International Journal of Advances in Computer Networks and Its Security– IJCNS
Volume 4: Issue 2 *[ISSN: 2250-3757]*
Publication Date : 25 June 2014

A Physical Measurement-Based Sybil Nodes Detection Mechanism in VANETs

[Dongxu Jin, Fei Shi, and JooSeok Song]

***Abstract*—In traffic safety applications of Vehicular Ad-hoc Networks (VANETs), security is a very important issue. Sybil attack is a particular attack where the attacker illegitimately claims multiple identities. In the past, several approaches have been proposed to solve this problem. They are categorized into PKI-based, infrastructure-based, observer-based, and resource-testing-based schemes. In this paper, existing protocols are analyzed, and a novel scheme for detecting the Sybil nodes in VANETs is presented, reducing the effect of a Sybil attack. The proposed Sybil nodes-detection scheme, Physical Measurement-Based Sybil Nodes Detection Mechanism in VANETs (PMSD), takes advantage of physical measurements of the beacon message instead of key-based materials, which not only solves the Sybil attack problem, but also reduces the overhead of detection. The proposed scheme has no fixed infrastructure, which makes it easier to implement. The simulation results show a 95% detection rate of Sybil nodes, with only about a 4% error rate.**

***Keywords*—VANETs, Sybil Attack, Physical Measurement, Security**

I. Introduction

Vehicular ad-hoc networks (VANETs) are wireless communication networks that do not require fixed infrastructures; they provide a novel networking pattern for supporting cooperative driving applications on the road. VANETs have several characteristics: (a) nodes are constrained by the road and have constrained speed patterns, (b) network topology changes frequently, (c) communication conditions vary due to time and space (e.g., signals can be blocked by buildings), (d) nodes do not have significant power constraints [1].

VANETs have many applications [2], such as vehicle-to-vehicle communication, vehicle-to-infrastructure communication, file sharing, and real-time traffic information sharing (such as jams and blocked streets), etc. VANETs face all the security threats of a wireless network [3, 4, 5]. Security issues in VANETs are critical because they are vulnerable to network attacks, and attacks are dangerous to vehicle drivers as the result of influenced network functionality. A security system should ensure that a transmission is from a trusted source to an authorized receiver and also should balance security and privacy.

Dongxu Jin, Shi Fei, Jooseok Song

Dept. of computer science, Yonsei Univ.
Korea

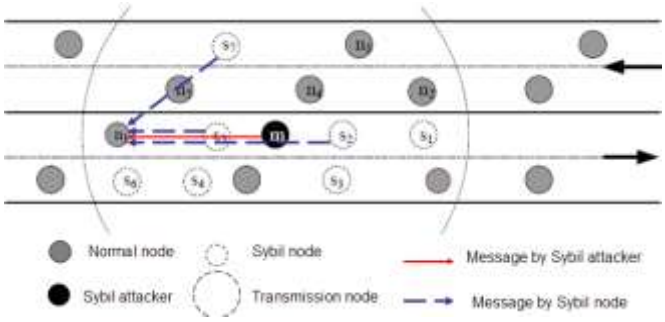

Figure 1. Sybil attack in a VANET

There are various kinds of attacks in VANETs. In this paper, we focus on one important attack called the Sybil attack. A Sybil attack [6] can occur when a network has no centralized authority. In this attack, a vehicle forges multiple vehicle identities, which can be used to launch any kind of attack on the VANETs. Fake identities also create an illusion that there are additional vehicles on the road. As Fig. 1 shows, the node forging multiple vehicle identities is called the Sybil attacker, and the nodes with forged identities are called Sybil nodes. The normal node n1 thinks the Sybil nodes s7, s2 really exist and are located where they claimed. The node n1 may routes messages through those Sybil nodes. Consequently, any type of attack can be launched after faking the positions or identities in the network, such as providing bogus information, replying or dropping packets, etc. This degrades the functionality and QoS of the VANETs.

Many different mechanisms have been proposed to prevent or reduce the effects of a Sybil attack. They can be categorized into PKI-based, infrastructure-based, resource-testing-based, and observer-based. PKI-based, infrastructure-based and observer-based mechanisms need a central authority that is not always available in VANETs. The resource-testing-based mechanisms are based on the assumption that every node is equipped with limited computational resources. But an attacker may be equipped with more computational resources compared to normal nodes.

The objective of this paper is to detect the Sybil nodes without the assistance of a centralized infrastructure because a road-side unit cannot cover the whole VANET area. It is easier to implement a protocol in VANETs if it does not require a centralized infrastructure.

In this paper, we propose a novel Sybil nodes detection scheme called the Physical Measurement-Based Sybil Nodes Detection Mechanism (PMSD), which uses physical measurement of message transmission to detect Sybil nodes in 802.11p-based VANETs. As shown in Fig. 1, the node m is a Sybil attacker, and nodes s1 to s7 are all Sybil nodes. The

proposed PMSD scheme takes advantage of the transmitted message's physical measurement, which cannot be forged by a Sybil attacker. Further, PMSD does not require the assistance of road-side units. The Time Difference of Arrival (TDoA) technique is used to locate the source of the message. If the location is different from the claimed location included in the beacon message, then the node will be judged as a Sybil node. In this way, a normal node can detect a Sybil node and can avoid the effect of Sybil attack.

This paper is organized as follows: Section 2 reviews the Sybil attack and related work on the Sybil node detection mechanisms. Section 3 presents a detailed description of our scheme and how it works. Section 4 is the simulation and security analysis, and finally Section 5 gives the conclusion of this paper and suggests future works.

II. Related Work

The Sybil attack, first discussed by Douseur [6], is a serious threat to VANETs as it reduces the functionality and QoS. In this attack, a Sybil attacker sends messages with multiple identities to other nodes. The node forging the multiple identities of the other nodes is called a Sybil attacker, and the nodes whose identities are forged by a Sybil attacker are called Sybil nodes. All other kinds of attacks can then be launched in a network that is under a Sybil attack. Sybil attack gives an illusion of a traffic jam or accident so that other vehicles will change their route and then the attacker will get the benefit of quick passing. A Sybil attacker can also inject false messages into the networks via Sybil nodes.

An attack through Sybil nodes can maliciously affect the normal functionalities of a network [7, 8, 9]. These functionalities include 1) Data aggregation: Through Sybil nodes, a Sybil attacker can send numerous data to change the outcome of data aggregation. 2) Fair resource allocation: when the resources are allocated equally to every node, due to the presence of Sybil nodes, a Sybil attacker is allocated more resources than normal nodes. This can lead to a Deny of Service attack to normal node. 3) Routing: In multi-path routing protocols, disjoint paths are implemented. The presence of Sybil nodes on these paths can interfere with the routing. Geographic routing is more severely affected as a Sybil attacker with different identities can appear in more than one place at the same time. It is easy for the Sybil attacker to launch wormhole, black hole, and gray hole attacks. 4) Voting: A Sybil attacker can vote many times through its Sybil nodes while normal nodes can only vote once. If the attacker creates enough Sybil nodes participating in a vote to determine a misbehaving node, then a legitimate and well-behaved node can be eliminated from the network. 5) Misbehavior detection: An Sybil attacker can impede the detection of a misbehaving node by spreading the blame to the Sybil nodes. The detection uses multiple observers to locate a misbehaving node, the attacker can escape from the detection by using different node identities at different time. Even if some Sybil nodes are detected and excluded from the network, the Sybil attacker still use other identities to continue the attack [10, 11].

For the prevention and detection of Sybil attacks, a trust mode is established among participating nodes [12]. The major challenge is that the receiving node needs to ensure the authenticity and trustworthiness of the message source before reacting to it. It assumes that every node in VANETs is equipped with trust system. There are two kinds of trust establishment: (1) based on the static infrastructure and (2) based on the self-organized dynamic establishment of trust. Trust based on static infrastructure is more efficient than dynamic establishment. The only concern is the unavailability of a fixed infrastructure in some locations. If all the nodes establish trust with other nodes in the VANETs, the probability of a Sybil attack can be mitigated.

Digital signatures and certificate-based systems are the most popular techniques for trust establishment [13, 14]. In VANETs alert messages of the traffic related application are not planned to be confidential so they do not need privacy. Alert messages require authentication but not encryption. Sets of public-private key pairs are assigned to vehicles for their messages' signatures and authenticating themselves to the receivers. Each message contains a digital signature for authentication. PKI is the most used self-trust management technique. Due to liability issues, PKI cannot be implemented in VANETs. Instead, a centralized authority is required to issue digital certificates.

In a certificate-based system, a node's identity can be revealed to any other nodes when it communicates with them [14, 15]. In [16, 17], privacy preservation using pseudonyms is proposed. These pseudonyms do not establish anonymity but protect privacy. Public keys in VANETs need to be changed periodically. This change is performed by some trusted third party which also grants pseudonyms. The association between pseudonyms and node identity is known only by the trusted third party. This mechanism is difficult to implement in VANETs because of the characteristics of high node mobility and frequently changed dynamic topology. Matching pseudonyms to a vehicle identity at a specific time requires accurate synchronization.

The approach in [18] provided privacy and Sybil-freeness without requiring continuous availability of the centralized authority (CA). Users computed pseudonyms from cryptographic identities. It was assumed that the initial identity domain was Sybil-free, and that this Sybil-freeness could be propagated to other identity domains without continuous availability of a centralized authority. The CA was only needed for the initial setup phase of a Sybil-free domain. In the beginning, users register with the CA and gain a membership certificate. With the membership certificate, each user then creates a self-certified pseudonym for every identity domain. These pseudonyms are only valid in the domains where they were created. Pseudonyms for different identity domains were unlinkable, which means Sybil attackers cannot identify the relationship between two pseudonyms generated by the same user in different identity domains. This scheme only requires the CA in the beginning stage, and after that the Sybil-freeness is propagated from one domain to other domains. But in VANETs either the CA or the initial Sybil-free domain is hart to guarantee.

In [19] resource testing-based Sybil attack detection in VANETs was proposed. This assumed that the vehicle attacker is equipped with limited computation resources. A typical puzzle is given to all the nodes in the network for testing their computational resources. The testing message is spread in a vehicle-to-vehicle manner. If the resources of a single node are used to simulate multiple nodes, then the node is resource-constrained and can not reply in time. In this paper, the resource testing approach is not suitable because we assume an attacker have more computational resources compared with normal nodes. Another problem is that this technique may cause network congestion because multiple requests/replies are used to identify the nodes. The network congestion and long delay is very dangerous to drivers in safety related traffic application in VANETs.

III. Proposed Scheme

In this section, we present an overview of the proposed PMSD scheme. First, the physical measurements are introduced and analyzed. Next, the most suitable physical measurement element is chosen to detect the Sybil node.

The continuous availability of a CA is difficult in VANETs. And Sybil attack is one kind of inside attack where the Sybil attacker has all the security-related information. Therefore, it is better to use physical measurement of the message transmission, which is only related to the hardware and physical environment. The physical measurement cannot be forged by the attacker. These physical measurements include received signal strength indicator (RSSI), angle of arrival (AOA), and time of arrival (TOA). Using these techniques, the location of the sender can be determined and compared with the claimed location: if they do not match, then the node is a Sybil node.

The RSSI-based mechanism is based on the propagation model formula 1

$$P(d)[dBm] = P(d_0)[dBm] - 10 \cdot n \cdot \log(d/d0) - X_\sigma \quad (1)$$

Here P(d) stands for the RSSI received at the receiver, d is the distance between the receiver and the sender, P(d0) stands for the transmission power, n is the proportional factor standing for the proportion between the transmission distance and transmission attenuation, $X\sigma$ is a Gaussian profile random variable whose mean is 0, and d0 is the standard transmission range. However, as mentioned previously, the Sybil attacker also can use formula 1 to calculate how much transmission power it should use to mimic other nodes. Hence, RSSI is not a suitable physical measurement element for Sybil node detection in VANETs.

The Angle of Arrival (AoA) technique locates the source by the angle of an incoming message, based on which sensors receive the signals. Geometry is used to estimate the location from the intersection of a radial line to each sensor, as illustrated in Fig. 2. In a two-dimensional plane, at least two receiving sensors are required for location estimation.

To deploy AoA mechanism, mechanically-agile directional antennas must be deployed at the receiving sensors. The process of identifying the signal arrival angle is as follows: the

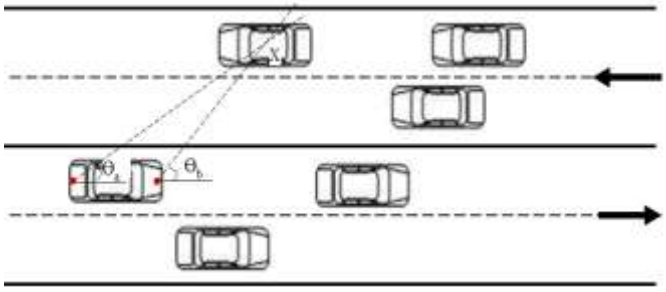

Figure 2. Angle of Arrival

antenna whirls to all directions and compares the collected RSSI then it finds the direction with the highest signal strength. This direction is the signal arrival angle. The position of the message source is determined with the AoA technology by the intersection of the radial line of the angle Θa and Θb. However, in VANETs, directional antennas are not time efficient. Mechanically-agile directional antennas require a continuous incoming signal to identify the signal arrival angle, but the beacon transmitted only for microseconds. Consequently, AoA is also not a suitable physical measurement for detecting a Sybil node in VANETs.

The Time of Arrival (TOA) method is based on the precise measurement of the arrival time of a signal transmitted from a node to several receiving sensors. It requires the timestamps in the beacon message and whole network synchronization. However, timestamps can be forged by a Sybil attacker, so Time Difference of Arrival (TDOA) is used to overcome this problem. TDoA techniques use relative time measurements at each receiving sensor rather than absolute time measurements. As a result, TDoA does not require time synchronization of the whole network, and timestamps are not required in the beacon message. With TDoA, a transmission with an unknown starting time is received by several receiving sensors, requiring only synchronization of the receiver times then the location of the sender can be located. Since the TDoA does not require a time period of continuous message transmission as in AoA to find the signal arrival angle, it is the most suitable physical measurement for finding Sybil nodes in VANETs.

In this approach, at least three time-synchronized receiving sensors are required. The time synchronization among these three receiving sensors is easy to achieve as they are equipped in the same vehicle.

In Fig. 3, assume that, when node X transmits a message, this message arrives at receiving sensor A at time T_A and at receiving sensor B at time T_B. The coordinates of sensors A, B, C are (xa, ya), (xb,yb), (xc,yc), respectively, where source X's coordinates are (x, y). The time difference of arrival for this message is calculated between the locations of sensors B and A as the positive constant Δt:

$$TDoA_{B-A} = | T_B - T_A | = \Delta t \quad (2)$$

The value of TDoA can be used to construct a hyperbola with foci at the locations of both receiving sensors A and B. This hyperbola represents the locus of all the points in the two-dimensional plane, the difference of whose distances from the two foci is equal to Δt×c meters. By excluding the negative

time period, which is unrealistic in real life, one curve of the hyperbola is eliminated. Mathematically, this represents all possible locations of node X such that:

$$| D_{XB}| - |D_{XA}| = \sqrt{(x_b - x)^2 + (y_b - y)^2} - \sqrt{(x_a - x)^2 + (y_a - y)^2} = \Delta t \times c \quad (3)$$

The probable location of the source node X can then be represented as a point along this hyperbola. To further resolve the location of node X, a third receiving sensor at location C is used to calculate the message time difference of arrival between sensors C and A:

$$TDoA_{C-A} = | T_C - T_A | = \Delta t' \quad (4)$$

Knowledge of constant Δt' allows for the construction of a second hyperbola representing the locus of all the points in the two-dimensional plane, the difference of whose distances from the two foci (that is, the two receiving sensors A and C) is equal to $\Delta t' \times c$ meters. Mathematically, this can be seen as representing all possible locations of mobile device X such that:

$$| D_{XC}| - |D_{XA}| = \sqrt{(x_c - x)^2 + (y_c - y)^2} - \sqrt{(x_a - x)^2 + (y_a - y)^2} = \Delta t' \times c \quad (5)$$

Fig. 3 illustrates how the intersection of the two hyperbolas $TDoA_{C-A}$ and $TDoA_{B-A}$ is used to locate the position of source node X.

If formula 3 and formula 5 have more than one intersection point, sensor B and sensor C can be used to create another formula. Based on that formula, a unique intersection can be found to represent location source node X. All these lead up to that TDoA is the most suitable physical measurement for locating the source node from a VANET message.

The total work flow of PMSD is as follows. We assume a vehicle knows its own location from the GPS locating system and it equips three time synchronized radio receivers. First, each node periodically exchange beacon message which include its location, speed, and ID. After receiving the beacon message, based on the different receiving timestamps from three radio receiving sensors, receiving node uses the TDoA technique and inputs the receiving timestamps into the formula (2) to formula (5) introduced earlier. By the outcomes of the equations, the node locates the source node. When the beacon-claimed location is different from the receiver-calculated location, the sender is judged to be a Sybil node by the receiver itself. The node put the source node into the black list and rejects the communication from it.

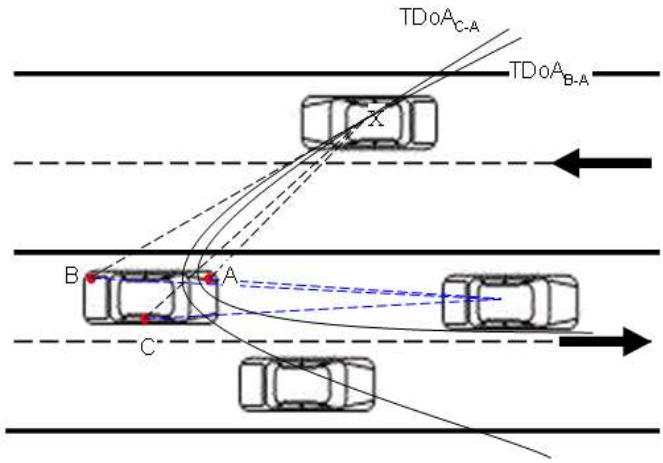

Figure 3. Time Difference of Arrival

IV. Simulation and Security Analysis

In this section, we evaluate the performance of the proposed scheme. Visual C++ is used for simulation and evaluation. Table 1 shows the simulation environment.

TABLE I. SIMULATION PARAMETERS

Transmission range	200 meters
Period of location exchange	1 second
Number of normal vehicles	200
Speed of Vehicles	24 ~ 60 miles per hour
Length of the road	3 kilometers
Number of Sybil attackers	10
Number of Sybil nodes	50 ~ 100
Size of vehicle	1.8 meter × 5.0 meter

Vehicles change their locations every second. A vehicle that violates a traffic rule is not considered. The simulation environment is a 3-kilometer-long highway with two lanes in each direction. A test vehicle drives from one end of the highway to the other end and receives all the beacon messages sent by both normal nodes and Sybil attackers. The test vehicle judges those nodes whose calculated locations are different from the locations claimed in the beacon messages as Sybil nodes. Based on the correctness of the judgment of the test vehicle, the proposed scheme PMSD is evaluated.

As Fig. 4 shows, the Sybil nodes detection rate is greater than 95%, and the error rate is less then 4%. Here the error rate includes both judging Sybil nodes as normal nodes and judging normal nodes as Sybil nodes. This is because the inaccuracy of the GPS. Even the node reports its GPS location,

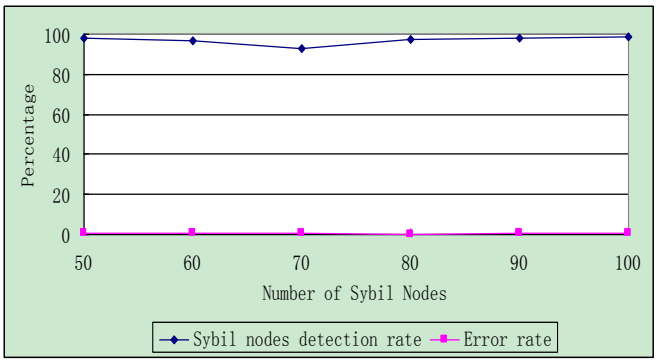

Figure. 4 Detection ratio

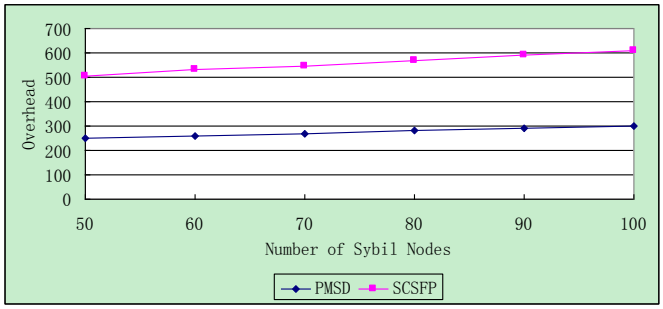

Figure. 5 Total overhead

the actual location is different. In this situation the normal node is judged as Sybil node. With the TDoA, the Sybil nodes can be detected efficiently and correctly. The proposed PMSD scheme locates the message sender and makes the decision. The decision is not affected by the Sybil attacker or the Sybil nodes. Thus, it has a very high detection rate. The result shows that the detection ratio is relatively low when there are 70 Sybil nodes because the original location of the Sybil attacker is close to the forged location of Sybil node. In this situation, it is difficult to find out the Sybil node.

As Fig. 5 shows, the PMSD has lower overhead than the SCSFP. This is because the PMSD detects the Sybil nodes by physical measurement of the beacon message. The detection is based on the received beacon message and does not require extra message exchanges such as a challenge, response between vehicles, or key materials exchange between the vehicle and RSU. Thus, the overhead is less than other schemes. Also, the PMSD is easy to implement as it does not rely on a centralized infrastructure.

v. Conclusion

In this paper, we analyzed existing Sybil node detection protocols in VANETs and presented their shortcomings. Based on this, we proposed a novel Sybil node detection mechanism, PMSD. By taking advantage of physical measurement of the message instead of a key-based mechanism, the proposed PMSD detection mechanism not only solves the Sybil node detection problem, but also reduces the overhead comparing with previous scheme. And the PMSD is infrastructureless which makes it easy to implement. Our simulation results show that, with PMSD, 95% of the Sybil nodes are detected, with only about a 4% error rate. Thus, PMSD can efficiently detect Sybil attacks. PMSD is a passive mechanism to detect Sybil nodes; it does not cause any extra overhead. In the future, more realistic situation will be studied. We will explore the influence of traffic-flow theory and the safe distance on the PMSD which may improve the outcome of the PMSD furthermore. The proposed mechanism is simulated in the two-dimensional environment and suitable for highway situations for now. More complicated scenario will be studied and simulated in the future. We also work on how to reduce the number of receivers as three receivers for each vehicle cause extra expense.

Acknowledgment

This research was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education, Science and Technology (2012R1A1B3004161).

References

[1] Jie Luo, Xinxing Gu, Tong Zhao, Wei Yan, A Mobile Infrastructure Based VANET Routing Protocol in the Urban Environment, Communications and Mobile Computing (CMC), 2010 International Conference April 2010.

[2] Teruhiko Teraoka, Organization and exploration of heterogeneous personal data collected in daily life, Human-centric Computing and Information Sciences, DOI: 10.1186/2192-1962-2-1, 2012.

[3] Y. Qian and N. Moayeri, Design secure and application-oriented VANETs. IEEE VTC2008- Spring, May 11-14, 2008.

[4] K. P, T. Nowey, and C. Mletzko, Towards a security architecture for vehicular ad hoc networks. The First International Conference on Availability, Reliability and Security (ARES), April 2006.

[5] T. Leinmuller, E. Schoch, and C. Maihofer, Security requirements and solutions concepts in vehicular ad hoc networks. Fourth Annual Conference onWireless on Demand Network Systems and Services, 2007.

[6] J. R. Douceur, The Sybil attack. The International Workshop on Peer to Peer Systems, March 2002, pp. 251-260.

[7] S. S. Manvi and M. S. Kakkasageri, Issues in mobile ad hoc networks for vehicular communications, IETE Technical Review 25(2), 59-72, 2008.

[8] M. L. Sichitiu and M. Kihl, Inter-vehicle communication systems: A survey, Communications Surveys & Tutorials, IEEE, 10(2), 88-105, Second Quarter 2008.

[9] D. Jiang and L. Delgrossi, IEEE 802.11p:Towards an international standard for wireless access in vehicular environments. In IEEE Vehicular Technology Conference, VTC Spring 2008, pp. 2036-2040.

[10] P. Papadimitratos, V. Gligor, and J.-P. Hubaux, Securing vehicular communications-assumptions, requirements, and principles. The Workshop on Embedded Security on Cars (ESCAR) 2006, November 2006.

[11] A. Aijaz, B. Bochow, F. Dtzer, A. Festag, M.Gerlach, R. Kroh, andT. Leinmuller, Attacks on inter-vehicle communication systems and analysis. The 3rd international Workshop on Intelligent Transportation (WIT), March 2006.

[12] P.Wex, J. Breuer, A. Held, and T. Leinmller, Trust issues for vehicular ad hoc networks. In 67th IEEE Vehicular Technology Conference (VTC2008-Spring), 2008.

[13] M. Raya and J.-P. Hubaux, Securing vehicular ad hoc networks. Journal of Computer Security, 15(1),39-68, 2007.

[14] A. Khalili, J. Katz, and W. Arbaugh, Toward secure key distribution in truly ad-hoc networks. The IEEEWorkshop on Security and Assurance in Ad hoc Networks, in Conjunction with the 2003 International Symposium on Applications and the Internet, January 28, 2003.

[15] L. A. Martucci, M. Kohlweiss, C. Anderson, A. Panchenko, Self-certified Sybil-free pseudonyms. In WiSec08: The First ACM Conference on Wireless Network Security, ACM Press, 2008, pp. 154 - 159.

[16] J.-P. Hubaux, S. Capkun, and J. Luo, The security and privacy of smart vehicles, IEEE Security and Privacy, 4(3), 49-55, 2004.

[17] M. Raya, P. Papadimitratos, and J.-P. Hubaux, Secure vehicular communications, IEEE Wireless Communications Magazine, 13(5), 8-15, 2006.

[18] P. Papadimitratos, L. Buttyan, J.-P. Hubaux, F. Kargl, A. Kung, and M. Raya, Architecture for secure and private vehicular communications. The 7th International Conference on ITSTelecommunications, June 2007.

[19] B. N. Levine, C. Shields, and N. B. Margolin, A survey of solutions to the Sybil attack. Tech report 2006-052, 2006.