# Misbehavior Detection in Vehicular Ad-hoc Networks

Rens van der Heijden, Stefan Dietzel, Frank Kargl
Institute of Distributed Systems
University of Ulm, Germany
{rens.vanderheijden, stefan.dietzel, frank.kargl}@uni-ulm.de

In this paper we discuss misbehavior detection for vehicular ad-hoc networks (VANETs), a special case of cyber-physical systems (CPSs). We evaluate the suitability of existing PKI approaches for insider misbehavior detection and propose a classification for novel detection schemes.

Cyber-physical systems (CPSs) are digital systems that are closely embedded into the physical world with which they interact through sensors and actuators. In contrast to classical embedded systems, they often form networks with a large number of sensor or actuator devices. These devices sense information, process it in a distributed system, and then influence the physical world using actuators. Notable examples of CPS are wireless sensor networks (WSNs), smart factories, distributed e-Health systems, and VANETs. In this paper, we focus on VANETs, which are a prime example for CPS and will soon be deployed on a large scale.

Vehicular ad-hoc networks (VANETs) are networks that are created by equipping vehicles with wireless transmission equipment. VANETs offer great potential to improve road safety and to provide information and entertainment applications for drivers and passengers. Due to the unique properties of VANETs, this type of network has attracted many researchers, including those in the domain of security. The security challenges in VANETs include the requirement for strong privacy, the computationally constrained environment, and the ephemeral nature of connectivity.

VANETs and other CPSs share a number of characteristics that require fundamentally new approaches for security, which differ from existing IT security requirements.

- **Critical usage scenarios.** CPSs often control systems where failure or malfunction may have severe consequences, including massive financial loss or loss of lives. Often, these systems fall under the term critical infrastructures (CI). VANETs are one example where failure or malfunction may lead to massive congestion with subsequent delays and financial losses or even to accidents with loss of lives in a worst case.
- **No clear security perimeter.** In many of these systems, there is no clear boundary between insiders and outsiders. Instead, the logically and physically distributed nature of CPSs leads to unclear security perimeters and possible insider attacks. VANETs are again a core example, as such networks are cooperatively formed by vehicles and road-side equipment. As vehicles are under distributed ownership and control, it needs to be assumed that some of the vehicles are under full control of attackers.
- **Limited physical security.** As nodes in CPSs are often distributed in a potentially hostile environment, they may be subject to hijacking, analysis, and reprogramming by attackers. Due to cost constraints, the protection against such hijacking is often limited. A typical example is a Wireless Sensor Network for environmental monitoring, where nodes may be scattered randomly in the environment. Due to the long lifetime of vehicles, similar challenges can be found in both VANETs and in-vehicle networks.
- **Sensor values as security assets.** The primary security assets in CPS are the sensor values and the actuators controlled based on this input. Spoofing and manipulation of sensor data are thus primary attack vectors. For instance, in a VANET that is used for detecting traffic jams, an attacker may want to suppress certain sensor readings that would indicate a traffic jam, or inject sensor values that indicate a traffic jam where none exists.

In summary, CPSs, and VANETs in particular, will likely attract attackers that try to manipulate sensed data and influence the resulting actions taken by the system. Such attackers may participate as regular network entities either because attackers can easily join the VANET or hijack already participating nodes. Once an attacker has entered the VANET, she can easily inject spoofed infor-

mation into the VANET and trigger incorrect behavior. From the perspective of the VANET, this attacker can be seen as a misbehaving node that is sending incorrect data. In addition to information injection and manipulation, other attack types are conceivable, such as compromising routing efficiency by not forwarding information for other nodes. In this paper, we focus on detection of information manipulation. Note we cannot necessarily distinguish whether information manipulation is due to malicious intent or due to faulty hardware. However, from an information quality perspective, the resulting countermeasures should arguably often be the same.

Classical IT security mechanisms, like encryption, signatures, access control, (signature-based) intrusion detection systems, and so forth, are not suitable to thwart such insider attacks. Instead, we need security mechanisms that can identify misbehavior, identify the misbehaving node, and react either by filtering out the incorrect data or excluding the misbehaving node from further participation in the VANET. Research on security in VANETs has already developed several novel ideas for these tasks, many of which align with the goals of other CPSs.

Golle et al. [1] propose a method to detect misbehavior as we defined it above in the context of VANETs. Instead of placing *trust* in nodes – as often done by classical cryptographic authentication mechanisms –, the proposed approach is to gain *confidence* in correctness of data by analyzing the local information base and deriving most probable explanations. During the following years, more research was done that proposes comparable misbehavior detection mechanisms for VANETs. Examples of these include [2], [3], [4], [5], [6], [7], and [8].

There are fundamentally different approaches to misbehavior detection that can be used for a categorization of different mechanisms as shown in Figure 1. A first distinction is whether mechanisms focus on data values contained in messages or on the node sending the messages. *Node-centric* mechanisms require authentication mechanisms to reliably distinguish between different nodes. Many systems achieve this by assuming a trusted third party like a PKI that issues credentials, which are then used to authenticate messages and the corresponding information, using a security mechanism like digital signatures. Node-centric mechanisms can further be divided into *behavioral* and *trust-based* mechanisms.

*Behavioral* mechanisms inspect a node's observable behavior (but not the information it is sending) and try to derive a metric that identifies how well a node behaves. For instance, a behavioral mechanism may inspect rates at which a neighboring node sends packets and decide whether a node significantly exceeds a "normal rate,"

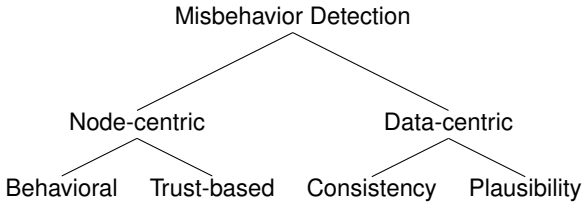


Fig. 1. Taxonomy of misbehavior detection.

which would then be considered as misbehavior. This approach is particularly common in WSNs, and is sometimes referred to as a Watchdog mechanism. However, attempts have been made to distribute these ideas in such a way that the need for a trusted node is removed, with the goal that a Watchdog mechanism can be used in VANETs [9].

On the other hand, *trust-based* mechanisms inspect the past and present behavior of a node and use this to derive a probability for future misbehavior. The assumption is that a node who behaved correctly in the past is more likely to behave correctly in the future. Essentially, this boils down to some form of reputation management scheme where correct behavior increases the reputation while misbehavior reduces it. These mechanisms are commonly used for reporting and local revocation of nodes in a VANET, for example through LEAVE [10].

In contrast to those node-centric mechanisms, the second major category, namely *data-centric* misbehavior detection, subsumes all mechanisms that directly inspect the disseminated information to detect potential misbehavior. While *data-centric* mechanisms do not primarily care about the identities of individual nodes, they often still require some form of linking between messages to be able to reliably distinguish between different hosts. However, these mechanisms do not depend on the linkability of messages, which makes them highly valuable for the detection of Sybil attacks. Sybil attacks are a type of attack where a node replicates itself arbitrarily to undermine the honest majority assumption. Due to the strong privacy requirements in VANETs compared to other cyber-physical systems, which makes linkage between different messages more difficult, concerns for Sybil attacks are particularly relevant. In response to this, many VANET researchers have developed novel schemes to perform data-centric misbehavior detection; these can be divided further into *consistency* and *plausibility* mechanisms.

Of these two types, *consistency* mechanisms rely more strongly on protection against sybil attacks. The purpose of consistency mechanisms is to compare measurements from different entities to detect and, where possible, resolve conflicts between these measurements. For in-

stance, in a VANET, a single vehicle could report a severe traffic jam while other vehicles report free flow of traffic. A consistency-based mechanism would use such information to conclude that there is likely no traffic jam and that the single vehicle may have misbehaved or be faulty.

Finally, *plausibility* checking mechanisms are all mechanisms that have some implicit or explicit model of the real world and check whether incoming information is plausible within this model. For instance, in VANETs, speed reports of 700 km/h are not very plausible and may be filtered out. However, plausibility should be applied with caution in VANETs, as part of the focus of such networks is to detect outliers that indicate important, but rare, events, such as collisions between vehicles.

Note that no single mechanism alone will likely provide a convincing misbehavior detection mechanism that detects all forms and types of misbehavior. Instead, mechanisms will likely be combined. For instance, consider the following as an example for a combined approach. First, a number of data-centric mechanisms work on the same knowledge base to jointly detect incorrect data. Results are then augmented using behavioral mechanisms that check whether nodes behave according to protocol specifications. All these mechanisms are then used as input to a node-centric reputation management system that determines whether nodes show long-term misbehavior. These misbehaving nodes can then be reported to a central authority, which can determine whether nodes should be removed from the network; meanwhile, the nodes can be revoked temporarily by the nodes that detected the misbehavior. In the case of VANETs, the latter is particularly important, as this provides protection against determined attackers that may not be discouraged by high fines.

Based on our categorization, we are currently preparing a broad literature study on misbehavior detection in both VANETs and other CPSs. Our goal is to identify general patterns for misbehavior that work across specific application domains and scenarios, and can be re-used for a generic misbehavior detection architecture. This will allow application of security mechanisms developed for VANETs to be applied to a broader spectrum of problems, and could lead to security mechanisms developed for other CPSs to be applied to VANETs, furthering the safety and security of both.

## REFERENCES


[1] 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*. Philadelphia, PA, USA: ACM, 2004, pp. 29–37.

[2] N. Biß meyer, J. Njeukam, J. Petit, and K. M. Bayarou, "Central misbehavior evaluation for VANETs based on mobility data plausibility," in *Proceedings of the ninth ACM international workshop on Vehicular inter-networking, systems, and applications - VANET '12*. New York, New York, USA: ACM Press, 2012, pp. 73–82.

[3] M. Raya, P. Papadimitratos, V. D. Gligor, and J.-P. J.-P. Hubaux, "On Data-Centric Trust Establishment in Ephemeral Ad Hoc Networks," in *2008 IEEE INFOCOM - The 27th Conference on Computer Communications*. Ieee, Apr. 2008, pp. 1238–1246.

[4] J. Grover, V. Laxmi, and M. Gaur, "Misbehavior detection based on ensemble learning in vanet," in *Advanced Computing, Networking and Security*, ser. Lecture Notes in Computer Science, P. Thilagam, A. Pais, K. Chandrasekaran, and N. Balakrishnan, Eds. Springer Berlin / Heidelberg, 2012, vol. 7135, pp. 602–611.

[5] H. Stübing, J. Firl, and S. A. Huss, "A two-stage verification process for Car-to-X mobility data based on path prediction and probabilistic maneuver recognition," in *2011 IEEE Vehicular Networking Conference (VNC)*. IEEE, Nov. 2011, pp. 17–24.

[6] J. Hortelano, J. Ruiz, and P. Manzoni, "Evaluating the usefulness of watchdogs for intrusion detection in vanets," in *Communications Workshops (ICC), 2010 IEEE International Conference on*, may 2010, pp. 1 –5.

[7] M. Mahmoud and X. Shen, "Stimulating cooperation in multihop wireless networks using cheating detection system," in *INFOCOM, 2010 Proceedings IEEE*, march 2010, pp. 1 –9.

[8] R. K. Schmidt, T. Leinmüller, E. Schoch, A. Held, and G. Schäfer, "Vehicle behavior analysis to enhance security in vanets," in *Proceedings of the 4th Workshop on Vehicle to Vehicle Communications (V2VCOM 2008)*, 2008.

[9] Z. Li, C. Chigan, and D. Wong, "AWF-NA: A Complete Solution for Tampered Packet Detection in VANETs," in *IEEE GLOBECOM 2008 - 2008 IEEE Global Telecommunications Conference*. IEEE, 2008, pp. 1–6.

[10] 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*, vol. 25, no. 8, pp. 1557–1568, Oct. 2007.