This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE CCNC 2010 proceedings

Establishing Email-based Social Network Trust for Vehicular Networks

Dijiang Huang*, Zhibin Zhou*, Xiaoyan Hong♭, Mario Gerla♮
* Arizona State University, ♭ University of Alabama, ♮ University of California - Los Angeles

***Abstract*—We propose a vehicular network trust model that integrates cryptography-based entity trust and email-based social trust. The entity trust provides security protections such as origin integrity, data integrity, and confidentiality. The social trust provides a level of belief on the data transmitted by an entity. To achieve the email-based social trust, we require each user to run an automated agent that performs trust evaluation checks and processes trust checking requests. The requests are from their highly trusted contacts or through a trusted proxy server maintained by the email service provider. We utilize identity-based cryptography (IBC) to integrate entity trust and social trust. This allows us to use a unique identity (e.g., an email address) for each entity. Further, we use the IBC based attribute based cryptography to develop secure group communications in vehicular networks. Finally, we present research challenges and potential research directions to extend this work.**

***Index Terms*—Email Social Trust, Vehicular Network.**

I. Introduction

Vehicular Ad hoc Network (VANET) applications require a security mechanism for distributing application relevant information to neighboring vehicles. Usually, the communications in VANETs are classified as Vehicle to Vehicle (V2V) and Vehicle to Infrastructure (V2I). However, before these applications can be deployed, security and privacy issues have to be addressed. Among these issues, establishing trust among drivers is most critical and is the essential prerequisite for many VANET operations.

Previous solutions [1] proposed security services for achieving messages and source authentication, message confidentiality, non-repudiation, etc. While establishing entity trust using PKI certificates is an effective method, further exploration of using social trust among drivers or passengers can help strengthening the above entity trust. The social trust in vehicular networks is essential, since many vehicular related applications not only require cryptographic protections on transmitted data, but also require a level of confidence on sending/accepting the data to/from their communication peers. For example, a driver may not trust another who sent a message "there is an accident on the Highway 10, south bound, exit 205, please detour" just by knowing his/her certified ID. Likewise, a female driver stranded at the side of the highway because her car broke down may be more willing to accept the offer of a ride from a "trusted" passing by driver (in her social network) than from a "certified" driver whose identity is guaranteed by the authorities. In general, although the identity of the originator is secured by public key based cryptography, a driver still needs to decide if the received message, or the offer, is trustable or not. Thus, it is important to include social trust in vehicular network communications and enhance the trust relationships among drivers and passengers.

In this paper, we propose a comprehensive trust management solution for VANETs by integrating social network trust models and cryptography based solutions. As example of social networking, we utilize the well established email system and use e-mail interactions among drivers to build social trust. Our approach can be generalized and applied to other popular "mobile" social networks, for instance the networks stemming from physical contacts among nomadic users. These "proximity" networks have been extensively used in "people" P2P systems such as Haggle [2] and Pocket Switching [3]. The e-mail social network paradigm offers several interesting properties outlined below:

(a) With the development of lightweight mobile devices, one can check emails through cell phones, laptops equipped with wireless cards, vehicular wireless stations, etc. This makes e-mail a "mobile" social trust builder: mobile users send e-mails (possibly embedded in SMS) to each other to keep in touch while traveling together and coordinate their movements. Moreover, email-based trust can be conveniently checked in real-time through an automated client agent.

(b) The structured nature of email allows us to evaluate trust among email users with minimal overhead. For example, email services usually have filter setups, such as moving important emails to a special folder, putting close friends' emails with label "friends", transferring Spams to a spam folder, and so on. These filters enforce a certain level of trust measures between the email receiver and his/her contacts.

(c) In addition, most of the web based email services also include software, such as chat, to allow close friends to talk over the Internet and to monitor their interactions. For example, Google's online chatting maintains the talking history in a separate folder. This information can provide a further measure of trust among email users.

(d) The email service will also provide statistics for each contact email address such as frequency of exchanging emails in the past year, month, week, etc., which will allows for incorporating the trust factor of timing. More sophisticated data mining techniques can also help us check the nature of a contact through key words used to express emotion, attitudes, relations, etc.

(e) As per data provided in [4], there are more than 650 million accounts for web based emails provided by Microsoft, Yahoo, Google, and AOL. North America has more than 20 percent of overall Internet users by 2006 [4]. As of today, almost every employee in Government and Industry and every student has at least one email account. The main benefit of using email based social network is that its trust value is more

978-1-4244-5176-0/10/$26.00 ©2010 IEEE

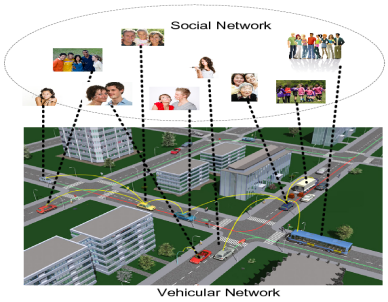

Fig. 1. Vehicular network architecture.

accurate than that of other social networks since we tend to rely on email services for most transactions in our daily life.

To establish email-based social network trust, we propose a trust query system, which provides distributed trust evaluation and query services. The prototype is provided at [5]. We must note that the query system builds on the premise that email addresses can be partially disclosed in spite of privacy concerns about third-party use. The user will disclose only certain sets of e-mail addresses and only to users he/she trusts. The trust query service has two main functions: (i) calculating trust between an email user and all his/her contacts to build a trust ranking list; and (ii) querying trust for a particular email address from his/her trusted contacts. To implement e-mail trust, vehicles exchange their IDs when they meet. To ease the key management overhead, we propose to use identity-based cryptography to verify each other's identity and set up common session keys. As previously discussed, the entity trust does not provide trustworthiness among email address owners. Thus, we use the trust query service to evaluate the level of trust for received email addresses. Once the email trust is set up, two vehicles can use an established shared key for later communication phases. To address the communication efficiency on the road, we also proposed a secure group communication solution by using identity-based cryptography.

The contributions of our research are as follows: (i) we present a novel email-based trust framework beyond identity trust, (ii) we present a comprehensive solution to incorporate social trust and cryptography, and (iii) we outline the research directions for the research communities in both social networks and vehicular networks.

The rest of paper is arranged as follows: in Section II, we present a trust architecture of vehicular networks; in Section III, we present the social trust model and attacker model; the integrated solution on setting up vehicular and social trust models are presented in Section IV; finally, we present several on-going research challenges in Section V.

II. System and Models

For the purpose of this study, we will define two layers of networks in a vehicular communication system: vehicular ad hoc networks (VANETs) and people's social networks (SocialNets). As shown in Fig. 1, a vehicle is the carrier that moves people in the urban grid. A general VANET communication scenario consists of vehicles and Roadside Units (RSUs). The vehicles can use a variety of communication techniques, such as 802.11 based wireless cards, Dedicated Short Range Communications (DSRC) technology [6] and WiMAX to communicate with the neighboring vehicles and the RSUs. In addition, vehicle riders can use their mobile devices, such as mobile phones, to establish social trust through social networks already established among pedestrians.

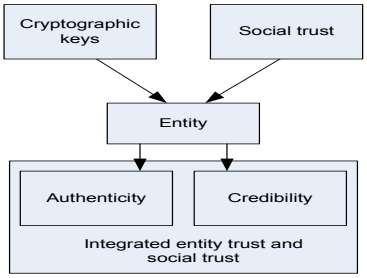

Fig. 2. Integrated entity trust and social trust.

The goal of social network trust is to establish confidence in peer actions during the vehicular communications exchange. As shown in Fig. 2, the main incentive of using both cryptographic keys and social trust models is to improve entity trust and provide users with a certain level of confidence on sharing/retrieving information to/from a vehicle.

To integrate entity trust and email-based social trust, we use email as the user identity. Since email address is unique, this allows us to utilize identity-based cryptography [7], [8] and make the email address as the public key for a user. Before using email IDs for authentication, each user must register at a trusted authority and derive his/her corresponding private keys. For secure communications, each user just needs to broadcast his/her email IDs. Upon receiving an email ID, the user will run a trust checking program on the received ID.

Communication model: The communication model includes two networks: vehicular network and social network over the existing Internet. The vehicular network model comprises physical network components such as: on-road units, off-road units, and the interfacing layer. The on-line trusted authority, usually managed by a local transportation department office, uses Internet based security services through RSUs or cellular networks for establishing trust. This approach will provide maximum flexibility and robustness to build up trust among vehicles. Off-road units consist of trusted authorities (TA) which can provide identity-based public key certificate services for users to derive their private keys and identity certificates. Communications between off-road and on-road units is enabled through the interfacing layer, i.e., the Internet.

Attack model on email social trust: The attackers can perform the following attacks: (1) breaching privacy of email users, e.g., disclosing email users' contact list, (2) impersonating an email user with valid or fake email addresses, and (3) vandalism of the email trust framework. Attackers can be from many sources. They are interested in putting together a holistic or partial picture of an email user's friends and associates.

III. Trust in Email Social Networks

In this section, we present the properties and design issues of email social networks.

A. Email based social relationships

People connections of all different types are set up through daily email exchanges. Thus, setting up an email-based social network can be relatively easy with less effort in extra

configurations. The application can present users with the opportunity when they log into the email system, and proceed with very few clicks or initial decisions. We tend to check our email daily, hourly. As a result, recurring engagement with your social network is easier than with destination social networks. Generally, people are more serious about their email related activities than open social network environments. This is the key advantage of email-based social networks over their counter-parts.

We can build email-based trust among users with the following information associated with an email account. (1) Contact list and email groups: e.g., Google Mail automatically puts all involved email addresses in the users' contact list. This feature is very useful for each user to maintain his/her social network connection with little maintenance efforts. (2) Email exchange frequency can be used to set the initial relationship trust level with someone else. Lots of recent backs-and-forth means possible strong bounds among email users. There can be a lot of one-way emails to you, which means it might come from an email list. Few two-way emails means you have a weak relationship. (3) The address book categories - personal, work - can become relationship definition metadata. (4) If a user does not have his/her email address book organized by relationship types, we can analyze the key words to categorize the relationship, such as romantic, friendship, professional, etc. (5) The e-mail service is currently made more personal because it displays messages more prominently from people who are more important to you. The inbox you have today is based on what people send you, not what you want to see. In general, email users categorize the emails from the people that they care about most. Thus, using email-based trust is a way to save time on making your own decisions about these relationships. Each email user can also actively engage with his/her social network, and take full control of the email-based social networks centered by the user.

B. Increase incentive of using social networks

Restriction of existing well known social networks is that the subscriber can read the updates of people just by declaring that he/she wants to. However, a key factor of email-based social network, you do so knowing that NOT anyone can read your personal information. Therefore, every user either needs to opt-in to having their updates read by their email contacts, or you must send a friendly request to whomever you want in your social network. Typical types of relationships are friends, common interest, professional, etc. We hold the opinion that different social networks are good for different types of relationships. Being a one size-fits-all is not easy.

In the context of vehicular networks, encouragements for drivers and passengers to export their email services for VANET trust are very important. The encouragements reside in two aspects. First, if we can build a concrete trust among vehicles, which are bootstrapped by using email-based social networks, more users will be encouraged to participate. Second, abundant information can be exchanged on the road through existing well established Internet-based applications, such as instant message, emails or RSS feeds, etc. These Internet-based applications can help drivers to achieve multiple benefits in enhancing driving safety, reducing congestions, and improving on-road entertaining experience.

IV. Setup inter-vehicle trust using social networks

A. Trust model of email service

We propose two trust models to handle email-based social trust: (1) peer-to-peer trust model, and (2) decentralized business trust model. In the peer-to-peer trust model, we assume each user will be able to run an email trust checking agent (TCA) software. The TCA will be running at the user's client device. It performs the following two main operations: (a) send trust checking requests, and (b) perform trust checking and ranking. After two users exchange their email addresses, they perform trust checking based on their email accounts. First, they need to check their contact list (L), labels or folders to check if the email address is L. If the email account (u) is found, they will use a trust evaluation algorithm running by the TCA to rank the trust level of their communication peers. A typical ranking scheme includes trust levels: (HT) high trust, (T) trust, (NT) not trust, and (U) unknown. If the TCA returns HT, T, or NT, the user will respond depending on pre-setup policies. For example, if the TCA returns U, it will form a trust checking request and send the request to its T and HT contacts. The detailed algorithm is presented as follows:

Algorithm (Trust Checking)

Receives request req(ID) to check the trust of ID.

```
1.  if ID is in the contact list L
2.      if Check(ID)==HT
3.          performs action(HT)
4.      if Check(ID)==T
5.          performs action(T)
6.      if Check(ID)==UT
7.          performs action(UT)
8.  elseif H<threshold
9.      H=H+1
10.     sends req(ID)||H to ∀u ∈ L(T, HT)
11. else
12.     return fail.
```

In the trust checking algorithm, if the req(ID) is received from other users, the *action* function will response to the requester with the corresponding trust level. If the algorithm returns an unknown (U), it will also check if the request path length (H) exceeds the *threshold*; if not, the TCA will generate a request and attaches the increased H to his/her contacts with the trust levels T and HT, otherwise, the TCA will return a "fail to find" to the requester.

For the decentralized business model, we consider that there exist multiple business domains. Each domain maintains its own trust checking server for its email users. In general, a business domain, usually a company, will control its own email services. Thus the trust checking can be done by constructing a trust graph based on the email data in the server. This is an effective method to compute the trust and each user does not need to run TCA's trust checking function. Instead, each user just sends a trust checking request to their email provider. The email provider will check the request and see if the checking email ID is in the same domain and then return the trust checking value; otherwise, the provider can use DNS and forward the request to another business domain that can handle the social trust checking. This trust checking procedure is similar to the procedure of BGP inter-domain routing protocol. Mutual trust checking agreement is required to be setup among different business domains.

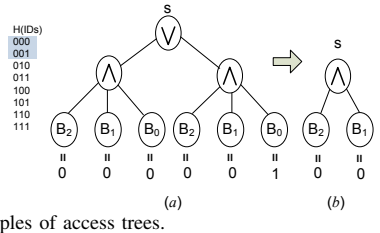

Fig. 3. Examples of access trees.

B. Establishing trust in vehicular networks

We propose to use identity based cryptography to integrate the email-based social trust model. Identity based cryptography requires a trusted Private Key Generator (PKG) to compute a unique private key component for each user's email address. Here, we refer a PKG as the trusted authority (TA). As presented in Section IV-A, the vehicles can exchange their identities (i.e., the drivers' email addresses) before they exchange data. Once a user finishes the trust checking on a received email address, the email address can simply be used as the public key to establish a session key. Usually, multiple drivers can exchange their email addresses, thus efficient secure group communications may require to be set up. To this end, we utilize our proposed group key management solution [9] for establishing a group key among users. Here, we present its basic construction. We use ID_k to represent the email address of user k. The TA generates a private master key MK, and a set of public parameters *Param* known by every user.

Before communication, a user is required to derive his/her private key S_k for ID_k by the TA. Moreover, a set of private key components is also distributed to each user using the following two-step key generation procedure: (i) TA runs the key generation algorithm that takes a set of predefined attributes S of a user as inputs and outputs a private key SK including multiple private key components with respect to each attribute in S. Here, the set of attributes is determined by the hashed bit sequence of a user's email address, which is represented by $H(ID_k) \rightarrow \{0,1\}^b$, e.g., $H(ID_k) = B_{b-1}B_{b-2}...B_0$. Thus, $H(ID_k)$ can be uniquely identified by the set of attributes $S = \{A_{i,B_i} | \ i \in \{0,1,\ldots,b-1\}\}$. An attribute A_{i,B_i} denotes "the i^{th} bit of $H(ID_k)$ is B_i", i.e., one bit position maps two attributes (one for value 0 and one for value 1). For example, $B_2 = 1$ maps to attribute $A_{2,1}$ and $B_2 = 0$ maps to attribute $A_{2,0}$. (ii). Once the set of attributes is determined by a user, we can use CP-ABE [10] to generate a set of private key components represented as SK for the user. After the key generation procedure is finished, each user will have a private key S_k for his email address ID_k, and a set of private key components SK which is mapped to each attribute identified by $H(ID_k)$. In other words, an email ID uniquely identify two private keys S_k and SK. The public/private key pair $\langle ID_k, S_k \rangle$ is used for traditional identity-based encryption, decryption, and signature. The public/private key pair $\langle ID_k, SK \rangle$ is then used for secure group communication in vehicular networks. In this way, we can efficiently incorporate email addresses with cryptography based operations. Now, we will discuss how to use $\langle ID_k, SK \rangle$ for secure group communications.

Once a user wants to set up a group communication with multiple users in $G = \{ID_k | k = 1\ldots, n\}$, he needs to construct an access tree that only selected group members in G can access the secret key encrypted at the root of the tree. To illustrate the group construction, we present a toy example to illustrate our solution, which is shown in Fig. 3. Our solution allows any user to construct an access control tree (e.g. trees in Fig. 3), so that only receivers who satisfy the access control tree can decrypt the message. Here, we present a toy example for a group containing 8 group members. Each group member is mapped to a unique binary ID (derived by hashing their email addresses), from 000 to 111. Each group member is preinstalled a set of secrets by the TA, i.e., a private key consists of multiple private key components, and a unique private key component is mapped to each bit position in its $H(ID_k)$. For example, if a group member's $H(ID_k) = B_2B_1B_0 = 000$, three private key components sk_2, sk_1, sk_0 are mapped to bits: $B_2 = 0$, $B_1 = 0$, $B_0 = 0$, respectively. Now, suppose user 000 wants to communicate with a group containing 000 and 001, he can simply combine two access control trees by adding a $\vee$ operator as shown in Fig. 3(a). Using this approach, the complexity of the combined access control tree is bounded by $\Theta(l \cdot log(n))$, where l is the size of group and n is the size of $H(ID)$ space. To reduce the complexity of the access tree, we can further reduce the access control tree from 6 leaves to 2 leaves as shown in Fig. 3(b) using the Boolean Function Minimization (BFM) techniques [11]. Note that the access tree shown in Fig. 3(b) is unique for group members 000 and 001. Thus, only 000 and 001 can satisfy the access tree and use extended CP-ABE [10] to decrypt the Date Encrypting Key (DEK) s at the root. In general, for a given group with size n, the complexity of both computational overhead and storage overhead is $O(\log n)$ [9]. For user ID_k, to encrypt a message M for a group of users confined by the access tree $\mathcal{T}$, he can use the following encryption form:

$$ID_k || \mathcal{T} || E_{\mathcal{T}}(s) || E_s(M) || Sig(S_k),$$

where S_k is the privacy key of users identity ID_k. In this way, we can use the email trust model to bootstrap the vehicular network trust. Once receiving the encrypted message, a user can first use the signature to validate the message and check if sender's $H(ID_k) = 000$ satisfies the access tree $\mathcal{T}$. For the presented example in above, we just need to see if the leading bit and the second bit values are 0s. Then, the user follows the decryption procedure to decrypt the session key s as presented in [10]. Finally, he can use the session key s to decrypt the message.

V. Conclusion and Future Work

We have proposed an integrated solution to address trust issues in vehicular networks. There are still many research issues that need to be answered. We identify several important ones and corresponding potential research directions.

Online and offline issues: The trust provided through email services may experience long delay due to network latencies, and the locations of email trust management entities to check the contact lists. Some users may choose to keep the contact list/trust management utilities at the mail servers, so to enjoy the flexibility of reading emails when they move. Some users may choose to keep the contact list/trust management utilities at the mail servers, so to enjoy the flexibility of reading emails when they move. Some users may have local copies.

Other users may use whatever their default configurations provide. Furthermore, some may have concerns about their hand-helds' storage and computation limitations to perform trust checking. If contact lists cannot be obtained from local copies, network connections to the servers are needed when performing the trust searches and validations. In some vehicle network scenarios, connection may be intermittent or short-lived. The possible scenario of the lack of instant connection suggests that a back-up plan could enhance the use of email-based trust in vehicular network applications.

On the other hand, we argue this trust service will be very useful to jumpstart the VANET trust at bootstrap phases. Thus, we need to provide reliable connections for V2V and V2I communications that can be used to strengthen the availability of the social network trust. As the matter of fact, e-mail has become one of the most important services for mobile users (pedestrians and drivers). For vehicles in the urban grid, the Internet is just one hop away. Thus, Email based trust can be introduced quick and helpful.

Pre-setup membership of trust group: The email trust can be classified for weak and strong trusts. Though "human filters" have been applied when accepting emails, the inherited security of the email senders, for example, a buggy client, may be more complicated than what the frequency or the number of emails implies. For the VANET application, where a strong trust is a must, a pre-setup is necessary. This pre-setup procedure should promote the users to further scrutinize the contact lists proposed by the email systems (we discussed them as trust agents). For this reason, such an email-based trust network can be regarded as a private network, where each node has only a view about their neighbors (in contrast to social networks like LinkedIn).

Performance issues: delay and hit rate: One way to extend the email-based social trust is to "pre-fetch" the trust. Ideally, a vehicle should set up trust before it can communicate with other cars. Since the VANET communication is usually ephemeral, a long delay in trust establishment makes the social trust scheme impractical. Thus, we prefer to predict the location of the vehicle and the need to join different groups along the way whenever possible. Thus, we require the trust establishment to be location predictive and situation aware [12], i.e., a vehicle can predict its future location and set up trust in advance with vehicles that have great chances to exchange information. This demands research in predictable and proactive VANET communication protocols.

Proactive and prediction requirements: One way to extend the email-based social trust is to "pre-fetch" the trust. Ideally, a vehicle can set up trust before they can talk. Since the VANET communication is usually ephemeral, long delay of trust establishment makes the social trust establishment impractical. Thus, we prefer the road situations should be predictable. To this end, we require the trust establishment to be situation aware [12], i.e., a vehicle can predict its future location and set up trust in advance with vehicles that have great chances to exchange information. This demands research in predictable and proactive VANET communication protocols.

Peer-to-peer trust evaluation: In peer-to-peer networks such as Bit-torrent, the trust builds on the nodes' reputation to upload files. Such a reputation can be observed based on network traffic activities. However, the email-service trust extends from pure network activity based trust to sophisticated human behavior and psychology fields. Such a shift poses the most challenging issue for this work. If possible, enhancement could pull data from community, police, Department of Motor Vehicles (MVD), and hospitals. In turn, all these issues are highly sensitive to privacy claims and may be only available off-line.

Privacy Considerations: Privacy consideration is the most critical issue when email users are requested to expose their email addresses (and their contacts addresses) during vehicular communications. Some of the email addresses are publicly known, this is especially true in the academia world. However, some email addresses are used only for internal purposes. For example, some companies restrict the email addresses used for non-business purposes. Our proposed solution can only protect users' privacy for not exposing each user's contact list. This is achieved by using a "distance vector" type of trust path exploration, i.e., each user only knows the trust level via one of his/her friends but does not know the exact trust path to the requested user. In order to prevent exposing the email address, especially for protecting companies' private email information, we need to exploit solutions that utilize proxy trust management (ie, cryptography protected delegation) services. For example, if we can allow a company's email service to run the trust checking, instead of exchanging email addresses, a user just need to exchange a reference number. This reference number is only recognizable by the company's email server to map to an internal email address.

REFERENCES

[1] P. Papadimitratos, L. Buttyan, J.-P. Hubaux, F. Kargl, A. Kung, and M. Raya, "Architecture for Secure and Private Vehicular Communications," in *Proccedings of the 7th International Conference on ITS Telecommunications*, 2007.

[2] J. Scott, P. Hui, J. Crowcroft, and C. Diot, "Haggle: A networking architecture designed around mobile users," *IFIP WONS*, 2006.

[3] P. Mutaf, "Pocket Bluff: A cooperation enforcing scheduled pocket switching protocol," *INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE, Technical Report NO. 5664*, 2005.

[4] Email marketing report, available at http://email-marketing-reports.com, April 2008.

[5] Secure Networking and Computing Research Group, Arizona State University, "Email Trust Services," https://www.wreferral.com/EmailTrust/faces/index.jsp, 2009.

[6] C. Cseh, "Architecture of the dedicated short-range communications (DSRC) protocol," *IEEE Vehicular Technology Conference (VTC)*, vol. 3, pp. 2095–2099 vol.3, May 1998.

[7] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," in *Proceedings of the CRYPTO 01, Springer-Verlag*, 2001.

[8] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the weil pairing," in *Proceedings of the Asiacrypt 2001, volume 2248 of LNCS*, 2001, pp. 514–532.

[9] Z. Zhou and D. Huang, "BGKM: An Efficient Secure Broadcasting Group Key Management Scheme," Cryptology ePrint Archive: Report 2008/436, http://eprint.iacr.org/2008/436, October 2008.

[10] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *IEEE Symposium on Security and Privacy*, 2007, pp. 321–334.

[11] E. McCluskey, "Minimization of Boolean functions," *Bell System Technical Journal*, vol. 35, no. 5, pp. 1417–1444, 1956.

[12] X. Hong, D. Huang, M. Gerla, and Z. Cao, "Sat: Building new trust architecture for vehicular networks," in *Proceedings of the 3rd ACM International Workshop on Mobility in the Evolving Internet Architecture (MobiArch)*, 2008.