Intrusion Detection in VANETs

Tim Leinmüller[+], Albert Held[+], Günter Schäfer[++] and Adam Wolisz[++]
[+]DaimlerChrysler AG, Telematics Research, {Tim.Leinmueller|Albert.Held}@DaimlerChrysler.com
[++]TU Berlin, TKN Research Group, {Schaefer|Wolisz}@tkn.tu-berlin.de

***Abstract*— Vehicular ad hoc networks (VANETs) have great potential to improve road safety and increase passenger convenience in vehicles. On the other hand, since they use an open medium for communication, they are exposed to several threats that influence the reliability of these features.**

This work presents a modular cross layer intrusion detection approach as a method to increase security in VANETs. The approach makes use of context information from systems such as GPS, radar or sensors, to evaluate the plausibility of information received via the network. The goal is to combine events on different layers and from different entities, in order to detect abuse and intrusion.

I. Introduction

Communication within vehicular ad hoc networks (VANETs) includes both, inter-vehicle communication as well as vehicle to infrastructure communication, directly between neighboring nodes, but also via intermediate nodes, i.e. multi-hop ad hoc communication.

In general, applications in a VANET environment can be categorized into three different classes: cooperative driver assistance applications (safety-related or active safety applications), decentralized floating car data applications and user communication and information services [1], [2].

To motivate our work, we use an example scenario out of the cooperative driver assistance applications class. Sensors of a car that is driving on a highway detect that the car driver has to start emergency braking because of an accident. The car's active safety communication system broadcasts this event to other cars driving on the same highway (see Figure 1). Upon the reception of one or multiple of these emergency braking alerts, the active safety systems of the following cars will display a warning message to the driver or even (as a future option) initiate an active braking procedure.

With this scenario in mind, one could also imagine a malicious person, trying to influence traffic flow on a highway by sending wrong information about the current road situation. As depicted in figure 2, this person could send wrong emergency braking messages.

Based on the above example, and taking into account that communication and security in VANETs are influenced by the following characteristics and requirements, the obvious conclusion is that VANETs are vulnerable to many security threats. VANETs use wireless communication, nodes are able to move with high velocity, resulting in a high rate of topological changes. Node density will vary, depending on current traffic situation. Communication partners will change frequently, in general, there are no previously established trust relationships. Instead of "traditional" routing and addressing schemes, position dependent routing and addressing is used. The deployed applications are time critical, additional delays, introduced by security providing systems (e.g. IDS, PKI), must be minimized. Furthermore nodes (vehicles) should be able to remain anonymous when sending messages, which

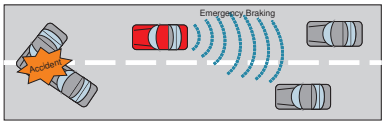

Fig. 1. Example Scenario: Emergency Braking

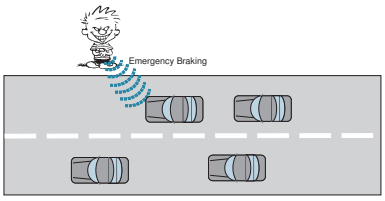

Fig. 2. Example Scenario: False Emergency Braking

contain sensor data such as velocity or current position. Due to these conditions, not all of the threats can be eliminated with preventive security mechanisms, thus, reactive mechanisms in form of an intrusion detection system can increase security, as we will describe in this paper.

In the following section, we discuss related work and explain, why the work published so far, does not meet the requirements of VANETs. In section III, we present our cross layer intrusion detection approach, which relies on context information to enable network and application data analysis. Finally in section IV we provide a conclusion and an outlook on our future work.

II. Related Work

In [3] and [4] the authors discuss a statistical anomaly detection approach for mobile ad hoc networks. So far, the authors concentrate on simulations at the routing protocol level, but in [3] they mention that multi-layer integrated intrusion detection would be helpful to increase detection rate. On the application layer, they suggest to use statistical analysis of service parameters, such as service time or service request rate. However, due to the continuously changing topology within VANETs, a statistical anomaly detection approach (especially on the routing level) seems not to be applicable, since it is very difficult to study normal behavior in training phases, that will later on differ from an attack.

The idea of using a distributed mobile security agent based intrusion detection system, as sketched by the authors of [5], presumes unambiguous node identification and absolute trust in elected agent nodes. High rate of topology changes do require frequent re-election of mobile agent hosting nodes. Overall, an approach that will not be suitable for VANETs.

Marti et al. propose a detection approach based on overhearing routing transmissions in [6]. In an environment with fast moving nodes, this approach could be difficult to realize, since

there is a high probability that the forwarding node leaves the physical range of the overhearing node during the forwarding process.

So far, the assumptions made in previous publications do not correspond to the features of VANETs, especially not to the high rates of topology changes. Nevertheless, taking information from multiple layers as mentioned in [3], as well as monitoring neighboring nodes [6], give indications on what could be applicable in VANETs.

III. Intrusion Detection in VANETs

Reconsidering the malicious road side attacker that is sending wrong emergency braking warnings, as described in the introduction, a defensive detection process could be as follows.

A first event of a suspicious action within the active safety system would be discovered, if an emergency braking event is received from a previously unknown node. One would normally expect such an event to come from a previously known node. A second event might come from another vehicle that previously passed this area and also received the same warning message. After passing the respective area, this car's intrusion detection system recognizes, that for itself, there was no emergency braking event and transfers this analysis to follow up cars.

Combining these two events results in a strong evidence that the received warning message must be a fake warning. Thus, the intrusion detection system tells the active safety system to ignore the warning and communicates the detection results to other nodes, especially follow up nodes.

In order to realize such an effective intrusion detection system in VANETs, we advocate the use of a modular cross layer intrusion detection system. On every node, different modules are in charge of collecting audit data on different layers. A local decision module receives continuously audit data summaries from the other modules and analyses them with the aid of additional information, available from other non-network devices, such as GPS, sensors and radar (side channel data or context data).

Apart from the central decision module, the different modules are: a monitoring module for the network and routing layer, a context information module, an application evaluation module, an action module and a module for communication with intrusion detection systems on other nodes (see Figure 3).

The monitoring module for network activity and routing is responsible for collecting data on communication within the node's communication range. This includes monitoring the neighboring nodes' forwarding attitude, as well as the generation of a list of current and previous neighbors, including their positions and movements, i.e. the creation of a network topology development report. The current neighboring nodes' position data can be verified by active probing messages, or GPS and sensor data from the context information module, in order to help to identify abnormal or malicious node behavior.

On the application layer, the received warning messages are first evaluated by the application evaluation module, which uses knowledge from applications, in combination with sensor data provided by the context information module. This verification could enable, for instance, the detection of false icy road warnings, which would be quite implausible when the outside temperature is above 10 degree.

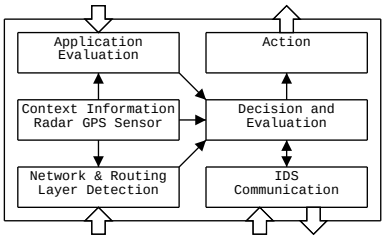

Fig. 3. Modular Cross Layer Architecture

The intrusion detection communication module is used to share the evaluated audit data with other nodes and forward other nodes' audit results to the local decision module. Audit results are either exchanged directly, via multiple hops, or via a temporarily accessible road network infrastructure (e.g. using 802.11p). Especially in case of sparse node density, a potentially accessible road network infrastructure will help to propagate intrusion alerts to follow up cars.

On the other hand, cooperative detection requires some kind of trust between the participating nodes. Hence, we will use dynamic trust establishment between communicating nodes and establish first trust relations during a direct communication phase, to keep them for later usage.

IV. Conclusions and Outlook

Due to fast changing network topology and deployed applications, intrusion detection in VANETs is a challenging task. Classical intrusion detection approaches are not directly usable, thus, we propose a modular cross layer detection system, which makes use of context information from different layers and sources, as well as knowledge from applications.

Compared to other intrusion detection systems, our approach is neither purely based on anomaly based detection, nor on signature based detection. It requires an abstract language to describe abnormal events on different layers, as well as terms to describe dependencies between these events.

In our ongoing research, we are evaluating context supported detection techniques on different layers. Our next steps will concentrate on combining application knowledge and information from location aided routing and addressing. On the one hand, we expect this to detect safety warnings coming from wrong directions and on the other hand, we expect this to help to detect malicious nodes, pretending to be at another place as they really are.

References

[1] W. Franz, R. Eberhardt, and T. Luckenbach, "FleetNet - Internet on the Road," 8th World Congress on Intelligent Transportation Systems, Oct. 2001.

[2] W. Franz, C. Wagner, C. Maihöfer, and H. Hartenstein, "Fleetnet: Platform for inter-vehicle communications," in *Proceedings of the 1st International Workshop on Intelligent Transportation (WIT 2004)*, Mar. 2004.

[3] Y. Zhang and W. Lee, "Intrusion detection in wireless ad-hoc networks," in *Proceedings of the 6th annual international conference on Mobile computing and networking*. ACM Press, 2000, pp. 275–283.

[4] Y. Zhang, W. Lee, and Y.-A. Huang, "Intrusion detection techniques for mobile wireless networks," *Wirel. Netw.*, vol. 9, no. 5, pp. 545–556, 2003.

[5] O. Kachirski and R. Guha, "Effective intrusion detection using multiple sensors in wireless ad hoc networks," in *Proceedings of the 36th Annual Hawaii International Conference on System Sciences (HICSS'03) - Track 2*. IEEE Computer Society, 2003, p. 57.1.

[6] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in *Proceedings of the 6th annual international conference on Mobile computing and networking*. ACM Press, 2000, pp. 255–265.