Trust Issues for Vehicular Ad Hoc Networks

Philipp Wex*, Jochen Breuer*, Albert Held*, Tim Leinmüller+ and Luca Delgrossi *
* Daimler AG, Group Research and Advanced Engineering,
{philipp.wex|jochen.breuer|albert.held|luca.delgrossi}@Daimler.com
+DENSO AUTOMOTIVE Deutschland GmbH, Technical Research Department,
t.leinmueller@denso-auto.de

***Abstract*—Characteristics and requirements of vehicular ad hoc networks (VANETs) differ quite significantly compared to standard ad hoc networks. Especially trust in VANETs is very important but still open issue, which will be addressed in this paper. We will describe, discuss and assess approaches and concepts that were proposed in ordinary fixed networks and mobile ad hoc networks and will show weak and strong spots. As basis for our considerations, we will describe a detailed automotive scenario, which relies on inter-vehicle communication for the exchange of safety relevant warning messages.**

I. Introduction

Vehicular ad hoc networks (VANETs) have some very specific characteristics and solutions to security issues are still in a very early stage of development. Especially the issue of trust between communicating vehicles (referred to as nodes) is an open question: How can one node trust a message it received from another node? Thus, trust establishment is a major challenge in vehicular ad hoc networks as the outcome of the trust establishment process is a trusted relation between nodes. Especially in critical applications like hazard warning a receiving node needs to ensure authenticity and trustability of received messages before reacting to them.

There are various types of trust models; some of them (especially the PKI based models) are even widely deployed already. They differ in their architecture, their trust establishment processes and flexibility.

In this paper we firstly describe VANETs in general (section 2) and present VANET applications that are of high interest (section 3). Then we show that the establishment of trust can be partitioned into two classes: infrastructure based trust and self organizing trust. Approaches and concepts for both classes will be discussed and presented (section 4). We conclude with a basic assessment of existing approaches regarding their applicability in VANETs (section 5).

II. Characteristics of VANETs

Compared to standard ad hoc networks, VANETs have several properties that introduce particular security challenges, which are not of major concern in other mobile ad hoc networks. In [1] Zarki et al. provide a list of characteristics of future vehicular networks, which are in some terms equivalent to what we see as major properties of VANETs.

Offline-infrastructure - Communication to a fixed infrastructure is possible, but it is unlikely that there is a permanent connection to this infrastructure. Infrastructure gateways are supposed to be located at gas stations, parking lots or even on selected points at the road side but not *everywhere* along the road side. We call this type of fixed infrastructure an offline-infrastructure, since in contrast to what we call online-infrastructure, it is not available all the time but only during (from the vehicles point of view) random periods of time.

Dynamic topology - One important characteristic of VANETs is that nodes move with high speed in respect to each other, which results in a very high rate of topology changes. Whereas for example during a conference people carrying PDAs "move" with a speed of $2\frac{m}{s}$ with respect to each other, cars on a highway normally easily achieve $55\frac{m}{s}$ when taking into account oncoming traffic.

Critical application requirements - Another important property is that applications within VANETs are often safety-critical and time-critical (e.g. alert messages, warnings, see section III for further details). Ad-hoc networks that mainly serve to distribute data do not underlie these aspects.

Auxiliary information - Furthermore, nodes in VANETs are context aware, they have access to additional data such as car sensor data or GPS. The usage of these so called "side-channel" information can be valuable when evaluating data obtained through communication with other nodes in the VANET.

Beside the specific properties, the application scenario of VANETs requires the achievement of special (security) goals.

Privacy - In some cases services in a VANET are related to personal data, such as current location or current speed, which requires anonymity in order to protect a driver's privacy. On the other hand, other services require identification and traceability.

Integration - Vehicles are not computers, applications or services in VANETs must work without interaction. Drivers can not act as administrators. For VANET nodes, battery power is not an issue (at least while driving).

III. Applications of VANETs

Applications within VANETs contain both inter-vehicle communication as well as vehicle to infrastructure communication. Both communication types can be performed via intermediate nodes, which results in multi-hop ad hoc communication. In [2] Franz et al. give an overview on applications and services that could be provided in a VANET. They distinguish three kind of different services: cooperative driver assistance applications (safety-related applications), local floating car data applications and user communication and information services.

Since especially safety-related applications are important in VANETs and in addition underlie special requirements and constraints, we use the following example scenario to clarify the motivation of this paper. A car driving on a highway detects

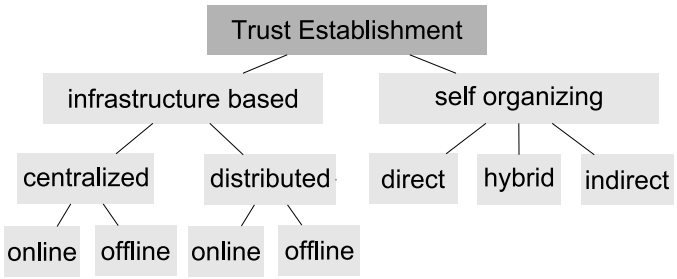

Fig. 1. Classification of trust establishment approaches

emergency braking because of an accident and communicates this event to other cars driving on the same highway.

Cars driving behind the sender receive this message and have to decide whether to display warning messages to their drivers or not. To be able to take this decision (and thus to protect the system against cars/nodes sending wrong warning messages) the cars need means to evaluate the trustworthiness of the message (origin).

IV. Trust Establishment in VANETs

Generally, it is assumed that each node in a VANET is equipped with a trust system, which can come to trust decisions (verify statements, be aware of trust, etc.).

There are two basic options for trust establishment: it can either statically rely on a security infrastructure or be built up dynamically in a self-organizing manner (see fig. 1). The former process relies on common, global, trusted and well-known system parameters (e.g. a central CA), which can be used for message authentication. The latter process lacks of this global knowledge and point of control and needs to take advantage of other trust supporting mechanisms.

A. Infrastructure-based Trust Establishment

In this section different approaches for infrastructure based trust will be addressed. This kind of trust relies on trust in the according infrastructure and is static over time (trust in security infrastructure is not lost) and most often makes use of certificates.

1) Classical Certificate-based Systems: Probably the most popular and most adopted trust system is the one proposed in the X.509 standard [3]. X.509 certificates contain attributes like the name of the issuing authority and of the subject node (in form of a "distinguished name"), the public key of the subject and a validity period. Because it binds the public key of a node to its name, this kind of certificate is called identity certificate (a verifier can verify that a prover node's pretended name has been certified by a trusted authority). In order for this approach to work, the name of the node must be globally unique; this is established by the hierarchical structure of X.500 namespaces. The complexity of X.500 motivated Rivest and Lampson to think of other approaches for the management of public keys and names resulting in an alternative mechanism for binding names to public keys locally: Simple Distributed Security Infrastructure (SDSI) [4].

In X.509 Version 3, additional fields within the certificates (e.g. access rights) can be defined. This leads the way to attribute certificates: those define the properties of a node with a distinguished name (a verifier can now verify that a prover node's attributes have been certified by a trusted authority). Properties can then be used during access control for authorization decisions. The Simple Public Key Infrastructure (SPKI) is an example of this kind [5]: Within this standard authorizations are directly bound to the public keys of nodes (not incorporating the strenuous management issue of names). Another novelty in this approach was the integration of delegation capabilities; a special flag, which is bound to a right indicates whether this right can be delegated. Thus verifiable certificate chains are built. Both developments, SDSI and SPKI, were combined to SPKI/SDSI in 1997. SPKI/SDSI alike systems, which rely on credentials are called Trust Management Systems. Keynote (and its predecessor PolicyMaker) is also a system of this kind: besides authorization information within its credentials, also security policies (as done e.g. in some IPSec implementations) can be defined.

VANETs could benefit of those concepts: certificates can be obtained from an offline infrastructure as defined in section 2 and later be used for offline trust verification; this is especially possible in a very dynamic environment with nodes one has never seen before. There are some open questions that have to be thought of though. Privacy is not a requirement in those systems making the certificates highly linkable to individual nodes. Furthermore, one has to carefully look at the time requirements of the certificate verifications: safety applications are very time-critical and it should be possible to verify certificates quickly.

2) Kerberos: One cannot talk about infrastructure based trust systems without mentioning Kerberos [6], [7], which is a successor of the Needham-Schroeder protocol, which revealed weaknesses in the sense of replay attacks. It relies on an online interaction with a central "Key Distribution Center" (KDC) for authentication in order to get a valid "trust" token for a service (contains a session key, a validity period preventing replay and the requesting node's identity encrypted with the server's secret key). The authorization information is kept at the services locally. Because of scalability problems in large environments, Kerberos V5 also allows for the central management of authorization information and to integrate those in the issued tokens.

Those approaches are not quite suited for VANETs: for every new interaction (which might happen quite often in VANETs) an online certification process with a central authority has to be launched (dependency of a permanent connection to infrastructure). Furthermore this interaction is time consuming, which makes it problematic for time-critical applications. Though, privacy can be established quite easily and unknown nodes' trustability can be checked as well.

3) Pseudonyms: Until now, each of the discussed trust concepts revealed the nodes' identities (node linkability) when interacting with other nodes: either their name and according public key is made public or the static public key with its attributes. Though, vehicular ad hoc networks require a high degree of privacy. A solution to this problem might be the use of pseudonyms, which can be changed over time (triggered automatically or by the user himself). This would not establish

anonymity but a higher degree of privacy. The central authority would be the only entity in the trust system, which can resolve pseudonyms and associate it with real world identities (vehicle IDs, user IDs).

This setting would reflect today's real-world situation (where there is always a central national authority that can resolve license plates to individuals) with the further enhancement that drivers' license plates are changed periodically. With the integration of pseudonyms the above mentioned certificated based approaches could be enhanced to provide better privacy.

4) Blind Signature: Other concepts go a further step ahead and introduce so-called blind signatures [8], i.e. anonymous certificates, within their trust systems.

Blind signatures allow a signer to digitally sign a statement without knowing the statement; it works as follows

- The requesting node uses a suitable blinding function f with a randomly chosen blinding factor b to compute $s' = f(s, b)$, where s is the clear statement. He sends s' to the authority.
- The authority signs s' using some ordinary signature algorithm sa and his private key k_{priv} to produce $Sig' = sa(s', k_{priv})$. He sends Sig' back to the requesting node.
- The node then applies the reverse blinding function f^{-1} to compute $Sig = sa(s, k_{priv})$

One example of this kind of systems is the following: a node requesting a certificate creates n blinded certificates with its attributes to be signed. The trusted authority will then randomly ask the node in an authenticated session to disclose $n-1$ of these certificates and can thus check the attributes. If all the attributes were correct, the authority would sign the last blind certificate, thus not knowing for which pseudonym it was signed and so granting anonymity to the node. The probability that wrong attributes are signed has then decreased to $\frac{1}{2^{n-1}}$. Furthermore the authority can prevent nodes from attacking the trust system by flooding the authority with certification requests: it can remember the frequency a node requests a certificate and forbid the issuing process in case of abuse.

This mechanism seems to be quite flexible as it is compliant to the above certificate based approaches and incorporates anonymity. One problem here is, that the requesting node has to create multiple statements for this to work.

5) Zero Knowledge / NIZKP: Zero-knowledge approaches can also be used for the establishment of anonymity: one node proves to another node the truth of an assertion (its certified statement) with knowledge of secret information (its ID) without revealing it.

Zero-knowledge approaches [9] have become fundamental cryptographic tools since the last 20 years. Simple zero-knowledge proofs are based on heavy interaction between communicating nodes (prover and verifier), which makes them unsuitable for our targeted time-critical applications; especially if a high degree of mobility was one characteristic the stability of the according communication links was a problem.

Non-interactive zero knowledge (NIZK) proofs [10] prevent this heavy interaction by providing a mono-directional interaction, from prover to verifier only. The main concept of NIZK proofs is the prover's and verifier's access to a common random string (public randomness).

That is also the reason why NIZK proofs are a very promising concept for trust establishment in VANETs. The only problem we found is its still questionable applicability (well-known algorithms, etc.).

6) Digital Credentials: An approach combing both blind signatures and zero knowledge proofs is proposed by Brands in [11]: Digital Credentials. In this concept, nodes holding certificates can selectively disclose attributes contained in the certificate while hiding any other information. The basic idea behind this is that the attribute values themselves are part of each node's secret and public keys and that a verifier could obtain all but one of the prover's attributes without being able to obtain all of the prover's secret key.

7) Group Signatures: The still emerging field of group signatures [12] is based on the following concept: in a group signature scheme a single public key has a large number of private keys. Each member of the group is issued a private key, which can then be used to generate signatures that verify with the according public key. Outsiders can only verify that a signature was generated by some member of the group but cannot tell which member (granting a certain level of anonymity). Generally, in this approach there exists a central authority, which can resolve signatures to individual nodes, which were issued the according private key.

This concept seems also very promising as all major requirements are met: no permanent online connection to infrastructure needed, works well in dynamic environments, privacy can be established, and the verification process can be worked out relatively fast.

8) Threshold Cryptography: All of the above trust systems relied on a physically centralized trust system. The following approach, which is based on threshold cryptography will oppose to this property and makes only use of some centralized part for initialization. The concept of threshold cryptography was first introduced by Adi Shamir [13]. The idea behind a (n, t)-threshold cryptography system is to share a secret between n parties so that any t parties can rearrange the secret. Such a system provides a greater robustness, because an malicious node has to attack at least t parties to obtain the secret.

This concept can be used to share secrets or keys in an ad hoc network [14], but the choice of t and n is quite hard. The fatality of this problem arises, when less than t nodes are available; then the whole system does not work. Due to the extreme vitality and the dissimilarity of available nodes in VANETs, this is an important issue.

B. Self-organizing Trust Establishment

Highly dynamic environments such as VANETs need an adapted form of trust establishment. Decisions regarding trust to other nodes must be made autonomously because no online connection to a security infrastructure is possible and must be based on partial information that is collected from unknown nodes during a short period of time only.

Therefore self organizing trust establishment is characterized by two properties

- there is no trusted third party such as an online infrastructure involved
- there is no global knowledge shared among the participating nodes

These properties imply that trust and the correspondent trust relationships are not static but dynamic. Trust in another node may increase, the longer this node is connected and reachable. Trust in nodes, which are visible only for a short period of time may be low. The trust model has to take this into account.

Mechanisms for self organizing trust establishment can be classified as follows (see fig. 1)

- *direct*: trust is established based on mutual communication with other nodes
- *indirect:* nodes exchange information about other nodes and the their trust relationships. This implies that trust relationships are transitive.
- *hybrid:* combines both direct and indirect mechanisms

In the following, several approaches for self organizing trust establishment will be discussed.

1) CONFIDANT: The CONFIDANT protocol, which was published by Buchegger and Le Boudec in [15], provides a possibility to detect and isolate uncooperative nodes of a mobile ad hoc network. The protocol mainly focuses on routing and forwarding aspects; it is intended to be an extension of a reactive source-routing protocol like Dynamic Source Routing (DSR). The basic principle of the protocol, namely punishing malicious and egoistic nodes, is derived from social behavior of birds in a biological experiment.

There are four main components involved in the CONFIDANT protocol, which have clearly defined responsibilities:

- The *Monitor* gathers information about the neighborhood by observing the routing protocol behavior using the promiscuous mode. If deviant behavior is registered, the reputation system is informed.
- The *Trust Manager* deals with ALARM messages, which warn friendly nodes against misbehaving nodes. The trustworthiness of these messages should be achieved by a mechanism similar to PGP.
- The *Reputation System* manages and updates the trust value of the nodes. These values are derived from own experiences, observations of the neighborhood and the incoming ALARM messages. These sources of trust are weighted according to their trustworthiness, e.g. own experiences have a greater weight than observations. If the trust value falls under a certain threshold the path manager is involved to act.
- The *Path Manager* tries to isolate malicious nodes in order to keep the vitality of the network alive. This is achieved by routing packets around these nodes and ignoring messages from them.

The CONFIDANT protocol introduces a high-level modular construction of a trust system. Anyway, there remain many open issues, e.g. the building of the friend list or the security of the protocol itself.

The deployment of the protocol in VANETs is even more problematic. CONFIDANT mainly deals with routing information, but in VANETs it is hard to distinguish between misbehavior of nodes and errors due to fast topology changes.

2) Terminodes: Hubaux and Buttyan propose in Terminodes [16] the use of a virtual currency called *nuglets* to cope with selfish nodes in ad hoc networks. Either the routing of a packet has to be paid or the packet is dropped. The main goals are on the one hand to encourage nodes to forward packets and on the other hand to discourage nodes to flood the network with too many packets. Two different paying models were introduced:

In the *Packet Purse Model* the sender has to pay nuglets for a sent packet. The main advantage is that nodes are discouraged to overload the network, but the straightforward problem of this approach is that the sender cannot know how many nuglets he has to pay as he does not know how many nodes have to forward the packet.

In the *Packet Trade Model* every node along the route trades in packets; they get payed for their forwarding service. The overall cost for the sending have to be paid by the receiver. Here, the main disadvantages are the possibility of flooding the network and denial-of-service attacks against an arbitrary receiver.

This approach, like most currency-based systems, needs a secure place to store the credits. Tamper-proof hardware is one possibility, but as seen in [17] this is not trivial. Furthermore the system does not deal with attacks, only with selfishness.

3) SPRITE: Similar to Terminodes, SPRITE [18] also uses credits to encourage selfish nodes to cooperate in the network. SPRITE mainly deals with the renumeration of forwarding messages. Every time a node receives a message he stores a receipt of that message in his local database. Later these collected receipts are sent to a central credit clearing service (CCS), which is only accessible when the nodes have an online connection to the Internet. The CCS is used as a central institution for accounting, i.e. it collects the receipts from the forwarding nodes and balances the nodes' accounts.

The SPRITE approach does not need tamper-proof hardware, because this is managed by the CCS. The central CCS could be established in VANETs, because frequent access to the Internet seems possible. Like Terminodes, SPRITE also deals with selfish nodes but not with malicious nodes. A serious problem could be the amount of receipts to be handled in the network.

4) Location Limited Side Channels: Another approach to establish a trust relation between nodes in a VANET is the use of a Location Limited Side Channel (LLSC). We use the term LLSC for a special channel, which is separated from the main communication link. The LLSC is set up in a way that an attacker cannot gain physical access to the channel (e.g. to read or inject messages). So two nodes are able to exchange critical information over a secure channel.

The main applications for LLSCs are authentication and pairing [19] of previously unknown nodes in an ad hoc network. Therefore, the involved nodes can exchange keys or hashes of keys over the LLSC to pre-authenticate themselves. The remaining steps for complete authentication are done over the normal wireless link [20]. These applications are also relevant in VANETs, e.g. as a precondition for secure communication between two nodes.

Possible technologies for establishing LLSC in VANETs are

	no online infrastr.	dynamic	privacy	timelin.	applicab.
Certificates	+	0	−	0	+
Kerberos	−	0	+	−	+
Pseudonyms	+	0	0	0	+
Blind Sign.	+	0	0	0	+
ZKP	+	0	+	−	+
NIZKP	+	0	+	0	+
Dig. Cred.	+	0	0	0	+
Group Sign.	+	0	+	0	+
Thresh. Cryp.	+	−	0	0	−
CONFIDANT	+	+	0	−	+
Nuglets	+	+	+	0	−
SPRITE	+	+	0	0	−
LLSC	+	+	0	+	+

TABLE I
EVALUATION OF DIFFERENT MECHANISMS

infrared and radar communication. These technologies have matured over the years, could provide acceptable interference liability, and are possibly already integrated in vehicles.

V. CONCLUSION

For a first evaluation, we assess the various mechanisms according the characteristics of VANETs: is an online infrastructure needed, how does the mechanism handle the dynamics in the system (e.g. how easily are new nodes integrated), does the mechanism provide for privacy of the nodes, are time-critical safety applications supported (how long does it take to establish trust between nodes), is the mechanism suited for VANET applications? The ratings are as follows: + good, 0 fair and − poor (see table I). Except Kerberos alike systems, all approaches can be run without an online infrastructure.

We rated the dynamics aspect of the infrastructure based approaches with "0" as in all systems a node has to communicate with a trusted third party first in order to get its trust material. Otherwise trust verification is not possible. Threshold cryptography was rated with "−" as e.g. new nodes cannot be integrated easily without starting a somewhat strenuous process.

The privacy aspect of pseudonyms and blind signatures was rated with "0" as the degree of privacy strongly depends on the frequency of changing pseudonyms respectively blind signatures. Blind signatures have the further privacy enhancement that neither other nodes nor the trusted authority itself can resolve the certified ID of the node as the ID is signed blindly.

The timeliness aspect of the two trust classes has to be treated differentiated: whereas in the infrastructure based approaches the time-critical part is the somewhat time consuming verification of certificates, the self-organizing trust models need quite lots of time to establish trust to other nodes dynamically (learning of each others trustworthiness, etc.) before being able to cope with safety applications.

The applicability of Digital Credentials has to be treated carefully, as the proposed mechanisms were patented. This could limit the degree of usage quite significantly if millions of cars would have to be equipped with it. The evaluation shows that some candidates (NIZKP, Group signatures, LLSC) seem quite suitable. However for a real system, the usage of only a single mechanism such as LLSC is not enough. Hence combinations of the mechanisms have to be taken into account. So at the time being, no favorite mechanism could be identified.

REFERENCES

[1] M. El Zarki, S. Mehrotra, G. Tsudik, and N. Venkatasubramanian, "Security issues in a future vehicular network," in *Proceedings of European Wireless 2002*, 2002.

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

[3] International Telecommunication Union: Telecom Standardization Sector, "Recommendation X.509: The Directory: Authentication Framework," 1997.

[4] R. L. Rivest and B. Lampson, "SDSI – A simple distributed security infrastructure," Presented at CRYPTO'96 Rumpsession, 1996.

[5] C. Ellison, B. Frantz, B. Lampson, R. Rivest, B. Thomas, and T. Ylonen, "SPKI certificate theory," Internet Draft, March 1998, iETF Network Working Group RFC 2693. [Online]. Available: http://www.ietf.org/rfc/rfc2693.txt

[6] J. Kohl and C. Neuman, "RFC 1510: The Kerberos Network Authentication Service (V5)," Sep. 1993. [Online]. Available: http://www.ietf.org/rfc/rfc1510.txt

[7] S. P. Miller, B. C. Neuman, J. I. Schiller, and J. H. Saltzer, "Kerberos authentication and authorization system," Massachusetts Institute of Technology, Tech. Rep., 1987. [Online]. Available: citeseer.ist.psu.edu/miller88kerbero.html

[8] D. Chaum, "Blind signature system," in *Proceedings of Crypto '83*, 1983.

[9] S. Goldwasser, S. Micali, and C. Rackoff, "The knowledge complexity of interactive proof-systems," in *Proceedings of the seventeenth annual ACM symposium on Theory of computing*. ACM Press, 1985, pp. 291–304.

[10] M. Blum, P. Feldman, and S. Micali, "Non-interactive zero-knowledge and its applications," in *Proceedings of the twentieth annual ACM symposium on Theory of computing*. ACM Press, 1988, pp. 103–112.

[11] S. Brands, "A technical overview of digital credentials," 2002. [Online]. Available: citeseer.ist.psu.edu/brands02technical.html

[12] D. Chaum and E. van Heyst, "Group signatures," *Lecture Notes of Computer Science*, vol. 547, 1991. [Online]. Available: http://link.springer-ny.com/link/service/series/0558/papers/0547/05470257.pdf

[13] A. Shamir, "How to share a secret," *Commun. ACM*, vol. 22, no. 11, pp. 612–613, 1979.

[14] L. Zhou and Z. J. Haas, "Securing ad hoc networks," *IEEE Networks Special Issue on Network Security*, 1999.

[15] S. Buchegger and J.-Y. L. Boudec, "Nodes Bearing Grudges: Towards Routing Security, Fairness, and Robustness in Mobile Ad Hoc Networks," in *Proceedings of the Tenth Euromicro Workshop on Parallel, Distributed and Network-based Processing*. Canary Islands, Spain: IEEE Computer Society, January 2002, pp. 403 – 410. [Online]. Available: citeseer.ist.psu.edu/article/buchegger02nodes.html

[16] L. Buttyán and J. Hubaux, "Nuglets: a virtual currency to stimulate cooperation in self-organized ad hoc networks," EPFL, Tech. Rep., 2001. [Online]. Available: citeseer.ist.psu.edu/article/buttyan01nuglets.html

[17] M. G. Zapata, "How to design wireless security mechanisms," in *Proceedings of Workshop on Security in Ad-Hoc Networks*, Ruhr University Bochum, Germany, december 2002. [Online]. Available: www.crypto.rub.de/adhocsec/Abs_Zapata.pdf

[18] S. Zhong, J. Chen, and Y. Yang, "Sprite: A simple, cheat-proof, credit-based system for mobile ad-hoc networks," in *Proceedings of IEEE Infocom*, San Fransisco, CA, april 2003. [Online]. Available: gunther.smeal.psu.edu/15502.html

[19] F. Stajano and R. Anderson, "The resurrecting duckling: Security issues for ad-hoc wireless networks," in *Security Protocols, 7th International Workshop Proceedings*, 1999, pp. 172–194. [Online]. Available: citeseer.ist.psu.edu/article/stajano99resurrecting.html

[20] D. Balfanz, D. Smetters, P. Stewart, and H. Wong, "Talking to strangers: Authentication in adhoc wireless networks," Feb. 2002, in Symposium on Network and Distributed Systems Security (NDSS '02), San Diego, California. [Online]. Available: citeseer.ist.psu.edu/balfanz02talking.html