scheme* (MDS), a two-part certificate revocation scheme (RTC and RC^{2}RL) and a majority voting scheme (LEAVE). The MDS aims to detect false data in VANETs like the scheme proposed in this paper and works by evaluating sensory data, received *Messages* from its neighbors and a set of *evaluation rules*. However, in contrast to REST-Net, no specific *evaluation rules* are provided, i. e., (like [24]) [26] is a high-level concept.

In [27] the authors define expected actions of a vehicle after sending a *Message* (e. g., a *Message* about a traffic jam might indicate that the vehicle will change its lane or slow down). Furthermore, a scheme to verify the received position information by using the received signal strength is proposed. While this concept contains interesting ideas and detailed information about the evaluation rules, its practicability is unclear as the authors did not evaluate their findings and restrict their concept on highways (multilane roads). Furthermore, only *Beacon* data after an event is analyzed and, like in all previously mentioned concepts in this section, no adaption of warning levels is provided.

To this end, we decided to evaluate this scheme of Ruj et. al. and thus implemented it in a VANET simulator. After our evaluation, we designed a new scheme (REST-Net) that improves on most limitations of the concepts discussed in this section. We will describe REST-Net and its difference from

[27] in the following two sections and compare the detection rates of both schemes in Sect. V.

III. Attacker Model

For this work we consider two types of attackers, the *constrained attacker* and the *unbounded attacker*. Both vary in the following characteristics. The *constrained attacker* is able to fake *Messages* (e. g., because he is exploiting a security breach of the VANET hardware or software in his vehicle) and tries to gain advantage over other road users. He is a local attacker and might for example forge a *Message* of an emergency vehicle to force other users to clear the road while driving or his car might send fake traffic jam *Messages* (while parked near his house) to reduce traffic density. The *constrained attacker* is *not* able to fake different identities.

In contrast, the *unbounded attacker* is able to fake (multiple) identities including those of privileged vehicles (like police cars). He is able to perform distributed attacks, i. e., he controls several VANET participants. Further, the *unbounded attacker* may prepare attacks over a *long* period of time to gain a high level of trust. Due to its strength, reliable protection from the *unbounded attacker* is not realistic. However, creating plausible fake *Messages* which do not contradict the observations of previous *Messages* and *Beacons* is still challenging, even if the attacker controls several participants. Thus, at least some of his identities may get detected over time.

IV. REST-Net

REST-Net is an Intrusion Detection System that enables ADAS to detect fake *Messages* by monitoring and analyzing *Beacon* data. In general, Intrusion Detection Systems help to protect (distributed) computer systems from both inside attackers abusing their privileges and outsiders exploiting security vulnerabilities (cf. [34] and [35]). REST-Net falls into the category of rule-based IDS which use patterns (or rules) to define invalid actions of users and thereby detect an adversary.

In the remainder of this section, we will describe the main features of the REST-Net detection engine and outline its key differences from [27] and other related work. To this end, we start with the core component of REST-Net, the **plausibility checks** before we describe two additional components, **adaptive warning levels** and a **message revocation scheme** (cf. Fig. 1).

Plausibility checks. REST-Net extends *plausibility checks* from previous work (cf. Sect. II) in two dimensions: It uses *dynamic rules* that adapt to the current traffic situation (*adaptive plausibility checks*) and it validates both *Beacons* broadcast before *and* after a particular warning *Message*, i. e., it performs pre-validation and post-validation (*extended plausibility checks*).

Adaptive plausibility checks: Generally, both static and dynamic rules are bound to different types of events and define *invalid actions* that contradict the respective event. In our case, each type of event is equal to exactly one of the different types of *Messages* encountered in VANETs, e. g., an *Emergency Electronic Brake Lights Message* (EEBL *Message*) is broadcast automatically when a strong brake application is performed and might indicate a broke-down vehicle (cf. Tab. I for further *Message* types). A matching *invalid action* would be *continuous driving of the event source* (since the *expected action* would be a brake application obviously).

TABLE I. Selected event types from [36]

Event type	Event description
Stopped/Slow Vehicle Advisor (SVA)	Traffic jam detected
Road Hazard Condition Notification (RHCN)	Icy or slippery road detected
Emergency Electronic Brake Lights (EEBL)	Emergency braking of sender
Emergency Vehicle Approaching (EVA)	Emergency vehicle requesting lane

TABLE II. Event types and the invalid actions (Ruj et. al. [27])

Event type	Expected action	Invalid action
SVA	Change lane Decrease speed	$D > d$ meters; same lane
RHCN	Car stops Changes route	$D > d$ meters; same route
EEBL	Car must slow down	$D > d$ meters
EVA	Change lane Slow down	$D > d$ meters; same lane as vehicle

Table II gives an overview of the static rules defined in [27]. For example, the *invalid action* stated before (*continuous driving of the event source*) maps to the static rule “$D > d\ meters$”, where D is the distance between the location of the vehicle at event start and the location after a specific amount of *Beacons*. We consider “$D > d\ meters$” a *static rule*, as it uses a fixed threshold (d) to distinguish between valid and invalid actions. In contrast, with REST-Net, the prevalent traffic situation can be taken into account, since sensor and *Beacon* data can be used as input for the calculation of a suitable (situation-dependent) threshold. For example, a suitable extension to the static rule “$D > d\ meters$” is to take the speed of the vehicle (that sent the related EEBL *Message*) into account, since obviously, the breaking distance depends on a vehicles actual speed.

This can be arranged with $\frac{v_{tn}}{v_{t0}}$ (a ratio of v_{t0}, the speed of the vehicle at the time of sending the EEBL *Message* and v_{tn}, its speed after a certain amount of time, i. e., the speed derived from the *Beacons* received next). A suitable threshold for an EEBL *Message* could be 0.5, i. e., the assumption that an alleged emergency break is only considered genuine if the vehicle decreases its speed to $50\,\%$ after sending the EEBL *Message* at t_0 and thus, if further warning *Messages* of that vehicle should be ignored or not. Generally, dynamic thresholds are a prerequisite for rules that adapt to different traffic situations, e. g., on highways or in cities. Further, they can be extended with additional information known to the ADAS, e. g., with the speed limit of the road in question, the density of attackers in the current area (cf. [37]) or with the aforementioned *extended plausibility checks*, that we will focus on next.

Extended plausibility checks can take into account both *Beacons* broadcast before and after the receipt of a warning *Message*. Thus, in contrast to static rules, they allow for pre-validation and post-validation and do not (necessarily) rely on singular events. For example, all rules defined in [27] perform post-validation only: They are based on the comparison of the *Beacon* sent along with the warning *Message* and the last

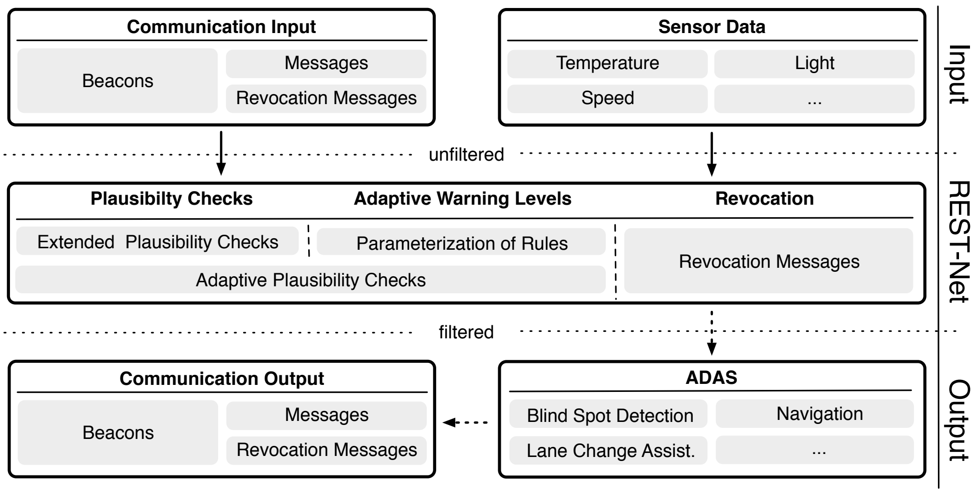

Fig. 1. Architecture of REST-Net

TABLE III. REST-NET RULES

	Rules
SVA	$T \vee (\neg P \wedge U) \rightarrow Attack$
RHCN	$P \vee (Q \wedge V) \rightarrow Attack$
EVA	$R \wedge S \rightarrow Attack$
EEBL	$P \vee Q \rightarrow Attack$

Beacon received when the validation is performed (cf. [27] and Tab. II).

However, pre-validation can be used to improve detection rates significantly. For example, a fake EEBL *Message* can be detected trivially, if the source vehicle was standing before it sent the *Message*, as EEBL *Messages* (which signal emergency breaking) require prior movement obviously. Generally, pre-validation enables very simple but effective rules in many cases (further rules are listed later in this section). However, in many cases, pre-validation and post-validation must be combined to achieve high detection rates. For example, if an attacker is able to change his identity to the role *emergency vehicle* in order to send *Emergency Vehicle Approaching Messages* (EVA *Messages*) to clear his way, we can assume that the attacker would not use this identity permanently to decrease the chance of getting caught. To this end, *Beacons* sent before and after an EVA *Message* can be analyzed to detect whether *Beacons* were sent under the identity of the emergency vehicle before and afterwards, or if those *Beacons* were sent under different identities, for which no *Beacons* are present anymore (note that the broadcast of *Beacons* is frequent enough and the contained position information suitable to distinguish between vehicles without the use of explicit identifiers [9], [10]; experiments in [38] show the detection of appearing sybil vehicles as well as vehicles with overlapping positions).

Table III shows several rules that we defined for REST-Net. The rules contain the examples of the previous paragraphs and are used in the feasibility study in Sect. V. Generally, the REST-Net rules are based on truth-functional propositional logic, which allows an intuitive creation of rules. Like in most IDS, the set of operator symbols consists of $\neg$, $\wedge$, $\vee$ and $\rightarrow$. The proposition symbols used in the rules in Tab. III, with t_0 (Event *Message* time), t_{min} (oldest monitored *Beacon* before t_0) and t_{max} (newest monitored *Beacon* after t_0), are:

- P: Vehicle was standing before t_0
- Q: Vehicle slowed down less than n % in time period t_{min} to t_{max}
- R: Received less than n *Beacons* without interruption
- S: Vehicle known for less than n ms
- T: Vehicle was standing less than n *Beacons* before t_0
- U: Vehicle did move more than n meters
- V: Vehicle was driving faster than v_0 at t_0

Adaptive warning levels. One key challenge for an IDS is to warn users or to ignore warning *Messages* only when a suffice probability for an attack exists, since IDS do generally not achieve a perfect detection rate. To this end, REST-Net uses *adaptive warning levels* to take into account the characteristics of different situations. REST-Net's *adaptive warning levels* are based on two concepts, the *adaptive plausibility checks* described before and the *parameterization of the rules*, i. e., the selection of appropriate thresholds.

Adaptive plausibility checks offer situation-aware decisions which lead to a lower error rate in general and, therefore, less disturbance for the user compared to fixed rules. In contrast, the *parameterization of the rules* can be used to select a suitable trade-off between *true negatives* (i. e., the percentage of *Messages* that are classified correctly as genuine) and *true positives* (i. e., the percentage of *Messages* that were classified correctly as attacks). This trade-off can be adjusted by choosing different thresholds for the propositions (listed before). For example, the threshold 0.5 described for EEBL *Messages* can be varied between $[0, 1]$. We will present *receiver operating characteristic* (*ROC*) *curves* for different rules and *Message* types in Sect. V, however, even with knowledge of the trade-off and the resulting true positive (TP) and true negative (TN) rates, an appropriate value (threshold) must be chosen. In our view, it is more important to optimize the TN rate, i. e., to prevent the suppression of genuine *Messages* at the cost of a lower TP rate, since a high number of unreported events will

TABLE IV. EXAMPLE OF TRUE NEGATIVE (TN) AND TRUE POSITIVE RATES (TP) IN AN IDS

	genuine Msg.	fake Msg.	TN	TP	errors
Threshold A	$100,000$	100	90%	80%	10020
Threshold B	$100,000$	100	91%	50%	9050

reduce the trust of the driver in the IDS (cf. [39]) and the suppression of genuine warning *Messages* is probably a more severe safety issue than undetected fake *Messages*. Further, repeated (considered genuine) warning *Messages* of the same sender that would have lead to an alert with a slightly different threshold can still be used to detect an attacker over time (since an IDS is not limited to a single threshold).

To this end, the thresholds suggested for REST-Net and used in Sect. V favor the TN rate over the TP rate. We want to point out that the *base-rate fallacy* (cf. [40]) must be taken into account if another trade-off shall be chosen in the future. Table IV shows an example. If $100,000$ genuine and 100 fake *Messages* are received in a time span, one might (intuitively) choose *Threshold A* over *Threshold B*. However, *Threshold B* clearly produces less errors.

Message revocation scheme. Besides rule-based protection, the REST-Net concept contains a component for the removal of false data after the detection of an attacker. Especially, in the case of a strong adversary like the *unbounded attacker* this feature is important. As discussed in Sect. III, a reliable and realtime protection against this adversary is not realistic. However, at least some attacks may be detected over time, which demands an effective way to clean up false data in VANETs. While there has been a lot of research in the revocation of VANET identities (cf. [41]–[45]) the revocation of single *Messages* in the area of Intrusion Detection Systems has found less attention. Ostermaier et al. [46] propose to revoke *Messages* after performing a voting scheme. Following, a possible way to implement this idea for REST-Net is discussed. The revocation of *Messages* can provide a fast way to cleanup data in VANETs before revoking the identity which takes time and resources. Furthermore, the status of the VANET identity is normally checked on first contact but not with every received *Message*.

A *revocation Message* vetoes the *Message* of the adversary. Equation 1 shows a normal *Message* M_A adapted from [5], signed with a private key PrK_A, a public key certificate $Cert_A$, with A being the attacker vehicle, X illustrating the *Message* text and the timestamp T.

$$M_A = X_A, Sig_{PrK_A}\left[X_A \mid T\right], Cert_A \tag{1}$$

A vehicle V, detecting abnormalities in M_A would respond with a revocation *Message* R_V as proposed in equation 2.

$$R_V = X_V, h(M_A), Sig_{PrK_V}\left[X_V \mid h(M_A) \mid T\right], Cert_V \tag{2}$$

In contrast to *normal Messages*, *revocation Messages* contain a hashed value of the contradicting *Message* $h(M_A)$ they refer to and a new *Message* X_V, which contains one of the following revocation reasons:

- **Human assistance**: After passing the *Message* location the vehicle sensors of V noticed no abnormalities (e. g., no traffic jam, no icy road etc.).
- **Identity revocation noticed**: V noticed that the identity of A has been revoked (depending on the revocation scheme and due to performance issues vehicles might not check every certificate for revocation in realtime).
- **Posterior IDS revelation**: The IDS of V noticed an attack after collecting additional data. In this case, it is important to attach supplementary data (e. g., type of IDS, version, IDS data etc.) to clarify how the conclusion was formed.

Of course, *revocation Messages* from various sources with different revocation reasons (e. g., different sensors and IDS types) provide a more convincing case to trust the senders, because a single revocation *Message* can simply origin from an adversary. To this end, a majority voting scheme (e. g., LEAVE [26]) should be used in conjunction with the REST-Net *Message* revocation scheme.

V. EVALUATIONS

The goal of this section is to evaluate the concept of Ruj et. al. [27] and REST-Net as realistic as possible. We focus on detection rates as well as stability in different (street) environments. Because VANETs are still a theoretical concept (except for some test fields[3]) a simulation-based evaluation approach was selected. The VANET-Simulator [47], [48], a micro-traffic simulator with integrated VANET-Model (based on [49]–[51]), features realistic traffic simulations as well as a focus on security regarding the application layer. Therefore, it is a suitable tool for our evaluation and enables more realistic results than plain analyses.

We have implemented both REST-Net and the IDS of Ruj et. al. for the *VANET-Simulator* and considered twelve different scenarios according to the four *Message* types defined in Sect. IV, as well as three different maps of real cities using Open-Street-Maps[4] of Berlin, New York and Puebla. The map extracted from Berlin with $854\,km$ street length represents cities with slightly obscure road networks. New York ($547\,km$) features a street grid and Puebla (496 km) displays both characteristics depending on the area. Each simulation contains $8,000$ vehicles with 100 adversaries, faking *Messages* at random locations. Furthermore, real events where added for each *Message* type (e. g., icy roads, traffic jams, random braking events or emergency vehicles). IDS of vehicles are preset to decide about attacks after collecting *Beacon*-data for $2000\,ms$.

To evaluate the Intrusion Detection Systems (REST-Net and [27]) and to discover the proper thresholds and limitations, diverse simulation runs varying each threshold 10 times with 10 iterations for $\approx 16,7\,min$ simulation time ($\approx$ 350000 attacks per *Message* type) were executed for all scenarios on the maps. Figures 2 and 3 show the results in form of Receiver Operating Characteristic (ROC) curves displaying the fractions of

[3] http://www.simtd.de/

[4] http://www.openstreetmap.org

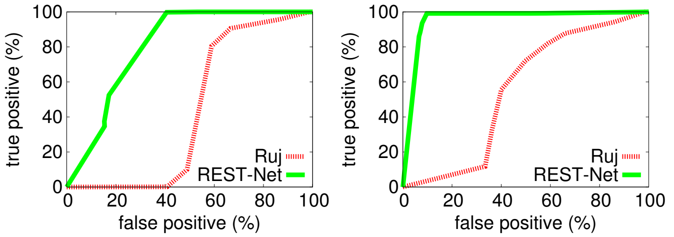

Fig. 2. Berlin ROC curves: RHCN (left); EEBL (right)

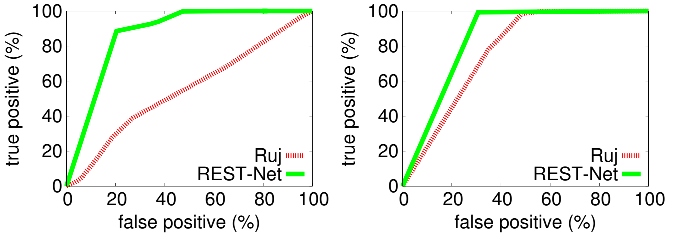

Fig. 3. Berlin ROC curves: EVA (left); SVA (right)

true positives versus the fraction of the false positives. REST-Net displays feasible results and improvements compared to the model of Ruj et. al.. Especially, RHCN, EEBL and EVA *Messages* show major improvements (note that, because of binary decisions in REST-Net, like *vehicle was standing before sending a SVA Message*, the curve progression in Figure 2 and 3 is partial discontinuous).

Besides the current traffic situation or street environment, considerations regarding TN rates and FP rates influence the choice of thresholds as already discussed in Sect. IV. The **adaptive warning levels** demand a selection of thresholds regarding the base-rate fallacy. It is important to maximize the true negative rate while still reaching a fair level of protection against attacks. Figure 4 shows an example of a selection for RHCN *Messages* with the rules of [27].

Following, equal thresholds for Berlin, New York and Puebla were selected to archive a trade-off between TN and TP rates, but with a preference for TN rates. Figures 5 - 7 present feasible results regarding REST-Net for all three cities and major improvements compared to the model of Ruj. et. al.. TN rates in REST-Net remain between $\approx 95,6\%$ and $\approx 99,9\%$ compared to $\approx 40,9\%$ and $\approx 99,9\%$ with [27]. Especially, RHCN, EEBL and EVA *Messages* display good improvements. With detection rates between $\approx 56,4\%$-$\approx 100\%$ for REST-Net and $\approx 28{,}8\%$-$\approx 63,9\%$ for the model of Ruj. et. al.. True positives improved, too, but leave room for improvements in REST-Net. As discussed before, lower TP rates might be accepted in exchange for higher TN rates. Nevertheless, while showing improvements to [27], SVA, RHCN and EEBL false *Message* detection should be improved by combining REST-Net with models monitoring other layers or using other techniques, e. g., trying to detect an attacker over time (by using different thresholds and raising an alert after several *suspicious Messages* of the same source, as suggested in Sect. IV).

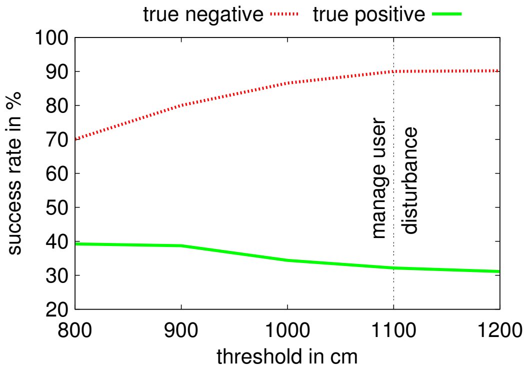

Fig. 4. Selection of thresholds for RHCN *Messages*

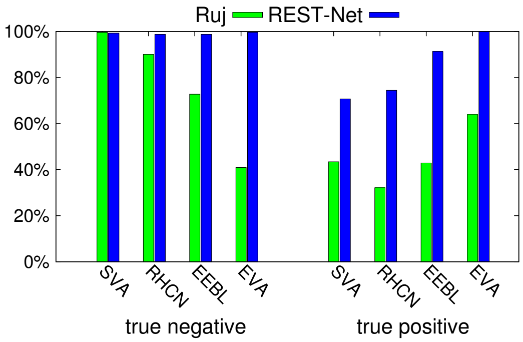

Fig. 5. Berlin: Detection rates of Ruj et al. and REST-Net

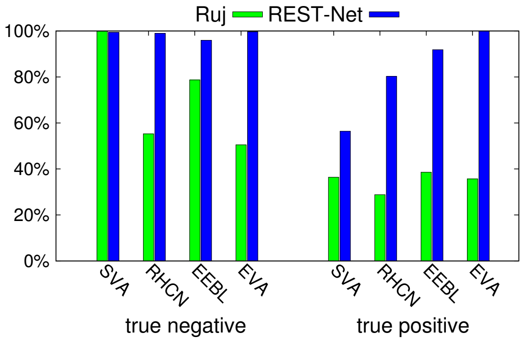

Fig. 6. New York: Detection rates of Ruj et al. and REST-Net

Besides improved detection rates, REST-Net is more stable to deviations in the road network and shows less variations in the detection rates in the different cities than [27]. Nevertheless, small adaptions seem to be necessary to different road networks, especially, when taking into account that in different cities and regions drivers might drive more aggressive or passive. While this optimization might lead to better results, getting suitable training data is challenging.

VI. Conclusion & Future work

In this paper we presented REST-Net, a novel Intrusion Detection System that assists in dealing with integrity and authenticity challenges in Vehicular Ad Hoc Networks. REST-Net processes *Beacon* data with plausibility checks to detect fake *Messages*.

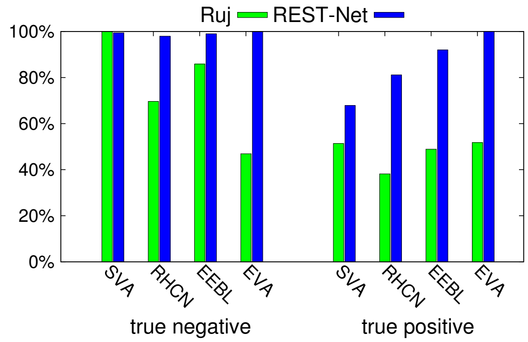

Fig. 7. Puebla: Detection rates of Ruj et al. and REST-Net

To the best of our knowledge, REST-Net is the first IDS for VANETs including a detection engine with pre- and post event validation, adaptive rules, adaptive warning levels and an agile way to revocate detected malicious *Messages*. Realistic simulation-based evaluations with a micro-traffic simulator indicate feasible detection rates as well as major improvements compared to existing solutions. Additionally, simulations in various cities demonstrate that REST-Net works stable in various road networks like grids or more obscure streets and offers high adaptability.

As future work, various ways of sharing REST-Net data and alerts between vehicles will be analyzed. Further, processing or transferring IDS data from neighbors or authorities might lead to improved detection rates, but also new attacks. Moreover, we plan to combine REST-Net with IDS modules from previous work for various OSI layers to further increase its detection rate.

References

[1] "IEEE Computer Society. IEEE Standard for Information technology– Local and metropolitan area networks– Specific requirements– Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Wireless Access in Vehicular Environments," Juli 2010.

[2] "IEEE Vehicular Technology Society. IEEE Standard for Wireless Access in Vehicular Environments." 2013.

[3] K. Plößl and H. Federrath, "A Privacy Aware and Efficient Security Infrastructure for Vehicular Ad Hoc Networks," in *Security in Information Systems: Proceedings of the 5th International Workshop on Security in Information Systems – WOSIS 2007*, 2007.

[4] G. Calandriello, P. Papadimitratos, J.-P. Hubaux, and A. Lioy, "Efficient and Robust Pseudonymous Authentication in VANET," in *Proceedings of the Fourth International Workshop on Vehicular Ad Hoc Networks, VANET 2007, Montréal, Québec, Canada, September 10, 2007*, 2007.

[5] M. Raya and J.-P. Hubaux, "The Security of Vehicular Ad Hoc Networks," in *Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks (SASN)*, 2005.

[6] "ETSI TS 102 637-2: Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Co-operative Awareness Basic Service." 2011.

[7] "SAE J 2735. Dedicated Short Range Communications (DSRC) Message Set Dictionary," 2009.

[8] "ETSI TS 102 637-3: Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Application; Part 3: Specification of Decentralized Environmental Notification Basic Service." 2010.

[9] L. Buttyán, T. Holczer, and I. Vajda, "On the Effectiveness of Changing Pseudonyms to Provide Location Privacy in VANETs," in *Proceedings of the Fourth European Workshop on Security and Privacy in Ad hoc and Sensor Networks (ESAS 2007)*, Juli 2007.

[10] F. Scheuer, K. Plößl, and H. Federrath, "Preventing Profile Generation in Vehicular Networks," in *WIMOB '08: Proceedings of the 2008 IEEE International Conference on Wireless & Mobile Computing, Networking & Communication*, 2008.

[11] J. Freudiger, M. Raya, M. Félegyházi, P. Papadimitratos, and J.-P. Hubaux, "Mix-Zones for Location Privacy in Vehicular Networks," in *ACM Workshop on Wireless Networking for Intelligent Transportation Systems (WiN-ITS)*, 2007.

[12] A. R. Beresford and F. Stajano, "Location Privacy in Pervasive Computing," *IEEE Pervasive Computing*, 2003.

[13] ——, "Mix Zones: User Privacy in Location-aware Services," in *2nd IEEE Conference on Pervasive Computing and Communications Workshops (PerCom 2004 Workshops), 14-17 March 2004, Orlando, FL, USA*, 2004.

[14] L. Huang, K. Matsuura, H. Yamane, and K. Sezaki, "Enhancing Wireless Location Privacy Using Silent Period," in *Proceedings of the 2005 IEEE Wireless Communications and Networking Conference (WCNC)*, 2005.

[15] L. Huang, H. Yamane, K. Matsuura, and K. Sezaki, "Silent Cascade: Enhancing Location Privacy Without Communication QoS Degradation," in *Security in Pervasive Computing, Third International Conference, SPC 2006, York, UK, April 18-21, 2006, Proceedings*, 2006.

[16] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," *Journal of Computer Security*, 2007.

[17] G. Yan, S. Olariu, and M. C. Weigle, "Providing VANET Security Through Active Position Detection," *doi:10.1016/j.comcom.2008.01.009*, 2008.

[18] S. Park, B. Aslam, D. Turgut, and C. C. Zou, "Defense against sybil attack in Vehicular Ad Hoc Network based on roadside unit support," in *Proceeding MILCOM'09 Proceedings of the 28th IEEE conference on Military communications*, 2009.

[19] T. Zhou, R. Roy, C. Peng, and N. K. Chakrabarty, "Privacy-Preserving Detection of Sybil Attacks in Vehicular Ad Hoc Networks," in *Proceeding MOBIQUITOUS '07 Proceedings of the 2007 Fourth Annual International Conference on Mobile and Ubiquitous Systems: Networking&Services (MobiQuitous)*, 2007.

[20] T. Zhou, R. Choudhury, P. Ning, and K. Chakrabarty, "P2DAP - Sybil Attacks Detection in Vehicular Ad Hoc Networks," *Selected Areas in Communications, IEEE Journal on*, 2011.

[21] B. Xiao, B. Yu, and C. Gao, "Detection and Localization of Sybil Nodes in VANETs," in *Proceedings of the 2006 workshop on Dependability issues in wireless ad hoc networks and sensor networks*, 2006.

[22] G. Guette and B. Ducourthial, "On the Sybil attack detection in VANET," *IEEE International Conference on Mobile Adhoc and Sensor Systems Conference*, 2007.

[23] M. S. Bouassida, G. Guette, M. Shawky, and B. Ducourthial, "Sybil Nodes Detection Based on Received Signal Strength Variations within VANET," *International Journal of Network Security*, 2009.

[24] P. Golle, D. Greene, and J. Staddon, "Detecting and Correcting Malicious Data in VANETs," in *Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks*, 2004.

[25] M. Ghosh, A. Varghese, A. Kherani, and A. Gupta, "Distributed Misbehavior Detection in VANETs," in *Wireless Communications and Networking Conference, 2009. WCNC 2009. IEEE*, 2009.

[26] M. Raya, P. Papadimitratos, I. Aad, D. Jungels, and J.-P. Hubaux, "Eviction of Misbehaving and Faulty Nodes in Vehicular Networks," *IEEE Journal on Selected Areas in Communications*, 2007.

[27] S. Ruj, M. A. Cavenaghi, Z. Huang, A. Nayak, and I. Stojmenovic, "On data-centric misbehavior detection in vanets," in *Vehicular Technology Conference (VTC Fall), 2011 IEEE*, 2011.

[28] T. Leinmüller, E. Schoch, and C. Maihöfer, "Security Requirements and Solution Concepts in Vehicular Ad Hoc Networks," *Fourth Annual Conference on Wireless on Demand Network Systems and Services*, 2009.

[29] J. Rizzo and T. Duong, "Here come the xor ninjas," *Unpublished manuscript*, May 2011.

[30] N. J. AlFardan and K. G. Paterson, "Lucky thirteen: Breaking the tls and dtls record protocols," in *IEEE Symposium on Security and Privacy*, 2013.

[31] C. Meyer and J. Schwenk, "Lessons learned from previous ssl/tls attacks-a brief chronology of attacks and weaknesses," *IACR Cryptology ePrint Archive*, 2013.

[32] N. Leavitt, "Internet security under attack: The undermining of digital certificates," *Computer 44.12*, 2011.

[33] J. R. Douceur, "The Sybil Attack," in *Peer-to-Peer Systems*. Springer Berlin / Heidelberg, 2002.

[34] J. P. Anderson, "Computer Security Threat Monitoring and Surveillance," James P. Anderson Company, Fort Washington, Pennsylvania, Tech. Rep., 1980.

[35] T. F. Lunt, "A survey of intrusion detection techniques," *Computers & Security*, 1993.

[36] F. Bai, H. Krishnan, V. Sadekar, G. Holl, and T. Elbatt, "Towards characterizing and classifying communication-based automotive applications from a wireless networking perspective," in *In Proceedings of IEEE Workshop on Automotive Networking and Applications (AutoNet)*, 2006.

[37] J. Petit, M. Feiri, and F. Kargl, "Spoofed data detection in vanets using dynamic thresholds," in *Vehicular Networking Conference (VNC), 2011 IEEE*, 2011.

[38] N. Bissmeyer, K. Schroder, J. Petit, S. Mauthofer, and K. Bayarou, "Short paper: Experimental analysis of misbehavior detection and prevention in vanets," 2013.

[39] S. Axelsson, "The Base-Rate Fallacy and the Difficulty of Intrusion Detection," *ACM Trans. Inf. Syst. Secur.*, 2000.

[40] M. Bar-Hillel, "The base-rate fallacy in probability judgments," *Acta Psychologica*, 1980.

[41] Y. Sun, R. Lu, X. Lin, X. Shen, and J. Su, "A Secure and Efficient Revocation Scheme for Anonymous Vehicular Communications," in *Communications (ICC), 2010 IEEE International Conference on*, 2010.

[42] A. Wasef, Y. Jiang, and X. Shen, "DCS: An Efficient Distributed-Certificate-Service Scheme for Vehicular Networks," *Vehicular Technology, IEEE Transactions on*, 2010.

[43] J. J. Haas, Y.-C. Hu, and K. P. Laberteaux, "Design and Analysis of a Lightweight Certificate Revocation Mechanism for VANET," in *Proceedings of the sixth ACM international workshop on VehiculAr InterNETworking*, 2009.

[44] C. Jung, C. Sur, Y. Park, and K.-H. Rhee, "A Robust Conditional Privacy-Preserving Authentication Protocol in VANET," in *Security and Privacy in Mobile Information and Communication Systems*. Springer Berlin Heidelberg, 2009.

[45] R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, "ECPP: Efficient Conditional Privacy Preservation Protocol for Secure Vehicular Communications," in *INFOCOM 2008. The 27th Conference on Computer Communications. IEEE*, 2008.

[46] B. Ostermaier, F. Dotzer, and M. Strassberger, "Enhancing the security of local dangerwarnings in vanets-a simulative analysis of voting schemes," in *Availability, Reliability and Security, 2007. ARES 2007. The Second International Conference on*, 2007.

[47] A. Tomandl, F. Scheuer, and H. Federrath, "Simulation-based evaluation of techniques for privacy protection in VANETs," *Wireless and Mobile Computing, Networking and Communications (WiMob)*, 2012.

[48] "VANET Simulator," 2013. [Online]. Available: http://www.vanet-simulator.org

[49] S. Krauß, "Microscopic Modeling of Traffic Flow: Investigation of Collision Free Vehicle Dynamics," Ph.D. dissertation, Universität Köln, 1998.

[50] K. Nagel and M. Schreckenberg, "A cellular automaton model for freeway traffic," *J. Phys. I France*, 1992.

[51] M. Treiber, A. Hennecke, and D. Helbing, "Congested Traffic States in Empirical Observations and Microscopic Simulations," *Physical Review E*, 2000.