

## A Survey of Existing Approaches for Secure Ad Hoc Routing and Their Applicability to VANETS

Version 1.1  
June 2, 2006

Emanuel Fonseca\* and Andreas Festag

NEC Deutschland GmbH  
{fonseca|festag}@netlab.nec.de

**Abstract.** Vehicular ad hoc networks (VANETs) are the technical basis of an envisioned Intelligent transportation system. They offer a wide range of applications improving road safety and driving comfort. Since VANET applications affect safety-of-life, data security in a vehicular system is mandatory. The unique characteristics of VANETs compared to conventional mobile ad hoc networks and sensor networks pose particular challenges for a security solution for vehicular environment. For secure routing a number of approaches exist that have been designed for different environments and security objectives, mostly extending well-known ad hoc routing protocols. This report systematically reviews the existing solutions and describes them on a comparable level of abstraction. Then, the report compares the solutions with respect to applied security mechanisms and performance criteria. Finally, it analyzes whether the features of the selected approaches meet VANETs requirements.

From a high-level perspective the main security objectives (authentication, integrity, potentially non-repudiation) of the reviewed proposals fit well to the potential requirements of secure VANET routing. Since future VANET routing will likely be based on a specific routing protocol that utilizes positions of forwarding, additional security countermeasures are needed. These include mechanisms to ensure location privacy, to protect beaconing and location service as part of the routing protocol, and to prevent specific attacks that exploit the positions carried in data packets. These aspects necessitate the design of a unique security solution for VANETs. Nevertheless, it can also be concluded from analysis of the VANET characteristics that some aspects aid a security solution, such as less power and processing constraints, central registrations and periodic technical inspections, as well as existing law enforcement procedures.<sup>1</sup>

---

\* Also with Universidade de Aveiro, Instituto Telecomunicações, Portugal.

<sup>1</sup> E. Fonseca and A. Festag acknowledge the support of the German Ministry of Education and Research (BMB+F) for the project 'NoW – Network on Wheels' under contract number 01AK064F.

## 1 Introduction

Nowadays, transportation systems are a major problem of our society, lots of lives, money, and time are lost due to their inefficiency. The effort to develop and improve transportation systems – to make them more *intelligent* – is globally known as *Intelligent Transportation Systems (ITS)*.

Vehicular Ad hoc NETWORKS (VANET) are the technical basis of ITS, for which first draft standards are coming up [1–6]. They enable vehicles to actively communicate among each other and to better perceive the traffic situation in their vicinity, like accidents and traffic jams. VANETs allow vehicles to avoid problems, either by taking any desired action or by alerting the driver. Besides the road safety enhancements that VANETs will bring, they also open doors to many applications to enhance the driving and traveling comfort, like Internet access from a car.

With such an important and huge network, it is worth thinking about potential vulnerabilities as a target of potential attackers. A successful attack to VANETs might have catastrophic results, such as the loss of lives. Therefore, making a vehicular communication network secure is not an extension but a primary concern. So far, only a few research efforts have addressed VANET security issues, focusing either on identification of their challenges, or proposing secure VANET architectures [7–12]. Likewise, surveys about security approaches for mobile ad hoc networks in general (e.g. [13, 14]) do not address the specific characteristics of VANETs.

This report focuses on routing attacks in VANETs, which can be performed in several ways and with different objectives. The attacks fall into the following main categories: *i*) spoofed, altered, or replayed routing information, *ii*) selective forwarding, *iii*) sinkhole attacks, *iv*) wormholes, *v*) acknowledgment spoofing. Some of the attacks can be performed by dropping, changing, or injecting packets into the network, others are executed by changing the real topology of the network. It is worth noting that security at routing level is very important, because if the routing is compromised, other protocol layers on top of the network layer are also compromised.

This survey gives an overview of existing approaches that attempt to provide some routing security to conventional mobile ad hoc networks. The existing approaches are systematically described, classified, and compared with respect to their security objectives, the applied security mechanisms, and performance criteria. We also analyze whether the existing approaches can be applied to secure VANETs, despite their unique characteristics compared to conventional ad hoc and sensor networks.

The approaches that have been selected for analysis are ARAN [15], ARIADNE [16], CONFIDANT [17], DCMD [18], SAODV [19], SEAD [20], SLSP [21], SPAAR [22], SOLSR [23], and WATCHDOG-PATHRATER [24]. While their main objective to secure ad hoc routing is common to all, their means to achieve it are quite different, i.e. symmetric cryptography, asymmetric cryptography, and reputation systems are used under different assumptions about network architecture and protocols, some also have additional features to prevent replay

attacks, such as the usage of timestamps. It is worth noting that many other existing approaches for secure routing in mobile ad hoc networks exists – for example, AODV-SEC [25], BISS [26], PACKET-LEASHES [27], VARS [28] and many others – we have preselected what we regard as representative for a certain group of approaches.

The remaining sections of the report are structured as follows: Section 2 briefly presents ad hoc routing and possible attack scenarios, Section 3 describes the selected approaches, Section 4 classifies the approaches and makes a comparison. Finally, we analyze the applicability of the solutions to VANETs and draw conclusions in Section 5.

## 2 Ad-hoc Routing and Possible Attacks

A mobile ad hoc network is an autonomous system of mobile routers (and attached hosts) connected by wireless links. The routers can move randomly and organize arbitrarily. Routing in an ad hoc network is based on multi-hop forwarding, where intermediate nodes forward data packets from the source towards the destination. Every node can simultaneously be a terminal and a router. Without any secure mechanisms nodes can perform any actions in the packets they forward. They are able to change the packets content, to drop it, or even inject new packets. This behavior can completely disrupt the routing of the packets, avoiding the availability of the network.

Several attacks can be performed, and they fall into the following categories (see also [29–32]):

- *Spoofed, altered, or replayed routing information* attacks are used to create routing loops, attract or repel network traffic, extend or shorten source routes, generate false error messages, partition the network, increase end-to-end latency, etc.
- *Selective forwarding* refers to the action of always dropping certain specific messages. Since simply dropping all packets can be easily detected by neighbors, the attacker can also perform a selection on the packets, just forwarding some of them, being able to degrade the service anyways.
- *Sinkhole attacks* are the ones that try to make all the traffic from a particular area go through the attacker, if this attack succeeds then the attacker will have control of all the area traffic, enabling the occurrence of many other attacks, such as *selective forwarding*. *Wormhole attacks* can be considered as a subclass of *sinkhole attacks*, where two nodes create a tunnel between them and forward the packets through it. This can be useful to lure a node of a better path to the destination.
- *Sybil attacks* is a kind of impersonation, where one single node pretends to be more than one node. With several entities in the network it will be able to reduce the effectiveness of fault-tolerant schemes. This attack is also very dangerous in geographical routing because a node can claim to be in several positions at the same time.

- *Acknowledgment spoofing* is used to describe the method of making some node believe that the link layer is weaker or stronger than it really is. This can be used to avoid other nodes sending messages to the attacker, or make them send most of the messages to him.

### 3 Overview of Selected Approaches

In the following selected approaches for secure routing are described. For every approach, we first summarize the main objectives and security mechanisms. Then, we describe how the approach works, and finally give a short justification for the approach compared to other approaches.

#### 3.1 ARAN

ARAN [15] stands for *Authenticated Routing for Ad hoc Networks*. Effectively, it is similar to AODV [33], but provide authentication of route discovery, setup, and maintenance. Main objectives of ARAN are to detect and protect against attacks from malicious nodes in a managed-open scenario where no network infrastructure is pre-deployed, however it expects a small amount of prior security coordination. ARAN introduces *authentication*, *message integrity*, and *non-repudiation* using pre-determined cryptographic certificates.

ARAN requires the use of a trusted certificate server whose public key is known by all valid nodes. Before entering the ad hoc network each node requests a certificate from the server. This certificate should contain the IP address of a node  $A$ , the public key of  $A$ , a timestamp  $t$  of certificates' creation and a time  $e$  at which the certificate expires. The certificates are used to authenticate a node to other nodes during the exchange of routing messages.

When a node wants to initiate a *route discovery* it broadcasts a signed *route discovery packet* (RDP) that includes the destination, it's certificate, a nonce  $N$ , and a timestamp  $t$  all signed with  $A$ 's private key. The nonce and timestamp together are used to ensure freshness when used in a network with a limited clock skew. Each node in the path validates the previous node's signature, removes certificate and signature, and records the IP address of the previous node. Then, the node signs the original contents of the message, appends its own certificate and forwards the message.

When the destination receives the first RDP it signs a *reply packet* (REP) and unicasts it back along the reverse path. The REP includes a packet type identifier, the IP address of the source, it's certificate, the nonce, and the associated timestamp sent by the source. Again, each node validates the previous node's signature, and removes it's certificate and signature. Then, the node signs the original contents of the message, appends its own certificate and unicasts the message to the next node in the route. When the source receives the REP, it verifies the destination's signature and the nonce returned by the destination.

When no traffic has occurred on an existing route for that route's lifetime, the route is removed from the routing table. When data is received on an inactive route it causes the node to generate an signed *error message* (ERR) that

travels the reverse path toward the source. These ERR messages are also used for reporting broken links due to node movement.

Compared to basic AODV, ARAN prevents a number of attacks, including spoofing of route signaling messages and alteration of routing messages (like altering TTL values). Also, replay attacks are prevented by a nonce and timestamp. The authors show in [15] that ARAN shows a good performance, equivalent to AODV, in discovering and maintaining routes. Besides its problems handling scalability with the number of nodes – that are inherited by AODV – it causes more packet overhead and higher latency in route discovery since each packet must be signed.

### 3.2 ARIADNE

ARIADNE [16] extends DSR [34] by security functions using symmetric cryptography. The authors suggest any of these three schemes: *shared secrets between each pair of nodes*, *shared secrets between communication nodes combined with broadcast authentication*, or *digital signatures*. Though the latter scheme does not use symmetric cryptography, it is also considered as an option due to its high reliability, but not as the preferred option because of high processing requirements.

We will focus the study of ARIADNE when using TESLA [35]. TESLA is a broadcast authentication scheme. A sender adds a message authentication code (HMAC) keyed according to time intervals. The receiver can verify the message when the key is sent in a future time interval based on a key disclosure interval. The time-delayed key disclosure is based on a loose, but bounded clock synchronization between the two involved nodes.<sup>2</sup>

The main objective of ARIADNE is to provide authentication and integrity of DSR signaling messages, i.e., routing discovery and route maintenance. With DSR, a *route request* (RREQ) carries the node list for the source route. In order to provide a reliable route discovery ARIADNE verifies *authenticity* and *integrity* of a RREQ making it infeasible to remove nodes from the list and to ensure senders' authenticity.

In a *route discovery*, each hop authenticates new information in the RREQ. The destination buffers the RREQ until the intermediate nodes release the corresponding TESLA keys. The TESLA security condition is verified at the destination, and the target includes a HMAC in the *route reply* RREP to certify that the security condition was met. In order to avoid that intermediate nodes remove others from the list in the RREQ (making the attacker the preferable shortest path), every intermediate node applies a one-way hash function in order to use per-hop hashing and appends it to the packet header.

ARIADNE's protects *route maintenance* of DSR, where after a limited number of retransmission attempt failures, the node returns a *route error* (RERR) to the route initiator. ARIADNE prevents unauthorized nodes from sending RERRs because it is required that each RERR message is authenticated.

---

<sup>2</sup> For details of TESLA refer to [35].

ARIADNE protects DSR from a number of attacks, including routing loops, black/grey holes, and replay. Regarding performance, it is worth noting that *i*) every intermediate node increases the length of the signaling messages (RREQ/RREP) which result in large signaling packets for long routes, *ii*) the time-delayed key disclosure increases the end-to-end delay of a route discovery process. Both issues negatively impact the packet delivery ratio, in particular for highly mobile scenarios.

### 3.3 CONFIDANT

CONFIDANT [17] is short for *Cooperation Of Nodes: Fairness In Dynamic Ad hoc NeTworks*. The objective is to detect malicious nodes by means of observation or reports about attacks. It allows to exclude nodes from route discoveries and to route around misbehaving nodes, and to isolate them by means of a reputation system. CONFIDANT was designed for DSR [34], however, it might be applied as an extension to other source routing protocols.

CONFIDANT introduces four new elements: *monitor*, *trust manager*, *reputation system*, and *path manager*. For each packet forwarded by a node, the *monitor* ensures that the next node in a forwarding chain also forwards the packet correctly. This is achieved by *passive-acknowledgments* or by observing route protocol behavior. If an anomaly<sup>3</sup> is detected, the node triggers an action by the reputation system, which manages a table with entries for nodes identifiers and their rating. The rating is changed only when there is sufficient evidence of misbehavior. These evidences have different weights, depending whether it was detected by the node itself (higher weight), it was obtained from a neighborhood observation (smaller weight) or it was reported by other node (even smaller weight). The *trust manager* is responsible for sending and receiving ALARM messages which are used to warn others of malicious nodes. On reception of an ALARM message, a node verifies its trustworthiness before triggering any action from the *reputation system* or before forwarding it to other nodes. The node can also send an ALARM message when itself experiences a malicious behavior. The *path manager* has the responsibility to *i*) rank paths according to security metrics, *ii*) remove paths containing malicious nodes, *iii*) to ignore route requests from malicious nodes, or *iv*) warn the source and ignore the message of a route request when the path contains malicious nodes.<sup>4</sup>

It is expected that CONFIDANT has scalability problems with the number of nodes. Then, the tables maintained by the reputation system of each node may become huge. Also, in scenarios with very high mobility, the overhead can increase considerably. However, for network with a small number of nodes and low mobility CONFIDANT represents a good solution since it has a low packet overhead increase over DSR, and it has low computational requirements.

<sup>3</sup> An anomaly can be a malicious behavior or just a network error.

<sup>4</sup> The listed actions, such as ignoring the message or warning the source node of a route request, represent examples of actions that may be applied depending on the desired security level.

### 3.4 DCMD

DCMD is short for *Detecting and Correcting Malicious Data in VANETs* [18]. It assumes is a sensor-driven technique that allows nodes to detect incorrect information and identify the node or nodes that are the source of this incorrect information with high probability. This approach is very general and rather focused on applications. However, the principle can also be applied to ad hoc routing and is independent of the type of ad hoc routing protocol.

In DCMD, every node builds a model that contains all the knowledge of the VANET. Based on a formal definition of events and nodes, the model specifies rules or statistical properties for assertions and then defines whether an event is consistent or inconsistent with the model. When a node receives a message, it compares the received data with it. When the received data does not agree with the VANET model, it is used an adversarial model which assumes that an attack involving a few malicious nodes is more likely than an attack that requires collusion between a large number of nodes. Given this model, a node will use the simplest possible explanation of the disagreement in order to restore the consistency. The adversarial model will be changeable in order to adjust itself to future changes of the adversarial patterns of attacks.

The model of the VANET can be rule-based or based on statistical properties of events. And the decision whether an event is valid or not can either be a binary or a probabilistic. In principle, this approach can be used for validation of both, application data and routing information.

DCMD uses some ideas of reputation systems, but in order to fulfill VANETs' requirements, such as scalability and mobility, nodes reputation is used for a small time interval since this classification is not used to classify a node, but rather to classify an event validity, based on its plausibility.

### 3.5 SAODV

As the name suggests, SAODV [19] is a secure extension for AODV [33]. The main objectives of SADV are integrity, authentication, and non-repudiation of AODV routing information. It uses two mechanisms to secure messages: digital signatures to authenticate the non-mutable fields of messages, and hash chains to secure the hop count information which is the only mutable information in the packets.

Every time a node originates a RREQ or a RREP message, it generates a random number and sets a *max hop count* from the *time to live* field of the IP header. The node sets the hash field with the random number as well as the identifier field of the hash function. Finally, it calculates the *top hash* by hashing the random number *max hop count* times. This algorithm allows the receiving nodes to verify the hop count of each message by applying the hash function *maximum hop count - hop count* times to the value in the hash field. If the calculated value and the *top hash* field are the same the hop count is verified. Every time a RREQ is re-broadcasted or a RREP is forwarded, the node has to apply the hash function to the *hash field*.

The previous mechanism is enough for verifying the hop count, but it does not ensure the integrity of non-mutable data. Digital signatures are used to solve this problem by signing everything but the *hop count* and the *hash* field.

Both mechanisms mentioned are quite efficient in security, however, when we apply them, the intermediate nodes cannot reply to RREP messages if they have a 'fresh enough' route to the destination, like what is done in AODV. This would only be possible if the node would be able to sign it on behalf of the final destination.

The authors propose two solutions. The first solution ignores this optimization and the node just forwards the RREQ as if he didn't have the route, the other solution allows the optimization but requires some additional packet overhead: Every time a node generates a RREQ message, it includes the RREP flags, the prefix size and the signature that can be used by intermediate nodes in case they already have a route to the destination. Moreover, the intermediate nodes should include the previous lifetime to verify the signature of the route destination, and they should also sign the new lifetime. Using this method the original information is signed by the final destination and the lifetime is signed by the intermediate node.

In RERR messages the only relevant information is which node sent the message. The best way to achieve this requirement is using signatures to sign the whole RERR message. This way, when a node receives a RERR message it can verify whether the sender is who it claims to be. And, since destination sequence numbers are not signed by the corresponding node, a node should never update any destination sequence number of its routing table based on RERR messages. However, even without updating the routing table information, a node will use the destination sequence number to decide whether to invalidate or not the route.

Since SAODV is an extension of AODV and their performance characteristics are similar. However, the known problems of AODV become a greater problem in SAODV. It is well known that AODV increases the packet overhead when the mobility increases. This will even be a bigger problem for SAODV since the processing of each packet requires some extra processing time, due to the usage of asymmetric cryptography. This property may cause DoS of low computational resource nodes, even without the existence of malicious nodes.

### 3.6 SEAD

SEAD (*Secure Efficient Ad hoc Distance Vector*) routing protocol [20] was designed with the objective to protect against multiple uncoordinated attackers creating incorrect routing state in any other node. In order to be deployed in an environment with low computational power and to guard against DoS attacks in which an attacker tries to make other nodes consume excessive bandwidth or processing time, it only uses efficient one-way hash functions instead of asymmetric operations. The design was based in DSDV, but the main ideas can be applied in other distance vector protocols.

Every node that wants to send a route update about itself must use a single next element from its hash chain. Based on this initial element, the one-way hash chain conceptually provides authentication for the lower bound of the metric in other routing updates for this destination. The reason it only provides authentication for a lower bound on the metric is because nothing prevents a malicious node from claiming the same metric, or higher, as the node from which it heard this route. This mechanism also allows the authentication of each entry of routing updates describing a route to another destination.

Hash chains were useful for authenticating the metric and sequence number, however, this doesn't prevent an attacker from advertising the same distance and sequence number that he received. To defend against this attacks, *hash tree chains* are used in conjunction with *packet leashes*. This is done by tying the authenticator to the sender address preventing an attacker from replaying an authenticator that it hears from a neighbor. It constructs a hash tree chain, where each element of the chain encodes the node identifier, thus forcing a node to increase the distance metric if it wants to encode its own identifier.

SEAD also requires the usage of some method to authenticate the source of each routing update. The authors suggest some solutions such as TESLA, TIK [30]<sup>5</sup> or just a shared secret key among each pair of nodes. This authentication is required because otherwise an attacker would be able to create routing loops.

SEAD performance is good when compared to other distance vector routing protocols such as DSDV. In fact, it's packet overhead is higher and sometimes may cause some congestion in the network. However, this increase of the number of routing advertisements also allows nodes to have more recent routing tables, allowing a better performance when we are in an environment with high mobility. And also, as already said, it's a good option for networks where we have low computational resources because it doesn't use any asymmetric cryptography, which usually require some extra computational resources.

### 3.7 SLSP

SLSP [21] stands for *Secure Link State routing Protocol*. Main objective is to provide secure proactive routing by protecting the topology discovery and the distribution of link state information across mobile ad hoc domains. It uses one-way hash function and a public key cryptosystem. The keys certification can be provided by a coalition of some nodes and the use of a threshold cryptography<sup>6</sup>, the use of local repositories of certificates provided by the network nodes, or a distributed instantiation of a CA. SLSP can be used as the *Intra-Zone Routing Protocol* in the *Zone Routing Protocol (ZRP)* [37].

In order to secure the topology discovery and the distribution of *Link State Updates* (LSU), SLSP disallows advertisements of non-existent, fabricated links,

<sup>5</sup> TIK stands for TESLA with instant key disclosure. It avoids the *round trip delay* required by TESLA but requires tight clock synchronization between nodes.

<sup>6</sup> See [36] for details.

stops nodes from masquerading their peers, strengthens the robustness of neighbor discovery, and thwarts deliberate floods of control traffic that exhaust network and node resources.

This approach is based on zones which means that nodes send their LSU and maintain topological information only of their neighbors within a previously defined number of hops. Nodes also have to broadcast regularly their public keys within the zone so that when topology changes they can learn the keys of new nodes. This also allows nodes to keep track of a low number of keys at every instance.

When discovering nodes, SLSP uses a *Neighbor Lookup Protocol* (NLP) which is responsible for: *i*) maintaining a mapping of MAC and IP addresses of the node's neighbors, *ii*) identifying potential discrepancies, such as the use of multiple IP addresses by a single data-link interface, and *iii*) measuring the rates at which control packets are received from each neighbor. The last property can easily help defending against DoS attacks.

Nodes sending LSUs must take some action to prevent packets from being propagated outside its zone. This is achieved by one-way hash chains that authenticate the hop count. The hash chain values are authenticated using the hash chain's anchor, which is included in the signed fields of the LSU.

Besides securing topology discovery and link state updates information, it also uses a mechanism to protect against network flooding. This is done by *rating* nodes. Nodes generating or forwarding less LSUs are given higher priority over any node that sends more LSUs. If the neighbor has a high rate flooding, its packets can even be discarded.

Since SLSP is based on zones, there should be no problem in deploying it in large networks. From the protocol description it seems that it can easily adapt to topology changes, depending on the time interval between each LSU and broadcast of nodes' public keys. Since the protocol also makes use of asymmetric cryptography, it also requires some additional processing resources that may bring problems when there are nodes with limited processing resources.

### 3.8 SPAAR

*Secure Position Aided Ad hoc Routing* [22] (SPAAR) uses position information in order to improve the efficiency and security of mobile ad hoc networks. It was designed for use in an environment where security is a primary concern and uses geographical information to make forwarding decisions, resulting in a significant reduction in the number of routing messages. It uses asymmetric cryptography to protect against malicious nodes and attempts to minimize the potential for damage of attacks from compromised nodes.

Each node in the network requires a public/private key pair, a trusted certificate server binding its identity to its public key, and the public key of the certificate server. It provides the necessary elements to offer *authentication*, *non-repudiation*, *confidentiality*, and *integrity*.

Besides the public/private key pair, each node also needs a public/private key pair for communication with its neighbors. This key pair is generated and

exchanged, using the global public/private key pair, when new neighbors are detected.

When a node sends a multi-hop message, like a RREQ or a RREP, it must be signed with its private key and encrypted with the public key of a neighbor. Every node can verify that the message was sent by a one-hop neighbor, and the destination can also verify that the sender is who it claims to be.

This method requires each node to maintain two tables, one for one-hop neighbors, and another for the recent destinations it has communicated with. The tables are very similar, except that the destination table also has to save information about the speed of the node, so it can predict the next position of the node. This information is not required in one-hop neighbors, since position is exchanged regularly through *table update* messages, which are piggybacked in every routing messages. Nodes also have to broadcast regularly *hello* messages so that topology changes can be quickly detected.

There are two more types of messages, *location request* and *location reply*. When a node doesn't have an entry for a destination it broadcasts a *location request*, if any node that receives the message has the location coordinates for the required node, it replies with a *location reply*.

This approach is very efficient when talking about security issues, however, it requires the double of processing time, since it uses asymmetric cryptography, not only for end to end communication, but also for hop-to-hop communications. The adaptation to topology changes should also not be a problem since it will depend on the time interval between the *hello* messages. The fact it makes use of geographic routing also helps reducing the overall overhead.

### 3.9 SOLSR

SOLSR [23] is a security extension to the OLSR [38] protocol. The purpose is to provide authentication to OLSR signaling packets, and to prevent replay attacks. This is achieved by using *message authentication codes (HMAC)* in every hop, and by making use of *timestamp exchanges*. It is assumed that all nodes have access to the same shared key in order to sign and verify the authenticity and integrity of each message.

The *timestamp exchange* is performed in a *challenge-response* scheme. It does not require synchronized time but the clocks are assumed to be relatively synchronized. When a signed message is received a certain slack  $S$  in the calculated timestamp difference is allowed. This timestamp difference is recalculated every time a verified message is received, so that any skew between clocks can be quickly compensated.

This approach adds some extra packet overhead to the OLSR protocol, however the computational requirements can be considered low, since it only makes use of symmetric cryptography. SOLSR should have no problems with low mobility networks, but it may have some problems in high mobility scenarios. The same applies to scalability, where small networks should be not problem, but larger networks may reveal some performance issues.

### 3.10 WATCHDOG–PATHRATER

WATCHDOG–PATHRATER was proposed by [24]. The objective is to detect misbehaving nodes by means of observation and reports by other nodes, and to route around misbehaving nodes. WATCHDOG–PATHRATER was designed as an extension to DSR [34].<sup>7</sup>

The approach introduces two extensions to DSR: A *watchdog* detects misbehaving nodes. A *pathrater* avoids routing packets through the detected malicious nodes. Both extensions are executed in every ad hoc node.

In detail, the *watchdog* maintains a buffer of transmitted packets and observes forwarding of other node (by overhearing or *passive acknowledgments*). It compares each overheard packet with the packets in the buffer. If a packet has remained in the buffer longer than a predefined timeout interval, the watchdog increments a failure counter for the node responsible for forwarding. If the counter exceeds a certain threshold, the node is marked as misbehaving.

The *pathrater* defines a metric to estimate a link with respect to the reliability of links and knowledge about misbehaving nodes. A node assigns this metric to every other known node and periodically updates the metric. If a link is actively used, the metric is increased. In case a link break occurs, the metric is decreased. High negative numbers are assigned to nodes suspected to misbehave. In order to determine a path, the source node calculates a path metric by averaging the node ratings in the path. If multiple paths are available the one with the highest metric is selected. When a *pathrater* of a node learns that a node on a path misbehaves and an alternative path free of misbehaving nodes cannot be found, it sends a *route request*.

The WATCHDOG–PATHRATER approach has some limitations, as stated in [24]: Since a packet collision might occur and prevent a node to forward a packet, a forwarder should not immediately be accused of misbehaving, but rather observed for a longer period of time. Hence, detection of misbehaving nodes can take long.<sup>8</sup>

## 4 Comparison and Applicability to VANETs

### 4.1 Categorization of Existing Approaches

Depending on the network assumptions and requirements we can choose between several basic secure mechanisms, which can fall into different categories. In the higher tier we have asymmetric cryptography, symmetric cryptography, reputation systems, and plausability.

---

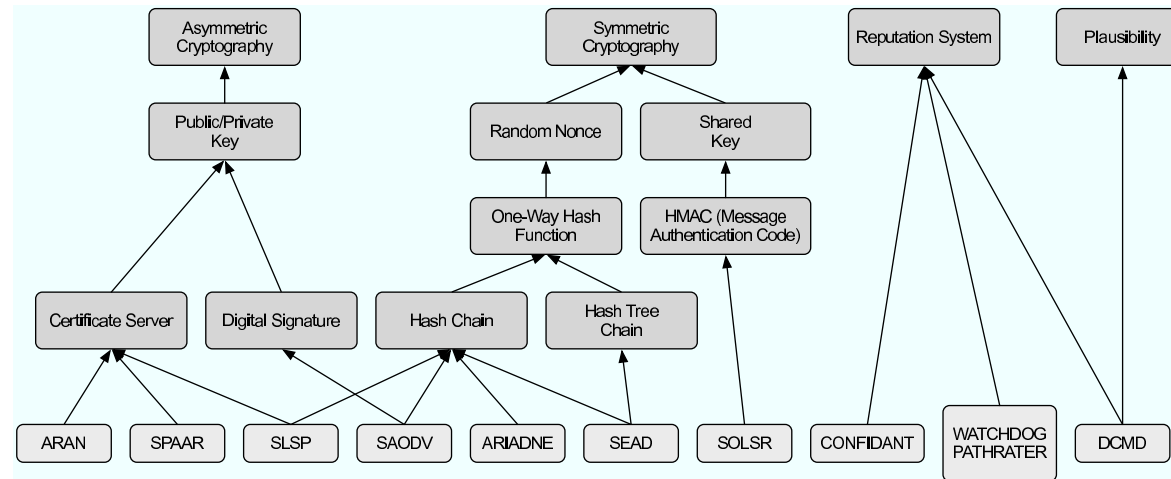
<sup>7</sup> It is worth noting that the approach requires a-priori knowledge about paths. Hence, the underlying ad hoc routing protocol must be based on source routing and can not be applied to other routing protocols.

<sup>8</sup> Other problems include purposefully collisions, misusing power control, and false accusing other nodes. All these actions prevent detection of misbehaving nodes. For details see [24].

With asymmetric cryptography each node has a public/private key pair that can be appended to a message as a digital signature, or if bound to with additional information of the entity, the key pair can be part of a certificate. In symmetric category we can use a nonce or a shared key between each pair of nodes. The shared keys are used to generate keyed-hash message authentication codes, while the nonce is used by one-way hash functions in order to generate hash chains, or hash tree chains.

Figure 1 depicts the graphical representation of these dependencies, as well as the mechanism applied by each approach. Some protocols adopt more than a single mechanism in order to achieve different secure objectives. Most of them use one way hash functions, either to generate hash chains or hash tree chains, for securing mutable data. Certificates, digital signatures or HMACs provide in principle authentication and integrity of messages.

Most of the cryptographic schemes are defenseless against attacks from compromised nodes. However, reputation systems can be used complementary with cryptography to better achieve security against both malicious and compromised nodes. Another method for defending against compromised nodes is the usage of mechanisms that perform plausibility checks over the received data. This latest mechanism can be very efficient and avoid scalability and mobility problems, that are known to exist in reputation systems.



**Fig. 1.** Dependencies between the adopted security mechanisms by existing approaches

## 4.2 Comparison of Existing Approaches

In Table 4.2 we summarize the main features of the described approaches and performance aspects. Features include the main objectives of the approach, the applied basic security mechanisms, and specific design considerations.<sup>9</sup> Performance aspects cover adaptation to topology changes, scalability with the number of nodes, packet overhead, and processing overhead. The intention of the performance classifications is rather a high level qualitative estimation of existing secure routing approaches than a precise quantitative performance evaluation.

Below, the criteria for comparison are explained.

- **Adaptation to topology changes** is used to describe the protocols adaptation to high mobility scenarios as well as spontaneous attachment/ detachment of nodes. The protocols can be classified as follows: *Good adaptation* stands for protocols which can handle mobility scenarios and are able to maintain their normal performance. *Average adaptation* stands for protocols which can handle mobility scenarios but the global performance of network degrades, i.e. lower *packet delivery ratio* (PDR). *Bad adaptation* means that the performance of the protocol is low making packet transport among nodes difficult.
- **Scalability** refers to the performance of the approach with increasing number of nodes in the network. It can be classified as follows: *Good scalability* is used when a network grows as much as it needs and the approach is still able to maintain a good performance. *Average scalability* means that an approach can handle networks with a reasonable size, but may have problems if it grows. *Bad scalability* describes approaches which restrict to small networks like offices, or small companies. This usually means that every node *knows* who the others are. This can also be applied to approaches that require the usage of symmetric keys because it is not reasonable to share secret keys between each pair of nodes in large networks.
- **Packet overhead** is the criteria used to refer to bandwidth consumption due to larger packets and/or higher number of signaling packets. The protocols can be classified as follows: *Low overhead* stands for protocols which require no additional overhead when compared to their basis protocol, or if they have larger packets but they also use some optimization to reduce the bandwidth usage. *Average overhead* is used to classify the approaches that require some larger packets, due to cryptography needs but do not require any additional signaling packets. It can also be used to approaches that do not require larger packets, but do require more bandwidth. *High overhead* means that an approach requires larger packets as well as an increased number of signaling packets.
- **Processing** is the criteria to associate an approach with processing requirements and is classified as follows: *Low processing* refers to approaches that

---

<sup>9</sup> Design considerations means whether the approach extends an existing ad routing protocol or develops a new one.

require a low CPU processing. This will mostly fit approaches based on reputation systems or symmetric cryptography. *Average processing* will be used to classify the approaches using both reputation and symmetric systems. *High processing* is used to classify any approach that requires asymmetric cryptography.

Approach	Objectives	Basic Security Mechanisms	Design Considerations	Adaptation to Topology Changes	Scalability	Packet overhead	Processing
<i>ARAN</i>	Authentication, integrity and non-repudiation of signaling packets	Certificate authority and timestamps	Based on AODV, and designed to substitute reactive routing protocols	Good adaptation	Average scalability	Average overhead	High processing
<i>ARIADNE</i>	Authentication and integrity of signaling packets	Symmetric cryptography primitives, hash functions and timestamps <sup>10,11</sup>	Based on the basic operations of DSR, though the mechanisms used for attack robustness should be general	Average adaptation	Average scalability	Low overhead	Average overhead <sup>1,2</sup>
<i>CONFIDANT</i>	Exclude misbehaving nodes from route discovery	Reputation system	Designed to be an extension for reactive source-routing protocols	Average adaptation	Average scalability	Average overhead	Low processing
<i>DCMD in VANETs</i> <sup>13</sup>	Detect and correct malicious data based on its plausability	Observation and plausability of events	Designed to be an extension of VANETs communication system	Good adaptation	Good scalability	Average overhead	Low processing
<i>SAODV</i>	Authentication and integrity of signaling packets	Digital signatures and hash chains	Designed to be an security extension for AODV	Average adaptation	Average scalability	Average overhead	High processing
<i>SEAD</i>	Authentication and integrity of signaling packets (route state update)	Hash chain and sequence numbers	Based on DSDV but can be applied to other distance vector protocols	Good adaptation	Average adaptation	High overhead	Average processing
<i>SLSP</i>	Authentication, integrity, and non-repudiation of signaling packets	Certificate authority	Extends an intra-zone protocol for ZRP	Good adaptation	Good scalability	Average overhead	High processing
<i>SPAAR</i>	Authentication, integrity, non-repudiation, and confidentiality	Certificate authority and timestamps	New secure position aided ad hoc routing protocol	Good adaptation	Good scalability	Average overhead	High processing
<i>SOLSR</i>	Authentication and integrity of signaling packets	MACs and a timestamps	Security extension for OLSR	Average adaptation	Average scalability	Average overhead	Low processing
<i>WATCHDOG-PATHRATER</i>	Exclude misbehaving nodes from route discoveries	Observation and reputation system	Designed as an extension to DSR	Good adaptation	Average scalability	Average overhead	Low processing

Table 1. Overview of the main features presented by each approach

### 4.3 Unique VANET Characteristics

Though vehicular ad hoc networks share common characteristics with conventional ad hoc and sensor networks, such as self-organization and lack of central control, VANET have unique challenges that impact the design of the communication system and its protocol security. These challenges include:

**Potentially high number of nodes.** Regarding VANETs as the technical basis for envisioned *Intelligent Transportation Systems (ITS)* [39–41] we expect that a large portion of future vehicles will be equipped with communication capabilities for vehicular communication. Taking additionally potential road-side units into account, VANETs needs to be scalable with a very high number of nodes.

**High mobility and frequent topology changes.** Nodes potentially move with high speeds along streets and highways. Hence, in certain scenarios, such as when vehicles pass each other, the duration of time that remains for exchange of data packets is rather small, typically in the range of seconds. Also, intermediates nodes in a wireless multi-hop chain of forwarding nodes can move quickly. Hence, established routes between between two nodes are frequently interrupted and a network can be partitioned.

**High application requirements on data delivery.** Important VANET applications are for traffic safety to avoid road accidents, potentially including safety-of-life. These application have high requirements with respect to real-time and reliability. An end-to-end delay of seconds can render an safety information meaningless. Loss of messages, e.g. due to security attacks, may affect dead-or-life decisions. Also, these applications are typically based on a broadcast distribution of data (geographically-scoped flooding) where destination nodes are those located in a geographic area.

**No confidentiality for safety information.** For safety applications the information contained in a message is of interest for all road users, and hence not confidential.

**Privacy.** Communication capabilities in vehicles might reveal information about the driver/user, such as identifier, speed, position, and mobility patterns. Despite the need for message authentication and non-repudiation of safety message, privacy of users and drivers should be respected, in particular location privacy and anonymity.<sup>14</sup>

---

<sup>10</sup> The authors suggest three authentication methods: *pairwise shared secrets*, *TESLA* or *digital signatures*. Though the latter scheme does not use symmetric cryptography, it is also considered as an option due to it's high reliability, but not as the preferred option because of high processing requirements.

<sup>11</sup> Even only using symmetric cryptography, ARIADNE can provide authenticity because of TESLA properties.

<sup>12</sup> Assuming TESLA as cryptographic scheme.

<sup>13</sup> Detecting and Correcting Malicious Data in VANETs.

<sup>14</sup> "Anonymity is the state of being not identifiable within a set of subjects, the anonymity set" [42], or "the ability to prevent other parties from learning one's

**IEEE 802.11-based wireless technology.** Regarding the wireless technology, the current plans for ITS rely on a modification of the IEEE 802.11 standard, termed IEEE 802.11p [1]. The limited transmission range of the wireless technology deserves wireless multi-hop communication for communication beyond the transmission range.

**Less power and processing constraints.** In comparison to mobile phones and sensor nodes, we assume that communication devices in vehicles, i.e., on-board units (OBUs), are more powerful with respect to processing capabilities and memory. Despite the quest for minimal OBU costs with less capabilities, the expected lifetime of an OBU ( $\geq 10$  years) is longer compared to usual consumer devices and hence would allow higher investment with higher OBU capabilities. Also, since the devices are interconnected to the vehicle's on-board power supply, energy constraints are a non-issue.

**Clock synchronization.** With the assumption that future vehicles are equipped with GPS, nodes are provided with absolute time information. Hence, clock synchronization among nodes is not needed.

**Infrastructure access.** Communication infrastructure along the road, such as road-side units (RSUs) and public hot spots, allows access to network servers, typically in the Internet. Since road-side units and public hot spots do not provide full wireless coverage, it is expected that for security mechanisms, such as for management and distribution of cryptographic keys via a centralized architecture, infrastructure is not available all the time.

**Central registration and periodic technical inspection.** Unlike ad hoc and sensor networks, nodes must register with a central authorities. Hence, every vehicle has a globally unique identifier that could potentially be reused for security purposes. Finally, in most countries every vehicle a periodic technical inspection is mandatory. This inspection could be used to ensure the standard conformance and integrity of the communication system and alleviate security.

**Existing law enforcement mechanisms.** Existing law enforcement can aid the security of vehicular networks. If an attacker is unambiguously identified, existing procedures for legal remedies could be applied to punish attackers and provide disincentives.

#### 4.4 Discussion

In the previous parts of this section we have categorized the existing approaches and compared them with respect to their security objectives, applied security mechanisms, and performance criteria. Then we have described the unique characteristics of VANETs compared with conventional mobile ad hoc networks and sensor networks. We now discuss whether the existing approaches meet the requirements of VANETs and attempt to answer the following questions:

---

*current or past location*“ [43]. With location privacy, the location of a user cannot be linked to its identity.

1. Do the security objectives of VANETs match those considered by existing approaches for secure ad hoc routing?
2. Are the potential attacks on MANETs and VANETs compliant or what are differences?
3. Are the security mechanisms applied for MANETs also appropriate for VANETs?
4. Finally, what are VANET-specific challenges not covered by existing approaches for secure ad hoc routing?

From the comparison of the existing approaches we can state that notwithstanding the divergence of VANETs from conventional mobile ad-hoc and sensor networks, the main security objectives for routing are very similar, except the need for privacy and anonymity as it will be discussed below. In principle, however, the main differences lie in the applied security mechanisms used to achieve the same objectives, and the assumptions we can make about the network.

Some of the unique VANETs characteristics – *high number of nodes, high mobility, and frequent topology changes* – are a concern for most of the existing approaches. Most of them use routing protocols that have problems with scalability, either because of the huge amount of state information each node needs to maintain or the signaling packets are not appropriate for frequent mobility changes, originating some traffic delay or network overhead. The scalability problem also suits the approaches that suggest the usage of symmetric cryptography, where every pair of nodes would require a unique shared key, originating a complexity of  $O(n^2)$  instead of the  $O(n)$  for asymmetric complexity where  $n$  represents the number of nodes in the network. In VANETs where  $n$  can be very large, the complexity would be too high. However, the complexity problem of using symmetric cryptography would be alleviated if a broadcast authentication scheme, such as TESLA, would be applied. Nevertheless, there would still exist problems because of the *high application data requirements* – real-time – that TESLA cannot provide, since authentication needs one round-trip delay for the key disclosure procedure. Another option would be the usage of TIK, which requires tight *clock synchronization* possible through the usage of GPS information. But even if these issues could be solved, another reason to discourage symmetric cryptography would be the fact that VANETs could not cooperate with *existing law enforcement mechanisms* in order to identify and punish misbehaving entities. In order to achieve this property, we will need to provide non-repudiation which can only be guaranteed if asymmetric cryptography is used. For efficiency reasons, asymmetric cryptography might be used in combination with symmetric cryptography.

By now it should be clear that symmetric cryptography is not suitable for VANETs requirements, but asymmetric cryptography still has not been discussed in depth in order to be considered as an appropriate solution. As described in Section 4.3, we assume that VANETs have (temporary) *infrastructure access* via road-side units and public hot-spots. Also, today's vehicles require a *central registration* and *periodic technical inspection* in most countries. Both assumptions render good pre-conditions for asymmetric key distribution. In ad-

dition to key distribution, a certificate authority could potentially bind the keys to the entity itself, making it feasible to use message information for legal reasons. Without the usage of *certificate authorities* it would be difficult to have non-repudiation of messages sent, since there would be no trusted third party that could relate an entity's key to its real identity in case message information had to be used in courts.

A serious drawback of asymmetric keys is their high processing requirement, which may be a perfect target for DoS where attackers try to exhaust a nodes processing time and battery, by forcing them to spend time doing cryptographic calculations that are not required. But VANETs have *less power and consumption constraints*, and therefore we consider that these attacks hardly succeed and will be ignored. It should also be mentioned that VANETs have strict timing requirements, and the signing and signature verification of every packet may take some additional processing time, originating network latency. This problem can be surpassed by the use of dedicate hardware able to fulfill the existing timing constraints.

We have already discussed that asymmetric cryptography should be used in order to bind the identity of the entity and the message sender. However, at a first glance this will imply that *privacy* requirements of VANETs are corrupted. It is noted that for general communication privacy in communication a number of existing approaches exist, such as BLIND [44], SNF [45], and FARA [46]. Also, new communication network architectures consider privacy and anonymity, such as  $IP^2$  [47], TRIAD [48], TurfNet [49], and I3 [50]. Finally, there have been few studies of privacy for VANETs (e.g., [51]). These considerations are beyond the scope of this report and we can identify privacy and anonymity as an open issue that need to be been explored in more detail.

Applying confidentiality to VANETs routing packets would not be beneficial since most of the information carried by them can and should be used by intermediate nodes. As an example, nodes should be able to read the position sent in every packet in order to always have up to date position information about the surrounding nodes. Therefore, confidentiality should not be a concern of secure routing. However, it is a good idea to apply it on application data when private information is exchanged.

Along with the cryptography scheme chosen it would also be possible to use some reputation system in order to defend against compromised nodes, and not only malicious ones. However, it is known that these systems do not scale well since they have to track the reputation of all nodes, which might require huge tables of information that are difficult to manage and to keep up to date. Therefore this option would interfere with VANETs growth tendency, as referred before and needs further study.

Another possibility for protecting against compromised nodes falls into plausibility checks category. These checks can be done by comparing the data received from all the neighbours with the state of the surrounding environment obtained by sensors, or by pre-defined rules. Plausibility check mechanisms can be easily applied to VANETs whithout overall degradation of performance, but in order to

work correctly, a previous model of the VANET must be designed and integrated into each node.

The previous argumentation allows us to conclude that it is easier to provide secure routing in VANETs than in MANETs. The relaxed power and processing constraints, infrastructure access, central registration and periodic technical inspection offer the possibility to manage key distribution as well as key revocation without having to modify the base characteristics of the network, as it is required in most of the approaches. We can also make use of asymmetric cryptography without being concerned about processing and battery limitations. Another important issue is the geographical routing which makes it possible to have larger networks without scalability problems.

However, geographical routing also offers attackers new opportunities [32, 52, 53]. Node positions can be faked, making other nodes believe that he is in a different position. This can induce nodes in error, making them believe that the attacker is the closest node to the destination, and consequently being the next hop. This *sinkhole* attack is enough to compromise the whole communication, since the attacker will be able to eavesdrop, tamper, or drop packets. Consequently, a solution for secure ad hoc routing in VANETs, such kind of vulnerabilities need to be carefully analyzed and appropriate countermeasures taken.

## 5 Summary and Conclusions

This report has presented the current state of secure ad hoc routing. Several existing approaches were systematically described on a comparative abstract level, and compared with each other. After comparison of the existing solutions and analysis of the VANET requirements, we can conclude that the basic secure mechanisms used depend not only on the level of efficiency desired but in the assumptions made for the final deployment scenario.

VANETs have strong assumptions about their environment, which partially ease design decisions for a potential secure routing approach for VANETs. These assumptions made it possible to choose asymmetric cryptography as the most appropriate scheme for VANETs. This brings advantages such as reduction of key distribution complexity, and provision of non-repudiation, useful for legal issues. Also due to the assumptions made for VANETs – *less power and processing constraints* – the inherent disadvantages of asymmetric cryptography are not considered as a threat for DoS attacks. With the public/private key pair we are able to verify *integrity, authentication, and non-repudiation*. We can now defend against several attacks from malicious nodes, but there is no defense scheme against compromised nodes. This could be achieved by integrating the cryptographic system with a reputation system, but since they are known to not scale well it is not considered at this stage. However, the integration with a plausibility check technique would be beneficial when protecting against compromised nodes since they wouldn't influence the overall performance of VANETs, and incorrect information would be detected and corrected.

VANETs research has been increasing quickly, but before it leaves the research laboratories there are still some open issues that must be solved. Location privacy is one of the most important issues that needs to be addressed, since it is expected that people are not willing to trade their security in the road with their privacy. Another problem of VANETs is the usage of geographical routing, which is relatively new and therefore is still not mature enough. A more intense work must be done in order to identify new specific attacks, as well as finding the solutions. Finally, it is worth considering alternative security schemes that are not based on infrastructure for key distribution (PKI/CA). These might not be available in the introduction phase of a VANET.

## **6 Acknowledgment**

The authors are grateful to Matthias Gerlach, Joao Girao, and Tim Leinmüller for helpful comments on this survey.

## Nomenclature

<i>AODV</i>	Ad hoc On demand Distance Vector
<i>ARAN</i>	Authenticated Routing for Ad hoc Networks
<i>BISS</i>	Building secure routing out of an Incomplete Set of Secure associations
<i>CA</i>	Certificate Authority
<i>CONFIDANT</i>	Cooperation Of Nodes: Fairness In Dynamic Ad hoc NeT-works
<i>DCMD</i>	Detecting and Correcting Malicious Data
<i>DSDV</i>	Destination-Sequenced Distance-Vector Routing
<i>DSR</i>	Dynamic Source Routing
<i>DoS</i>	Denial of Service
<i>ERR</i>	ERRor message
<i>HMAC</i>	Message Authentication Code
<i>ID</i>	Identifier
<i>IP</i>	Internet Protocol
<i>ITS</i>	Intelligent Transportation System
<i>LSU</i>	Link State Updates
<i>MAC</i>	Medium Access Control
<i>MANET</i>	Mobile Ad-hoc NeTwork
<i>NA</i>	Not Applicable
<i>NLP</i>	Neighbor Lookup Protocol
<i>OBU</i>	On Board Unit
<i>PDR</i>	Packet Delivery Ratio
<i>PKI</i>	Public Key Infrastructure
<i>RDP</i>	Route Discovery Packet
<i>REP</i>	route REPlY packet
<i>RREQ</i>	Route REQuest
<i>RSU</i>	Road Side Unit
<i>SAODV</i>	Secure Ad hoc On demand Distance Vector
<i>SLSP</i>	Secure Link State routing Protocol
<i>SPAAR</i>	Secure Position Aided Ad hoc Routing
<i>TESLA</i>	Time Efficient Stream Loss-tolerant Authentication
<i>TIK</i>	TESLA with Instant Key disclosure
<i>TTL</i>	Time To Live
<i>VANET</i>	Vehicular Ad-hoc NeTwork
<i>VARS</i>	Vehicle Ad hoc network Reputation System

*In the context of communication networks, MAC usually refers to the medium access control protocol at the link layer, whereas it means message authentication code in the security community. In order to avoid ambiguity, HMAC refers to the keyed hashing for message authentication.*

## References

1. IEEE. Draft Amendment to Standard for Information Technology - Telecommunications and information exchange between systems - LAN/MAN Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Amendment 3: Wireless Access in Vehicular Environments (WAVE), January 2006.
2. Committee SCC32 of the IEEE Intelligent Transportation Systems Council. Draft Standard for Wireless Access in Vehicular Environments – WAVE Resource Manager. IEEE P1609.1/D12, November 2005.
3. Committee SCC32 of the IEEE Intelligent Transportation Systems Council. Draft Standard for Wireless Access in Vehicular Environments – Security Services for Applications and Management Messages. IEEE P1609.2/D3, November 2005.
4. Committee SCC32 of the IEEE Intelligent Transportation Systems Council. Draft Standard for Wireless Access in Vehicular Environments (WAVE) – Networking Services. IEEE P1609.3/D18, December 2005.
5. Committee SCC32 of the IEEE Intelligent Transportation Systems Council. Draft Standard for Wireless Access in Vehicular Environments (WAVE) – Multi-Channel Operation. IEEE P1609.4/D07, December 2005.
6. Vehicle Safety Communication Project. Final report. Submitted to the United States Department of Transportation, Federal Highway Administration and National Highway Traffic Safety Administration, May 2005.
7. J. Blum and A. Eskandarian. The Threat of Intelligent Collision. *IT Professional*, 6(1):24–29, January/February 2004.
8. J. Blum, A. Eskandarian, and L. Hoffman. Challenges of Intervehicle Ad Hoc Networks. *IEEE Transactions on Intelligent Transportation Systems*, 5(4):347–351, December 2004.
9. J. Hubaux, L. Buttyan, and S. Capkun. The Quest for Security in Mobile Ad Hoc Networks. In *Proceedings of the 2nd ACM International Symposium on Mobile and Ad Hoc Networking & Computing (MobiHoc 2001)*, pages 146–155, Long Beach, CA, USA, October 2001.
10. J. P. Hubaux, S. Capkun, and J. Luo. The Security and Privacy of Smart Vehicles. *IEEE Security and Privacy Magazine*, 2(3):49–55, May/June 2004.
11. B. Parno and A. Perrig. Challenges in Securing Vehicular Networks. In *Proceedings of ACM Workshop on Hot Topics in Networks (HotNets-IV)*, page 6, College Park, MD, USA, November 2005.
12. J. Crowcoft. The Privacy and Safety Impact of Technology Choices for Command, Communications and Control of the Public Highway. *ACM SIGCOMM Computer Communication Review*, 36(1):53–57, January 2006.
13. Y. C. Hu and A. Perrig. A Survey of Secure Wireless Ad Hoc Routing. *IEEE Security & Privacy*, 2(3):28–39, May-June 2004.
14. H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang. Security in Mobile Ad Hoc Networks: Challenges and Solutions. *IEEE Wireless Communications*, 11(1):38–47, February 2004.
15. K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, and E.-M. Belding-Royer. A Secure Routing Protocol for Ad Hoc Networks. In *Proceedings of International Conference on Network Protocols (ICNP)*, pages 78–87, Paris, France, November 2002.
16. Y.-C. Hu, A. Perrig, and D. B. Johnson. ARIADNE: A Secure On-Demand Routing Protocol for Ad Hoc Networks. In *Proceedings of ACM International Conference on Mobile Computing and Networking (MOBICOM'02)*, pages 12–23, Atlanta, GA, USA, September 2002.

17. S. Buchegger and J.-Y. LeBoudec. Performance Analysis of the CONFIDANT Protocol (Cooperation Of Nodes: Fairness In Dynamic Ad-hoc NeTworks). In *Proceedings of the 3rd ACM International Symposium on Mobile and Ad Hoc Networking & Computing (MobiHoc 2002)*, pages 226–236, Lausanne, Switzerland, June 2002.
18. P. Golle, D. Greene, and J. Staddon. Detecting and Correcting Malicious Data in VANETs. In *Proceedings of the 1st ACM Workshop on Vehicular Ad Hoc Networks (VANET 2004)*, pages 29–37, Philadelphia, PA, USA, October 2004.
19. G. M. Zapata. Secure Ad hoc On-Demand Distance Vector Routing. *ACM Mobile Computing and Communications Review (MC2R)*, 6(3):106–107, July 2002.
20. Y.-C. Hu, D. B. Johnson, and A. Perrig. SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks. In *Proceedings of 4th IEEE Workshop on Mobile Computing Systems and Applications (WMCSA 2002)*, pages 3–13, Calicoon, NY, USA, 2002.
21. P. Papadimitratos and Z. J. Haas. Secure Link State Routing for Mobile Ad Hoc Networks. In *Proceedings of the 2003 Symposium on Applications and the Internet Workshops (SAINT'03)*, pages 379–383, Washington, DC, USA, January 2003.
22. S. Carter and A. Yasinsac. Secure Position Aided Ad hoc Routing Protocol. In *Proceedings of the IASTED International Conference on Communications and Computer Networks (CCN02)*, November 2002.
23. T. Clausen, C. Adjih, P. Jacquet, A. Laouiti, A. Muhlethaler, and D. Raffo. Securing the OLSR Protocol. In *Proceeding of IFIP Med-Hoc-Net*, June 2003.
24. S. Marti, T. J. Giuli, K. Lai, and M. Baker. Mitigating Routing Misbehavior in Mobile Ad Hoc Networks. In *Proceedings of 6th Annual ACM/IEEE International Conference on Mobile Computing and Networking (MOBICOM 2000)*, pages 255–265, Boston, MA, USA, August 2000.
25. S. Eichler, F. Dötzer, C. Schwingenschlögl, F. J. F. Caro, and J. Eberspächer. Secure Routing in a Vehicular Ad Hoc Network. In *Proceedings of IEEE Vehicular Technology Conference (VTC Fall 2004). Wireless Technologies for Global Security*, Los Angeles, CA, USA, September 2004.
26. S. Capkun and J. P. Hubaux. BISS: Building Secure Routing Out of an Incomplete Set of Secure Associations. In *Proceedings of 2nd ACM Wireless Security (WiSe'03)*, pages 21–29, San Diego, CA, USA, September 2003.
27. Y. Hu, A. Perrig, and D. B. Johnson. Packet Leashes: A Defense Against Wormhole Attacks in Wireless Networks. In *Proceedings of IEEE Infocom 2003*, San Francisco, CA, USA, March 2003.
28. F. Dötzer, L. Fischer, and P. Magiera. VARS: A Vehicle Ad Hoc Network Reputation System. In *Proceedings of the IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM 2005)*, Taormina, Italy, June 2005.
29. J. R. Douceur. The Sybil Attack. In *Proceedings of 1st International Workshop on Peer-to-Peer Systems (IPTPS'02)*, pages 251–260, Cambridge, USA, March 2002.
30. Y.-C. Hu, A. Perrig, and D. B. Johnson. Wormhole Detection in Wireless Ad Hoc Networks. Technical Report TR01-384, Department of Computer Science, Rice University, June 2002.
31. C. Karlof and D. Wagner. Securing Routing in Wireless Sensor Networks: Attacks and Countermeasures. In *Proceedings of First IEEE International Workshop on Sensor Network Protocols and Applications*, pages 113–127, Anchorage, AK, USA, May 2003.
32. Z. Zhou and K.C. Yow. Geographic Ad Hoc Routing Security: Attacks and Countermeasures. *Ad Hoc & Sensor Wireless Networks*, 1(3):235–253, March 2005.

33. C. Perkins, E. Belding-Royer, and S. Das. Ad hoc On-Demand Distance Vector (AODV) Routing. RFC 3561 (Experimental), July 2003.
34. D. B. Johnson and D. A. Maltz. Dynamic Source Routing in Ad Hoc Wireless Networks. In Tomasz Imielinski and Hank Korth, editors, *Mobile Computing*, chapter 5, pages 153–181. Kluwer Academic Publishers, 1996.
35. A. Perrig, R. Canetti, J. D. Tygar, and D. Song. The TESLA Broadcast Authentication Protocol. *RSA CryptoBytes*, 5(2):2–13, Summer/Fall 2002.
36. Y. G. Desmedt. Threshold Cryptography. *European Transactions on Telecommunications*, 5(4):449–457, July/August 1994.
37. Z. J. Haas. A New Routing Protocol for the Reconfigurable Wireless Networks. In *Proceedings of IEEE 6th International Conference on Universal Personal Communications (ICUPC'97)*, volume 2, pages 562–566, San Diego, CA, USA, October 1997.
38. T. Clausen and P. Jacquet. Optimized Link State Routing Protocol (OLSR). RFC 3626 (Experimental), October 2003.
39. Dedicated Short Range Communications (DSRC) Working Group. <http://grouper.ieee.org/groups/scc32/dsrc/index.html>.
40. Car 2 Car Communication (C2CC) Consortium. <http://www.car2car.org>.
41. Internet ITS Consortium. <http://www.internetits.org>.
42. A. Pfitzmann and M. Kohntopp. Anonymity, Unobservability, and Pseudonymity - a Proposal for Terminology. In *Proceedings of International Workshop on Design Issues in Anonymity and Unobservability*, pages 1–9, Berkeley, CA, USA, July 2000.
43. A.R. Beresford and F. Stajano. Location Privacy in Pervasive Computing. *IEEE Pervasive Computing*, 2(1):46–55, 2003.
44. J. Ylitalo and P. Nikander. BLIND: A Complete Identity Protection Framework for End-points. In *Proceedings of 12th International Workshop on Security Protocols*, Cambridge, UK, April 2004.
45. A. Jonsson, M. Folke, and B. Ahlgren. The Split Naming/Forwarding Network Architecture. In *Proceedings of 1st Swedish National Computer Networking Workshop (SNCNW)*, Arlandastad, Sweden, September 2003.
46. D. Clarcn, R. Braden, A. Falk, and V. Pingali. FARA: Reorganizing the Addressing Architecture. In *Proceedings of the ACM SIGCOMM Workshop on Future Directions in Network Architecture (FDNA'03)*, pages 313–321, Karlsruhe, Germany, August 2003.
47. T. Okagawa, M. Jo, K. Nishida, and A. Miura. IP Packet Routing Mechanism Based on Mobility Management in IP-Based IMT Network Platform. In *Proceedings of 8th International Conference on Intelligence in Next Generation Networks (CIN 2003)*, Bordeaux, France, April 2003.
48. D. R. Cheriton and M. Gritter. TRIAD: A Scalable Deployable NAT-Based Internet Architecture. Technical report, Computer Science Department, Stanford University, Stanford, CA, USA, January 2000.
49. S. Schmid, L. Eggert, M. Brunner, and J. Quitteck. TurfNet: An Architecture for Dynamically Composable Networks. In *Proceedings of 1st International Workshop on Autonomic Communications (WAC 2004)*, pages 94–114, Berlin, Germany, October 2004.
50. I. Stoica, D. Adkins, S. Zhuang, S. Shenker, and S. Surana. Internet Indirection Infrastructure. In *Proceedings of ACM SIGCOMM 2002*, pages 73–88, Pittsburgh, PA, USA, August 2002.

51. K. Sampigethaya, L. Huang, M. Li, R. Poovendran, K. Matsuura, and K. Sezaki. CARAVAN: Providing Location Privacy for VANET. In *Proceedings of Workshop on Embedded Security in Cars (ESCAR 2005)*, Cologne, Germany, November 2005.
52. A. Aijaz, B. Bochow, F. Dötzer, A. Festag, M. Gerlach, T. Leinmüller, and R. Kroh. Attacks on Inter Vehicle Communication Systems - an Analysis. In *Proceedings of 3rd International Workshop on Intelligent Transportation (WIT)*, pages 189–194, Hamburg, Germany, March 2006.
53. T. Leinüller, E. Schoch, F. Kargl, and C. Maihöfer. Influence of Falsified Position Data on Geographic Ad Hoc Routing. In *Proceedings of 2nd European Workshop on Security and Privacy in Ad Hoc and Sensor Networks (ESAS'05)*, pages 102–112, Visegrad, Hungary, July 2005.