2011 IEEE Intelligent Vehicles Symposium (IV)
Baden-Baden, Germany, June 5-9, 2011

Entropy-Based Anomaly Detection for In-Vehicle Networks

Michael Müter, Naim Asaj
Daimler AG
Research and Development, GR/PTA
Böblingen, Germany
{michael.mueter|naim.asaj}@daimler.com

***Abstract*— Due to an increased connectivity and seamless integration of information technology into modern vehicles, a trend of research in the automotive domain is the development of holistic IT security concepts. Within the scope of this development, vehicular attack detection is one concept which gains an increased attention, because of its reactive nature that allows to respond to threats during runtime. In this paper we explore the applicability of entropy-based attack detection for in-vehicle networks. We illustrate the crucial aspects for an adaptation of such an approach to the automotive domain. Moreover, we show first exemplary results by applying the approach to measurements derived from a standard vehicle's CAN-Body network.**

I. Introduction

Modern vehicles can comprise up to 70 electronic control units (ECU), which communicate and interact with each other over specialized automotive bus systems, e.g., CAN, MOST, or Flexray. Moreover, recent advances in wireless communication technology led to an introduction of numerous wireless interfaces, such as GSM, 802.11, or Bluetooth, to the vehicular system. In the future, these interfaces can serve as an enabler for new functions, like firmware updates over the air or Car-to-Car communication [12].

However, alongside the benefits of an increased connectivity and functionality comes an increased exposure and vulnerability. Attackers could try to access the automotive network in order to inject messages, manipulate data or access confidential information. For instance, an adversary could inject a malicious packet via a vulnerability in one of the numerous external interfaces which interferes with the normal operation of the vehicle [4]. In the world of desktop computers similar risks are known and have caught increasing attention in recent years. Several measures have been explored in this area which promise to mitigate these threats. But the consideration of these standard measures, e.g., firewalls and virus scanners, is not sufficient enough to provide useful protection for vehicular networks because of their exclusive focus on a preventive approach and limited resources. Additionally, vehicles have a very long life span and are in use for decades in different conditions and locations. To provide an efficient protection, preventive measures only are not sufficient enough over this long period of time.

In this paper, we attempt to go beyond present work by introducing the concept of entropy-based anomaly detection to the area of in-vehicle networks. The approach realizes a reactive concept and serves as an additional layer of protection even when preventive measures failed. Thereby, we show how its self-adapting nature allows an easy adaption to the automotive domain and a convenient extension to new vehicles. We further investigate the main parameters which are crucial for the realization of an information-theoretic intrusion detection concept for the in-vehicle domain. Afterwards, we demonstrate the applicability of our concept by testing it at different attack scenarios on the CAN network of a real vehicle.

II. Related Work

Previous research regarding in-vehicle networks has mainly focused on safety issues [12], more recent activities go beyond and consider IT security aspects as well [16], [19]. Different potential attack scenarios on future automotive systems have been presented [8] as well as the implementations of concrete attacks on the CAN bus [3]. In the world of desktop computers intrusion detection systems (IDS) are one well known countermeasure by now, and different concepts like misuse and anomaly-based detection have been developed. More details and comprehensive IDS surveys can be found in the literature [6], [15].

The first concept for in-vehicle intrusion detection was introduced by Hoppe et al. [4] with a presentation of three selected characteristics as intrusion detection patterns. This includes the recognition of an increased frequency of cyclic CAN messages, the observation of low-level communication characteristics based on typical properties of electric signals on the physical layer, and the identification of obvious misuse of message IDs. Larson et al. [9] introduce an approach to specification-based attack detection for in-vehicle networks, which depicts how to gain a description of the vehicle's normal behavior out of the network protocol and ECU specification based on the CANopen protocol [5]. As illustrated before, this comprises challenges like the achievement of a low rate of false positives and the fact that false alerts can be very costly, as well as the lack of suitable training data [6], [15].

Several recent publications propose anomaly detection as one potential security approach for future automotive systems, but leave the details to future work [7], [19], [13]. At this point, our work attempts to go beyond by taking a first step towards an integrated approach to anomaly detection for in-vehicle networks.

978-1-4577-0891-6/11/$26.00 ©2011 IEEE

III. The Entropy Approach

In-vehicle intrusion detection systems are reactive security components which can monitor the vehicular networks in real-time and respond immediately if a potential threat has been detected. In the Internet world, typical intrusion detection systems like Snort (http://www.snort.org/) are based on signatures of known attacks. Signature-based detection requires regular updates of attack signatures but rewards the user with a high accuracy in detection and a low rate of false-positives. However, due to different reasons like the restriction to known attacks, the limited update possibilities in combination with the long lifetime of vehicles, the anomaly-based detection approach looks more promising for the automotive domain than the signature-based concept [11]. Nevertheless, anomaly-based systems require a definition of the normal behavior of the system and recognize every deviation from this behavior as an attack.

However, one question remains: How exactly can the normal behavior of a vehicular network be defined? This is where an entropy-based approach yields promising results: In this paper, we suggest to measure the entropy of an automotive network and use the result as a specification of the behavior for an intrusion detection system. Generally speaking, entropy is a measure of how much coincidence a given data-set contains. The more coincidence it comprises, the higher the entropy it contains. The entropy of a (finite) sequence of values can be measured without knowing the semantic meaning of all parts of this data. Instead, entropy can be calculated by representing the sequence in a binary form and specifying the portions of the measurement to consider. Consequently, entropy allows an abstract representation of the randomness of this data. In the context of network and Internet systems, the concept of entropy-based intrusion detection has been considered in various publications [10], [2]. However, in this area of application the big disadvantage of the entropy approach is typically its high rate of false positives [6]. This is due to the fact that traffic in standard computer networks can vary a lot and is usually not limited in a strict manner. Neither the type nor the protocol of a packet are generally restricted, arbitrary data content and numerous options are allowed. Moreover, the timing behavior of message can vary strongly and service guarantees are usually at a best-effort level. All these aspects show that the amount of randomness in standard computer networks is fairly high.

Instead, traffic in automotive networks is much more restricted. Every packet in a vehicular CAN network and its possible data content is specified before. The identifier of a CAN message, which determines the destination(s) of a packet, also specifies which kind of payload this message is allowed to comprise in terms of different signals and values. The permitted value range is defined as well as the length of every signal and the packet function. For many messages the exact timing behavior and frequencies are defined as well. Moreover, the number of additional options typical vehicular protocols like CAN offer is very limited. Because of the clear and more restricted specification of traffic in vehicular networks we conclude that the amount of randomness in a standard computer network is much higher than in a vehicular network, or – said differently – the entropy of an automotive network in general is lower. This is the reason why we consider an adaption of the entropy-based approach for intrusion detection to be well-suited and yield a low rate of false-positives in the automotive domain. Most attacks on vehicular networks, like the injection of new packets, the manipulation of the payload of messages, or the omission of packets, e.g., by disconnecting a special ECU or launching a man-in-the-middle attack, will influence the traffic on the bus system and with it the normal system behavior in the network. This change in the normal behavior is reflected by the entropy in the automotive network because every attack that influences the network traffic changes the randomness on the automotive bus system. Therefore, the attacks lead to an increased entropy in the vehicular system, which in general contains a comparatively low entropy as explained before. This raise in entropy can thus be detected by an automotive intrusion detection system and used as an indicator of an attack.

IV. Concept of an Information-Theoretic Detection Approach

In the previous section we explained why an entropy-based detection method for attacks in the automotive domain is a promising and worthwhile approach. This section investigates the different dimensions which are relevant for the general concept of an information-theoretic intrusion detection approach for in-vehicle networks.

A. Data Abstraction Level

The first dimension which influences the results of an information-theoretic anomaly detection approach for in-vehicle networks is the level of data abstraction. In general, various information-theoretic measures can be applied to the input data. However, the selection of the parts of the input data which are relevant and suitable for the detection of anomalies is a non-trivial task. The interpretation of the input-data depends on the selected abstraction level. In our context, different classifiers exist which describe how the input-data is selected and interpreted. We identified three major abstraction levels for the data selection:

1) Binary Level: This level describes the situation that the communication flow in the automotive network is monitored as a binary stream consisting of ones and zeros. The boundaries between messages and fields are not considered and the corresponding delimiters are neglected. At binary level, two different types of classifiers are possible: The *bitwise classifier* considers every single bit in the data stream of the network as a separate event class. The *x-bitwise classifier* considers combinations of x bits of the data stream as an event class.

2) Signal Level: In comparison to protocols like IP, where arbitrary content can be transferred, the payload in automotive bus systems, like CAN, is strictly specified (for details

refer to the book by Etschberger [1]). Generally, CAN is a shared medium which allows every participant to listen on the bus and select relevant messages based on the identifier. Typically, the payload of a CAN message comprises different CAN signals each of which carries the data for a specific function, option or configuration. For instance, different signals with status information, configuration data and sensor values of the Antilock-Braking-System (ABS) could be summarized in the data field of one CAN message. At signal level, the classifier generates one event class for every signal value of a message. It requires exact information about the signals which can be derived from the specification of the vehicular network. For CAN, this is specified in the *CAN-Matrix*.

3) Protocol Level: The highest data abstraction level we consider is based on the protocol specification of the automotive network. For CAN, the protocol defines 12 different fields for data frames of the base format [1]. The classifier at protocol level considers the content per field in the data frame and generates an event class for every field value. However, not all fields of the CAN protocol are suitable for an investigation, e.g., fields like the CRC check. Currently, our investigations focus on two fields: The identifier and the data field. The CAN identifier is a unique value which identifies the data and determines the receiver(s) of the message. The data field contains the payload of a message and can take up to 8 bytes [1].

B. Information-Theoretic Measures

The next dimension we introduce describes the choice of the information-theoretic measure to utilize for detection. In the following, we just give a short definition of these measures, more detailed explanations can be found in various texts on information theory, e.g., the book by Cover and Thomas [18].

1) Conditional Self-Information: The self-information of a message is an information-theoretic measure that describes how much information-content has been transferred with this message [18].
Definition: The *conditional self-information* $I(x|y)$ of a message x with probability $P(x|y)$ under the previous occurrence of y is defined as

$$I(x|y) = \log_a \tfrac{1}{P(x|y)}$$

where the base of the logarithm a specifies the unit of $I(x)$. In the following we assume the unit of $I(x)$ is in bits and set $a = 2$.

2) Entropy: Entropy describes a measure for the uncertainty of a collection of data items and can be calculated as the expected value of the self-information [17].
Definition: Given a set of classes C_X for a data set X, where each data item belongs to a class $x \in C_X$, the *entropy* of X relative to C_X is defined as:

$$H(X) = \sum_{x \in C_X} P(x) log \tfrac{1}{P(x)}$$

where $P(x)$ is the probability of x in X.

3) Relative Entropy: The relative entropy can be used to measure the *distance* between two data sets. As we will see in Sect. V, the distance between individual items of two data sets can be determined by using the definition below without using the sigma sign to sum up all values of the sets.
Definition: For two probability distributions $p(x)$ and $q(x)$, which are defined over the same $x \in C_x$, the *relative entropy* is specified as

$$RelEnt(p/q) = \sum_{x \in C_X} p(x) log \tfrac{p(x)}{q(x)}$$

C. Vehicle Status

Finally, the last dimension we want to discuss is the *vehicle status*. The vehicle status describes the current condition the vehicle is in, meaning if the car is standing or moving, driving forward or backwards, and what position the ignition switch is set to. For instance, the number of messages on the network usually is much lower if the car is standing and the ignition is just turned off. Consequently, the entropy can change depending on these aspects. For a comprehensive investigation all issues related to the vehicular state could be included in a finite state automaton where each state represents one status of the vehicle. Then, each state would require a separate investigation of the impacts on the entropy.

V. Evaluation of Anomaly Detection Concept

After introducing the main aspects an information-theoretic approach of vehicular anomaly detection needs to consider, we continue with a presentation of first experimental results we received by applying the concept to a real vehicle. We start with a description of the test setup and the three attack scenarios. Afterwards we illustrate the results and discuss advantages and drawbacks of the approach.

A. Test-Setup

For the application of the information-theoretic measures introduced in Sect. IV-B, access to the network traffic of a vehicle is required. In our setup, we used a normal serial-production vehicle, which is licensed for road usage, and added a connector to the vehicular network, more precisely, to its CAN-Body network. This network was chosen due to its intermediate impact on safety critical functions [14], which allows realistic attack scenarios without the immediate danger of causing permanent damage in case of test errors, like an activation of the airbag. As an interface we used the CAN-CardXL from Vector Informatics (http://www.vector.com/), which establishes a connection between the CAN-Body connector and a standard laptop; for logging and analysis purposes we used the software CANoe Version 7.0.80 (SP6).

B. Attack-Scenarios

In the following we describe three attack scenarios which we explored to show the usefulness of the approach. All scenarios are based on well-known attacks which have been described in previous research publications.

1) Attack Scenario I - Increased Frequency: In the first attack scenario we simulate an attacker who wishes to disturb the system, e.g., for the manipulation of the hazard lights or the electronic window lift as described by Hoppe and Dittmann [3]. Both attacks have one aspect in common: Due to the topology of the CAN bus they result in an increased frequency of a message type. For the first attack scenario we increase the frequency of the message with the exemplary identifier `3FB`, while the engine is running and the vehicle is standing. The normal cycle time for `3FB` is 100ms, meaning the message appears every 100ms on the CAN-Body network. For the attack, we double the frequency and send another additional message every 100ms.

2) Attack Scenario II - Message Flooding: Usually, communication in automotive networks is real-time or near real-time critical. In addition, certain communication, e.g., in the Chassis- or Powertrain-Domain, is not only time- but safety-critical as well. Therefore, this attack describes a scenario where an adversary tries to attack the availability of a bus system by performing a flooding attack on the CAN bus. The implementation is done with a CAN message containing the most dominant identifier `0x00` and measuring the effects in real-time. Due to the nature of CAN, at the occurrence of a high busload situation with low availability for arbitrary messages, only the most dominant CAN messages should prevail in the network.

3) Attack Scenario III - Plausibility of Interrelated Events: Many events on signal level are interrelated. This means, an event at time *t* directly depends on the event at time *t-1*. This scenario investigates if the disturbance of gradually correlated events can be detected. As an exemplary progression, we monitor the speed signal of a test vehicle for 300 seconds recorded in an urban driving situation. It reaches a maximum velocity of around 60km/h and also comprises brief full-stop situations, e.g., due to traffic lights and other road users. The result is utilized as normal behavior for the anomaly detection model. We assume the attacker tries to disturb the system by injecting selective, spurious speed signals, e.g., to provoke a malfunction of the engine ECU or other devices in the powertrain domain. Compared to the previous scenarios, this setup tries to recognize single spurious packet injections instead of detecting a larger number of spoofed messages.

C. Evaluation

1) Scenario I: When measuring the entropy during normal operation of the vehicle, we received a value of 5.95 bit. The value drops down to 5.64 bit while performing the attack with an additional message every 100ms. The reduction of the entropy can be explained by considering the number of messages with the identifier `3FB`: As the number of messages of this type increases, the "randomness" of the traffic decreases, which leads to a slightly lower entropy.

Although the reduction in entropy allows to recognize the attack, it does not enable us to give more details about the attack. Especially, it does not tell us which type of message, i.e., which identifier, has been disturbed in order to attack the system. Therefore, in the following we analyze the data furthermore to acquire additional information.

As explained in Sect. IV-B, based on the concept of relative entropy we calculate the relative distance $RD_{p|q}(x)$ between two data sets *p* and *q* which are defined over the same identifier $x \in C_x$ by

$$RD_{p|q}(x) = p(x) log \frac{p(x)}{q(x)}.$$

Whereas *q* describes the normal behavior of the system, meaning the normal probability distribution of the CAN messages without executing an attack, *p* shows the empirical values measured when performing the attack scenario. As we consider the identifier of every packet, data abstraction is on *protocol level* (see Sect. IV-A).

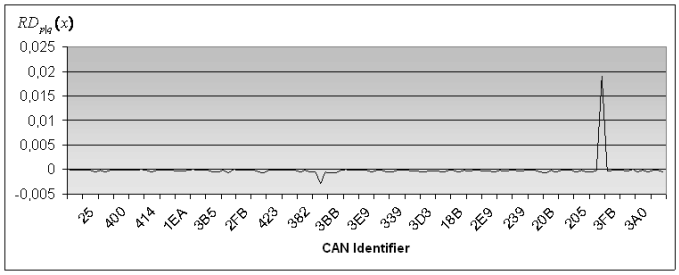


Fig. 1: Deviation between normal behavior and measured data with cyclically injected messages in Scenario I

Fig. 1 shows the results for each identifier *x*, which we received when measuring the described scenario. For most identifiers the distance $RD_{p|q}$ stays close to zero, meaning the empirical probability distribution of the messages measured on the CAN network matches the previously recorded normal behavior. On one point, namely for the identifier `3FB`, the distance strongly increases and the graph shows a peak. If we introduce a reasonable threshold *t* and define every deviation where $RD_{p|q}(x) > t$ as an anomaly, we can use the result for the detection of attacks during runtime.

2) Scenario II: The entire measurement covers a period of 15 seconds. The attack is started after 8 seconds and stays active for a duration of 2 seconds. During this time period, the controller is instructed to inject as many messages with the CAN identifier `0x00` into the network as possible. The

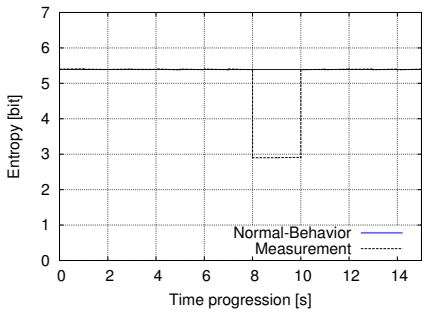
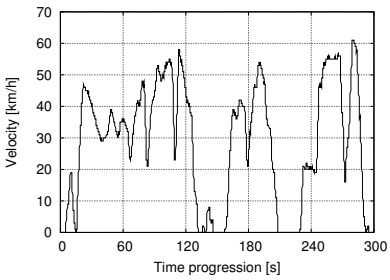
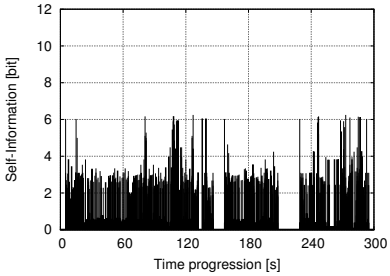


Fig. 2: Entropy of CAN network during flooding attack



(a) Speed progression of the test vehicle



(b) Conditional self-information extracted from the speed progression

Fig. 3: Measurements on test vehicle under urban driving conditions

entropy of the network is monitored over the complete time and the outcome is displayed in Figure 2. The normal ID-based entropy in this scenario is measured as 5.39 bit. As soon as the attack is started after 8 seconds, the entropy sharply drops down by about 48% to a level of approximately 2.82 bit. After two seconds the injections are deactivated, and we can observe that entropy goes back to the previous level immediately. The shift in entropy in this scenario allows an easy recognition of the flooding attack on the CAN bus. The change in entropy reflects the idea of the detection concept: Due to the injected messages the number of identical packets - in this case messages with CAN identifier `0x00` - strongly grows. Consequently, the overall coincidence of traffic in the bus system decreases in contrast to previous values. Therefore, the entropy decreases as well during the attack, and once the injections are stopped it goes back to the normal level.

Usually, the error management of benign CAN devices avoids that single components completely overload a network with messages, e.g., in case of a hardware error, for instance, by setting the device into *error passive* or *bus off* mode [1]. This, however, does not necessarily apply to malicious devices as well because once a component has been attacked or modified by an adversary it may not obey to every step of the CAN protocol any more.

3) Scenario III: In this scenario we probe information about the coherence of events. We investigate how the attack can be detected by utilizing a probability table comprising the coherent speed values. For each velocity *x* of the vehicle at time *t*, the table contains the probability that the previous velocity at time *t-1* was *y*. The table is initialized by a probability unequal but very close to zero, to avoid division by zero errors in computation. Hence, the table comprises $P(x|y)$, meaning the normal behavior of the speed signal and the coherence to the previous values, which we use as a model for the detection of attacks targeting interrelated events.

Accordingly, we consider the speed progression of the given scenario as shown in Fig. 3a and use the probability table to extract $P(x|y)$ for every point of the graph. The output is used to compute the conditional self-information and is presented in Fig. 3b. It can be seen that the self-information realizes values from 0 up to a maximum of around 6 bit. Different peaks can be observed in the distribution, which especially occur when the driving behavior shows a strong deviation to the previously seen values. Nevertheless, the maximum of 6.17 bit is never exceeded, even when the vehicle is accelerating rapidly or making a quick full-stop the self-information does not swell above this limit.

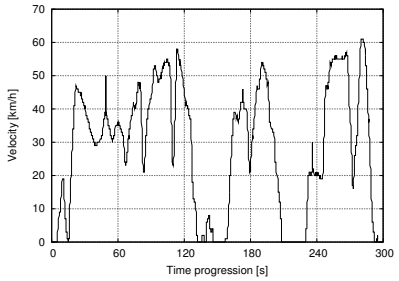
Nr.	Injection Time	Injected Value	Actual Vehicle Speed
1	49s	50km/h	39km/h
2	120s	45km/h	44km/h
3	173s	46km/h	42km/h
4	236s	30km/h	22km/h

TABLE I: Spoofed messages in attack scenario III

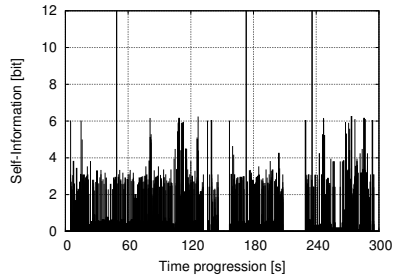
In the next step, this normal behavior is compared to the results achieved by observing the system during the attack. Therefore, we inject four spurious signals into the system, as listed in Table I. The corresponding speed progression is shown in Figure 4a and reflects the spoofed values. All injected values besides one show a reasonable deviation from the vehicle's actual speed. This depicts the attacker's motivation to seriously disturb the system and is based on the fact that if a spoofed value that sufficiently deviates from the vehicle's actual speed is processed by an ECU, the probability to cause serious malfunctions is significantly higher than just a slight deviation would provoke.

It can be seen that most of the time the self-information stays below 6 bit. Figure 4b displays the conditional self-information for this scenario during attack. We recognize three major peaks at the time points when the spoofed speed values number one, three, and four were injected into the system. Obviously, this is caused by the low probability the coherence of messages during the attack has in comparison to the normal behavior. At 120s, Figure 4b does not show any noticeable difference to the normal behavior. Evidently, the spoofed signal with a deviation of only 1 km/h cannot be recognized by the presented means, as it was presumed, because the deviation is part of the normal system behavior and can therefore not be distinguished from malicious activity. We did not determine the particular boundary at which a detection becomes impossible, due to the fact that the exact value of this threshold can depend on numerous different options of a certain scenario, such as the type and model of car, the observed bus system, the assumed normal behavior, etc., and would therefore not allow to draw reliable

and constructive conclusions. In summary, we conclude that once the data abstraction level is changed from protocol to signal level, the additional knowledge about the individual content of a CAN message in form of the particular signals comprised allows further detection and can be utilized to achieve a recognition of spurious speed values in the given scenario. Nevertheless, incorrect data that adheres to the normal behavior cannot be recognized by the introduced means, and indicates the limitations of the approach.



(a) Speed progression including spoofed messages



(b) Conditional self-information extracted from the speed progression during attack

Fig. 4: Measurements on test vehicle during attack

VI. Conclusion

In this paper we introduced the concept of entropy-based attack detection for in-vehicle networks. We presented a set of different parameters and dimensions which are of crucial importance for a deployment of such a technology. The evaluation of diverse attack scenarios has shown that deviations from the normal behavior of in-vehicle networks can successfully be identified by an information-theoretic detection approach. Currently, our measurements showed limitations for the recognition of small-scale attacks which could be part of the normal vehicle or user behavior. The approach includes several advantages with respect to a practical deployment in the automotive industry. At first, it only requires a record of in-vehicle network traffic as input for the normal behavior. No details about the specification of allowed messages, cycle times, header sizes, etc. are required, as they are typically provided by the CAN matrix of a bus system. Instead of requiring all this knowledge as well as individual configurations of thresholds for all these specific characteristics, the presented approach has the ability of self-adjustment based on the normal behavior deduced from its given input. Moreover, in combination with the threshold-based detection method, this approach reduces the memory and hardware requirements for a realization and implementation of such a concept in the embedded automotive systems. Besides, it allows an easy extension and adaption to new vehicle models and versions, just by incorporating an updated version of the normal behavior based on a new record of benign in-vehicle network traffic.

References

[1] K. Etschberger, *Controller Area Network - Basics, Protocols, Chips and Applications*. IXXAT Automation, October 2001.

[2] Y. Gu, A. McCallum, and D. Towsley, "Detecting anomalies in network traffic using maximum entropy estimation," in *Proceedings of the 5th ACM SIGCOMM conference on Internet Measurement*, 2005.

[3] T. Hoppe and J. Dittmann, "Sniffing/Replay Attacks on CAN Buses: A Simulated Attack on the Electric Window Lift Classified using an Adapted CERT Taxonomy," in *Proceedings of the 2nd Workshop on Embedded Systems Security (WESS 2007)*, 2007.

[4] T. Hoppe, S. Kiltz, and J. Dittmann, "Security Threats to Automotive CAN Networks - Practical Examples and Selected Short-Term Countermeasures," in *Proceedings of the 27th International Conference SAFECOMP 2008*, Newcastle, United Kingdom, September 2008.

[5] C. in Automation (CiA) e.V., "CANopen application layer and communication profile, CiA draft standard 3.01," January 2005.

[6] R. A. Kemmerer and G. Vigna, " Intrusion detection: A brief history and overview," *Computer*, vol. 35, no. 4, pp. 27–30, April 2002.

[7] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, and S. Savage, "Experimental Security Analysis of a Modern Automobile," in *IEEE Symposium on Security and Privacy*, 2010.

[8] A. Lang, J. Dittmann, S. Kiltz, and T. Hoppe, "Future Perspectives: The Car and its IP-Address - A Potential Safety and Security Risk Assessment," in *Proceedings of the 26th International Conference SAFECOMP*. Springer, 2007.

[9] U. E. Larson, D. K. Nilsson, and E. Jonsson, "An Approach to Specification-based Attack Detection for In-Vehicle Networks," in *Proceedings of the 20008 Intelligent Vehicles Symposium*, 2008.

[10] W. Lee and D. Xiang, "Information-theoretic measures for anomaly detection," in *Proceedings of the 2001 IEEE Symposium on Security and Privacy*, 2001.

[11] M. Müter, A. Groll, and F. Freiling, "A Structured Approach to Anomaly Detection for In-Vehicle Networks," in *Proceedings of the Sixth International Conference on Information Assurance (IAS 2010)*, Atlanta/Georgia, USA, August 2010.

[12] N. Navet, Y. Song, F. Simonot-Lion, and C. Wilwert, "Trends in Automotive Communication Systems," *Proc. of the IEEE*, vol. 93, no. 6, p. 1204–1223, 2005.

[13] D. K. Nilsson and U. E. Larson, "Combining Physical and Digital Evidence in Vehicle Environments," in *SADFE '08: Proceedings of the 2008 Third International Workshop on Systematic Approaches to Digital Forensic Engineering*. Washington, DC, USA: IEEE Computer Society, 2008, pp. 10–14.

[14] ——, "Simulated attacks on CAN buses: Vehicle Virus," in *Proceedings of the First International Conference on Forensic Applications and Techniques in Telecommunications, Information and Multimedia*, Adelaide, Australia, 2008.

[15] A. Qayyum, M. Islam, and M. Jamil, "Taxonomy of statistical based anomaly detection techniques for intrusion detection," in *Proceedings of the IEEE Symposium on Emerging Technologies*, 2005.

[16] I. Rouf, R. Miller, H. Mustafa, T. Taylor, S. Oh, W. Xu, M. Gruteser, W. Trappe, , and I. Seskar, "Security and Privacy Vulnerabilities of In-Car Wireless Networks: A Tire Pressure Monitoring System Case Study," in *Proceedings of the 19th USENIX Security Symposium*, Washington DC, USA, August 2010.

[17] C. E. Shannon and W. Weaver, "The Mathematical Theory of Communication," in *University of Illinois Press*, 1949.

[18] J. A. T. Thomas M. Cover, *Elements of Information Theory*. Wiley, 1991.

[19] M. Wolf, *Security Engineering for Vehicular IT Systems - Improving the Trustworthiness and Dependability of Automotive IT Applications*. Vieweg + Teubner, 2009.