SAT: Situation-Aware Trust Architecture for Vehicular Networks

Xiaoyan Hong
University of Alabama
Tuscaloosa, AL 35487
hxy@cs.ua.edu

Dijiang Huang
Arizona State University
Tempe, AZ 85287
dijiang@asu.edu

Mario Gerla, Zhen Cao
University of California
Los Angeles, CA 90095
gerla@cs.ucla.edu
caozhen@nrl.cs.ucla.edu

ABSTRACT

Establishing trust in vehicular networks is a critical but also difficult task. In this position paper, we present a new trust architecture and model - Situation-Aware Trust (SAT) - to address several important trust issues in vehicular networks that we believe are essential to overcome the weaknesses of the current vehicular network security and trust models. Our model also strengthens the tie between Internet infrastructure. The new SAT includes three main components: (a) an attribute based policy control model for highly dynamic communication environments, (b) a proactive trust model to build trust among vehicles and prevent the breakage of the existing trust, and (c) a social network based trust system to enhance trust and to allow the set up of a decentralized trust framework when the vehicular network is under infrastructure failure or under attacks.

Categories and Subject Descriptors

C.2.0 [**COMPUTER-COMMUNICATION NETWORKS**]: General—*Security and protection*

General Terms

Security

Keywords

Vehicular network

1. INTRODUCTION

Vehicular networks (VNETs) enable communications from mobile vehicles to fixed roadside infrastructure and also from vehicles to vehicles. The networks are expected to greatly enhance the experience of safe driving and improve the efficiency of the roadway systems. In addition, many information and Internet driven applications are also proposed, for examples, commercials, entertainment, content distribution, mobile sensing, etc. These applications are specially tailored to tackle the unique features of the high mobility and geographical stretch, e.g., exploiting location specification (location based services) and/or peer-to-peer dissemination (e.g., carTorrent [10]). All these VNETs applications rely on a trustworthy, secure, and reliable network infrastructure for providing correct traffic and road system data as well as application data. Nevertheless, traditional secure and trust framework is incapable in such a highly dynamic and mobile communication environment.

Architectural designs for secure vehicular network [12, 11, 7, 8, 13] mainly focus on building entity-level trust based on traditional shared and public key management solutions. The prime concerns of *entity trust* are authentication, message integrity, and users' privacy, where messages must be authenticated to prevent external attackers from injecting, altering and replaying messages, and messages should not disclose identities and locations. Recently, the concept of "*data-centric trust*" is used to summarize the research that deal with the correctness of the reported data [14, 15].

However, early work leaves many important factors not fully considered in order to meet the strict trust and security requirements for VNETs. In this paper, we identify the following factors for further investigation. (i) VNETs face a variety of situations and quick changes between situations, which require the corresponding security and privacy policies be able to reflect the situations and be adaptive to the changes. (ii) The sporadic interconnections among vehicles cannot provide a reliable communication channel to actively establish trust at many instants when the time is critical. (iii) A trust model can be built on social networks that have been already established in existing Internet based virtual communities.

In this paper, we propose new research directions through introducing a new trust model and the associated architecture. We describe a novel trust model called "Situation-Aware Trust (SAT)", which is quite different from traditional entity trust and data trust. In addressing the aforementioned weaknesses, we leverage Internet infrastructure to strengthen the design. The contributions of our research include using descriptive attribute based cryptographic solutions to efficiently perform policy control for various situations, building both off-line and on-line trust policies and requirements for proactive and predicting future trust situations, and transforming trust from Internet social communities to VNET to enhance and promote VNET applications. The rest of the paper is organized as follows. Section 2 introduces the new trust concept - *Situation-Aware Trust*. Section 3 describes the architecture to realize the SAT model.

MobiArch'08, August 22, 2008, Seattle, Washington, USA.

Section 4 presents the security related issues of SAT. Section 5 concludes the paper and points out the future work.

2. CONCEPT OF SITUATION-AWARE TRUST

The concept of Situation-Aware Trust (SAT) is inspired by the observations on various VNET application situations. We first describe what is a situation and then introduce the new concept: *situation-aware trust.*

2.1 VNET Situations

Some representative application situations are listed here. (a) *Situation 1*: 10am of 3/16/08, a policy car informs vehicles on highway 10, driving between the exits 114 and 116 north bound to slow down due to an accident at the exit 116; (b) *Situation 2*: a road information system provides services to its own large fleet of vehicles and business partners; (c) *Situation 3:* a VNET application allows the cars to collect traffic and environmental data (or car content distribution), especially those commuters who'd like to use their time better during their daily long drive. (d) *Situation 4*: components of vehicular network infrastructure can be malfunctioning or fall due to attacks or disasters, etc.

Each of the above described situations represents a group of situations that share similar properties, such as: an event that affects a certain region with immediate processing needs, a service that has a clear organizational boundary for its users, an application that allows users sharing common interests to join, and a system that incorporates survivable and reliable design.

2.2 Situation-aware Trust

The new concept of "trust" in VNETs introduces entity and data attributes, social and proactive factors to handle various situations and their changes. Particularly, our solutions focus on three main aspects: (i) policy control, (ii) proactive trust establishment, and (iii) social network impacts on establishing trust. We elaborate these three aspects below. SAT targets at providing situation-aware and proactive trust system.

Trust built on attributes: Traditionally, trust is categorized as entity trust and data trust [15]. The entity trust requires the evaluation of the trustworthiness of an entity (an identity, a license number, or a pseudonym), which is usually performed by using authentication. The data trust requires the evaluation of the trustworthiness of the data (event, data), which is usually performed by using data integrity checking. Location and time are very critical data, and they can be verified using passive or active verification solutions. For situation-awareness, we identify a broader scope of entity and data trust. We use attributes to describe them. Attributes abstract entity and data trust at a certain level, they can be used to identify a group of entities (e.g., taxes associated with a company, police cars in a city), a type of events (e.g., accidents, congestions), or the property of events (location-based services, road traffic updates). Attributes can be further classified as dynamic attributes and static attributes, depending on whether the attributes change frequently or remain the same during a relatively long period of time compared to ephemeral connections of VNETs. Vehicles that fulfill a set of descriptive attributes form a group. Considering these attributes as policies associated with that group, we introduce the new concept of "*policy group*". Our research is inspired by the observations on the existence of policy groups among various VNET situations. From the point of view of trust scope, each situation will have different requirements for secure communication and data correctness with respect to a certain group of stake holders. For example, a policy group can be a group of vehicles confined by their attributes, such as common interests, security or service requirements, or environmental constraints (such as street name, time, driving direction, etc). A policy group is specified by the information source and is organized automatically without relying on a trust party to manage the group.

Proactive trust: Another important factor of trust establishment in SAT is its proactive aspect. The proactive trust overturns the traditional reactive trust, which is started only if the system events occur. For examples, a vehicle and a roadside unit start negotiating cryptographic keys when they are within each other's communication range. Such a method has been identified challenging due to the high speed. This shortfall exists in all situational examples presented previously, which requires each VNET component to be prepared for situation changes. Thus, the proactive trust demands the trust to be set up in advance by predicting future trustworthy situations and proactively using the vehicular networks to set up trust in advance. Such proactive trust establishments can be very useful for active safety applications, such as cooperative collision warning, can play a critical role in reducing crash loss which were as high as 40,000 lives and $230 billion according to the National Highway Traffic Safety Administration (NHTSA) [1].

Social trust: Social networks are playing an important role to build up trust among human beings in Internet based communities. Since VNET is driven by humans, we propose using social networks for setting up trust among vehicles. In particular, the social network is very useful when the VNET application is running among people and in the scenarios when the roadside network infrastructure is not available or under attacks. The situational examples 3 and 4 presented in Section 2.1 explain such needs.

3. SAT ARCHITECTURE

In this section, we describe the secure Situation-Awareness Trust (SAT) architecture and supporting cryptography tools and communication protocols and research challenges associated with them.

3.1 SAT Architecture Description

SAT architecture is a middleware agent running at each vehicle. It includes two function layers: a *situation awareness trust layer* (SAT layer) and a *supporting and trust layer* (STL). The main goal of SAT layer is to enable the SAT trust model among vehicles and the STL is to support the SAT layer to achieve its goal. Figure 1 demonstrates the major functional blocks and their relations in SAT architecture.

With SAT architecture, each vehicle will be able to decide its actions according to its SAT layer statuses. Building the statuses involves four main steps: (i) perception, (ii) comprehension, (iii) projection, and (iv) decision.

Perception is supported by various networking and sensing devices, and their running protocols. The perceived events must be correct and with origination from trusted sources. The perception involves the processes of monitoring, event

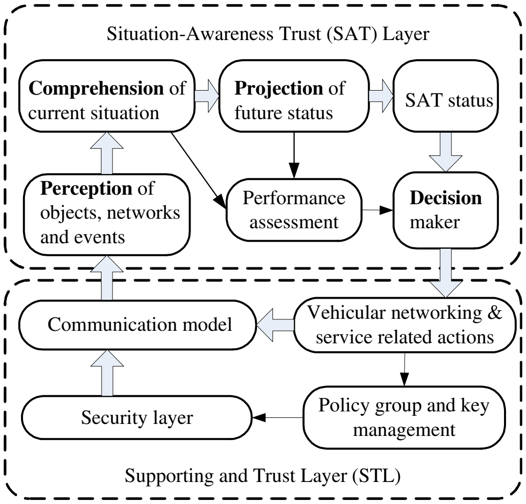
Situation-Awareness Trust (SAT) Layer
Comprehension of current situation
Projection of future status
SAT status
Perception of objects, networks and events
Performance assessment
Decision maker
Communication model
Vehicular networking & service related actions
Security layer
Policy group and key management
Supporting and Trust Layer (STL)

Figure 1: SAT Architecture.

detection and recognition. The latter leads to the awareness of multiple situational elements, such as neighboring vehicles, road conditions, roadside units, and environmental factors, such as locations, event timing, networks availability and connectivity, failures, attacks, etc.

Comprehension involves a synthesis of disjoint SAT perceptions through the processes of integration perceived situational events, i.e., through the processes of classification, aggregation, optimization, and prioritization. It requires to integrate the perception information to understand how it will impact upon the security services running on vehicular networks and corresponding actions of each individual vehicle. The process of comprehension includes developing a comprehensive picture of the trust status of the vehicle's neighbors and potential (through prediction) remote communication peers.

Projection is to project the future trust status for a vehicle on road. Projection is achieved through the knowledge about the vehicle itself, the dynamics of the vehicular networks and the results of comprehension. The process of SAT projection is to extrapolate the SAT comprehension information in real-time to determine how it will affect future trust states among vehicles and the vehicular networks for a certain road condition.

SAT layer includes a assessment model to evaluate the performance of SAT processes and SAT statuses. The SAT performance assessment model takes the current SAT status from the comprehension model and then compares it with the predicted trust status generated previously from the projection model. Both the SAT status and the assessment results are sent to the decision maker, where the vehicle needs to perform corresponding actions to maintain existing trust and to establish future trust. Service requests will be made through the decision maker, and they require further processes through the supporting and trust layer.

The STL provides security and privacy policy enforcement and networking services for SAT layer. It includes two main components: (i) a security layer for efficient policy management and coordination among different trust domains (e.g., a centralized party vs. distributed social networks) and (ii) a communication model for proactive trust establishment. STL is driven by the vehicular networking and service requests derived from the SAT layer. A service request describes the policy group, which specifies a set of attributes, such as the vehicular type, location, time, applications, services, etc., to identify the potential participants in the vehicular communications.

3.2 Building SAT Architecture

Developing the aforementioned SAT architecture requires a systematic and comprehensive study with innovative approaches in both cryptographic solutions and trust establishment protocols. In this section, we describe a sketch of our approaches approaches that have the following three key components: policy representations, attributed based policy enforcement, and proactive trust establishment protocols.

3.2.1 Attribute based Policy Group

Traditional entity trust and data trust are not sufficient to address complicated situations and corresponding security policy requirements. Additional policy enforcement mechanisms, such as group management and key distribution center, are required to handle situations and their changes. Thus, the research challenge is how to integrate policy enforcement and key management to improve the trust establishment performance in a highly dynamic communication environment.

Let us take the following example first. It highlights the salient features of our research in dealing with various situations. Similar to the situation 2 presented in Section 2.1, we have a taxi driver who works for a small company A, which does not have an operator to distribute information to their drivers. The driver wants to tell other drivers in the same company that there are many guests waiting for taxies on a particular road segment of Washington street. In this situation, the data privacy and the origin integrity are required to ensure the business secret. Then, the driver can send the following message through VNETs:

$$attributes(companyA \text{ AND } taxi \text{ AND } Washington\ St. \\ \text{AND } 10 - 11am : 3/28/08)||cipher||sig_{companyA}. \quad (1)$$

In this example, *attributes(companyA AND taxi AND Was -hingtonStreet)* specifies the policy enforced in the message on who can decrypt the message, i.e., if a taxi belongs to the A and it happens to be on the Washington street, the taxi can decrypt the message. The message is encrypted by the presented attributes (using attribute based encryption (IBE) scheme [2]). The message is valid in the time interval 10-11am, 3/28/2008. Here the message is required to be validated by the company's name through the identity based signature $sig_{companyA}$. This also provides a certain level of anonymity for the sender (using identity based signature (IBS) scheme [4]). This example presents a concise and integrated approach to deal with policy group formation and key management.

The formation of a policy group is different from traditional security group formation in that no clear definition and enforcement of a group boundary is required. This property is very useful in a vehicular communication system, since a vehicle usually does not care which entity it communicates with. In Figure 2, a policy tree (PT) is presented, where all attributes are leaves and the logic operators are internal nodes. As long as the receivers can satisfy the security/privacy polices, must they be able to decrypt the message, i.e., decrypt the root. In Figure 2 (left tree), we

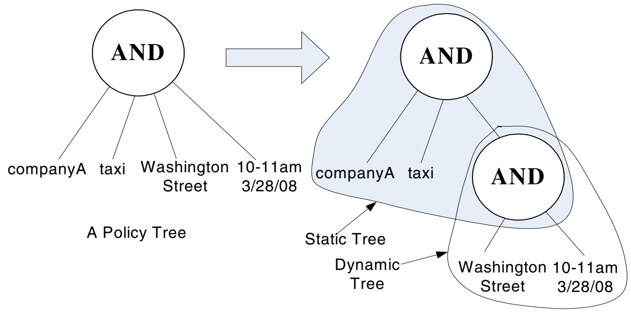

Figure 2: A Policy Tree Example.

present a policy-tree example based on the previous example presented in (1). The four attributes $\{A_1, A_2, A_3, A_4\}$ are the leaves in the tree. Further, in the right tree of the Figure, we use the attributes and the associated logic among them to represent a revised security policy: $PT = (A_1\ AND\ A_2 AND\ (A_3\ AND\ A_4))$. When performing related cryptographic operation, only if each attribute is true (i.e., the user own the attribute and corresponding private key), the user can traverse the logic operations to the root, which means the whole PT is true. If the PT is true, then the user can decrypt the cipher encrypted by the top level secret (i.e., a date encrypting key).

Some policy-tree based attribute examples are presented in Table 1. Note that we use attributes and associated logic among them to represent a security policy.

Table 1: Vehicular network policy group examples

Static Attributes	Dynamic Attributes	
Vehicle Attributes	Road Attributes	Surrounding Attributes
Vehicle Category	Road Direction Road Intersection	Emergency Event Hi Security
Vehicle Application or Service	Road Name Road Segment Number	Time Stamp Date
Network Category	City Name State Name	Privacy Protection Network Situation
Social Networks	Community name, Interests group ID, Self-defined credentials, and so on.	

3.2.2 Policy-based Group Key Management Scheme

Based on the policy tree, we require that a receiver of a cipher-text should be able to decrypt the message enforced by the PT as long as it has enough number of attributes to satisfy the logic from the bottom to the top of the PT. To enable such capabilities, we utilize the basic formation of attribute-based encryption (ABE) scheme [2], which utilize the identity based encryption (IBE) [3] and threshold secret sharing scheme [17]. Here, we consider each attribute as an identifier. The logic operator is realized by using the threshold secret sharing schemes. We highlight key management procedure as follows. (a) Sender encrypts a message by encrypting the data-encrypting key (DEK) based on secret sharing schemes through a top-down fashion of the PT. The encryption breaks the DEK in to multiple secret shares, and then recursively running a secret sharing scheme for each secret share down to the bottom level. Such a secret share is uniquely one-to-one mapped to a public known attribute at the bottom level of the PT. (b) Using the DEK to produce the cipher text and produce signature scheme. (c) The message receiver performs the decryption in the reversed order of the encryption by running the secret sharing scheme recursively from the bottom of the root of the PT to recover the DEK.

We must note that each private key component is derived for a unique public attribute and each user will be distributed with a different private key (containing multiple secret shares), even two users share the same set of attributes. This is a very important property that we utilize to enforce desired policies and build secure group communications. In essence, the attributes and logic operators construct the policies, and users share the same set of attributes in the policy tree form a secure communication group.

Our solution distinguishes it from the ABE [2] scheme by using a decentralized trust framework (for details, see [20]). The decentralized servers can be deployed through road side units (RSUs) or through well deployed cellular networks. The private key components of inherited attributes, such as vehicular attributes, can be derived in advance using an off-line method via a universal trusted authority. The secrets of dynamic attributes can be derived from a local on-line trusted server, such as an RSU, or can be managed by the vehicle itself using the social network based solution. As shown in Figure 2 (right tree), we refer to the policy tree created by the off-line trusted authority as static PT $(s - PT)$ and the policy tree created by the on-line trusted parties as dynamic PT $(d - PT)$. By combining the $s - PT$ and $d - PT$, we can prevent single point failure and enforce the security and privacy policies.

3.2.3 Build up SAT through Internet Infrastructure

SAT differs from early VNET trust frameworks in using the Internet infrastructure. SAT has a large scope of attributes that are available to construct various policy groups in ephemeral VNETs. Some of the attributes are static, which can be generated off-line. And some are dynamic which are associated with time and location of a particular vehicle. In SAT architecture, Internet trust infrastructure plays dual roles. SAT uses the static attributes derived off-line and uses them with dynamic attributes derived on-line for verifications. The off-line trusted parties like traditional certificate authorities provide the standard key management services for users to derive their static attributes and corresponding private keys. The on-line trusted party should use Internet based security services through road side units (RSUs) or cellular networks for establishing dynamic policy trees. This approach will maximally enable the flexibility and robustness to build up trust among vehicles. Moreover, the proactive features of SAT are achieved through vehicular ad hoc networks as well as Internet (through access services provided by RSUs or Cellular networks) to provide robust network connectivity for setting up trust in advance. Furthermore, when roadside network infrastructure is not available, SAT explores social networks, which have been already established in current Internet communities to sustain SAT services under extreme situations.

3.3 Social Network Models for VNET

Due to the high speed of vehicles and the short connecting time among them, it is challenging to establish entity trust among vehicles in VNETs. Here we explore social networks in Internet to enhance entity trust for VANETs. Recent work has observed that vehicular communities according to interests, activities, and daily commutes are useful in designing data dissemination protocols [6] and defending against Sybil attacks [23]. The advantage is that when mobile nodes' wireless contacts are not stable due to mobility, their relationships built within the social network overlay are relatively stable and can be used to compensate trust loss due to connection loss. We describe how to leverage the power of social networks to bridge trust among vehicles.

The motivation of using social networks is twofold. First, in case of infrastructure failure when no reliance on the road side units can be used, social networks will provide trust service within and across social communities. Secondly, social networks serve as an effective incentive for VNET users. The Internet social websites such as Facebook, MySpace would never win such popularity if they had not leverage the social network properties among Internet users. The VNET is not an exception. Our question is: "Can we build a vehicular social network to enhance the trust among users and increase their incentives to adopt our proposed SAT architecture?" To answer it, several important research issues need to be addressed. (a) How to establish vehicular social communities and manage the trust among them. (b) How to incorporate the social network with the SAT architecture to enforce attribute based situation-aware trust.

Constructing the social communities in vehicular networks is a challenging problem due to the high speed of vehicles and short contact time incurred. Social communities can be established in various ways. For example, drivers may join a supermarket community via electronic credentials released by its administrator. Moreover, leveraging social trust within a community and social trust across communities are challenging issues but are necessary when one community network is below the critical mass.

In the SAT architecture, one important consideration is to identify attributes shared by social community members in order to enforce policies in SAT. For examples, the static attributes can be the community name, Internet ID, credentials, certificates, etc.; and the dynamic attributes can be interest, social event (scheduled on demand), and social relationship (evolving with time). In addition, in the exceptional scenario where the infrastructure fails and a group of vehicles want to share some sensitive information, they can enforce a policy by the group leader and construct the policy tree as in Fig.2, which is not only an immediate application in an emergency scenario but also serves as an incentive mechanism to promote cooperation.

4. SAT AND SECURITY MODELS

Vehicle networks will not only improve the safety and the efficiency of the transportation system, but also assist communications in emergences such as planned evacuation [16] or unexpected disastrous failure of key infrastructure components (e.g., roadside unit support). When an emergence or infrastructure failure occurred, a secure and quick communication path to empower VNET in performing the above tasks are very important especially when potential human lives are involved. However, in the exceptional situations, many functions of SAT architecture are greatly challenged as well as traditional VNET protocols. How to sustain the challenges and continuously continuously provide trust service requests, often, they are tightened security requests, becomes a critical issue to SAT architecture. We investigate two extreme situations for SAT architecture: the failure of roadside units and the failure of GPS services. We also list security enhancements that SAT provides.

The situation of unavailable accesses to the roadside infrastructure or the connection services can occur in many cases, for examples, dense urban deployment transiting to less deployed suburban areas or rural areas, operational failure at certain regions, infrastructure broken down due to disasters or attacks. Such an exceptional situation poses a challenge to the policy tree and group key formulation. In SAT architecture, a policy tree includes the static subtree $s-PT$ and dynamic sub-tree $d-PT$. The dynamic subtree is derived from an on-line server through road side unit (RSU) Internet access. The common components in a $d-PT$ include a time period, road name, moving directions, etc. When the RSU fails, a vehicle can still use the $s-PT$ to perform basic policy enforcement functions. However, this compromises the level of trust that SAT architecture provides. The challenging issue is to investigate approaches that can restore the SAT architecture trust levels, or, improve the static policy enforcement if a fully compatibility level is not reachable. Thus, the social network trust will play a great role in this situation.

Another exceptional situation is the unavailable of GPS services, such as construction blocking, no GPS or faulty GPS devices, GPS service outages [9] or under attack. It has been shown that civilian GPS devices can be jammed and spoofed by GPS satellite simulators which transmit stronger radio signals, so fake GPS signals can flood the real GPS signal [21]. SAT architecture is greatly challenged by this situation, because location is an elementary attribute that will be used by constructing policy trees and group keys. To deal with the situation to enable SAT to build trust without GPS data, relative location based neighborhood topology (RLBT) can be an underlying element for trust and communication [19]. RLBT is a map showing the relative locations of cars in vicinity (e.g., in-front-of or following cars, left or right lanes). Existing work has studied obtaining and validating accurate relative locations [5, 22]. Situations of a short period of GPS outrage are also studied through relative positioning and dead-reckoning systems [9, 18]. For SAT architecture, a relative position system must have security built in. Typically, the relationship of the IDs in terms of their neighboring relation, must be verified.

VNETs are vulnerable to various security and privacy attacks. They can be in the following four dimensions [13] (capital letter notates the type): (1) Insider vs. Outsider, (2) Malicious vs. Rational, (3) Active vs. Passive, (4) Local vs. Extended. SAT strengthens VNET security (traditionally, entity trust and data trust) by enforcing policy based keys to provide additional security features that meet demands for various situations. Here we enumerate well-recognized attacks and common solutions used to protect vehicle networks using SAT architecture, shown in Table 2. Please note that DDoS attacks can also be decomposed to attacks like packet dropping, inject false data, etc.

5. CONCLUSIONS AND FUTURE WORK

The new concept "Situation-Aware Trust (SAT)" and related architecture are introduced in this paper. The SAT architecture uses descriptive attributes to efficiently perform security policy control, builds in mechanisms for predicting

Table 2: Attacks to VNET and defense methods

Attacks	type	Trust model	Defend methods
Impersonate	I.R.A.*	Entity trust	Authentication
Sybil attack	I.R.A.*	Entity trust	Authentication
Drop packets	I.R.A.*	Entity trust	Watchdog
Inject false data	I.R.A.*	Data trust	Majority rule
False location	I.R.A.*	Data trust	Location verification
Message fabrication	I.R.A.*	SAT trust	Policy based key
Message cracking	*.M.A.L	SAT trust	Policy based key
Selfishness	I.R.P.L	SAT trust	Incentive and punishment
location tracking	*.R.*.L	SAT trust	pseudonym, loc. cloaking
DoS	*.*.A.L	SAT trust	reputation, client puzzles

future trust situations, and transforms trust from Internet social communities to VNET trust to enhance and promote VNET applications. The secure Situation-Aware Trust architecture establishes solutions to achieve SAT.

With the introduction of the above concepts, we point to more research efforts in this direction. Here are two major research issues for future study: (i) Attribute based encryption (ABE) is the basic to integrate the policy control and security services for SAT. Issues such as how to add the authentication capability in ABE and how to effectively combine the $d-PT$ and $s-PT$ require further investigations. (ii) Social networks will play a great role in the future vehicular system. We will investigate the social models to construct a vehicular social trust model by adopting the research results from the current Internet community study.

6. REFERENCES

[1] Report and press release Ű the economic impact of motor vehicle crashes, 2000. National Highway Traffic Safety Administration website.

[2] J. Bethencourt, A. Sahai, and B. Waters. Ciphertext-policy attribute-based encryption. In *Proceedings of the 28th IEEE Symposium on Security and Privacy (Oakland)*, 2007.

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

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

[5] C. Chigan, V. Oberoi, and J. Li. Rpb-macn: A relative position based collision-free mac nucleus for vehicular ad hoc networks. In *Proceedings of Globecom'06*, 2006.

[6] E. Daly and M. Haahr. Social network analysis for routing in disconnected delay-tolerant manets. In *Proceedings of MobiHoc*. ACM, 2007.

[7] M. Gerlach, A. Festag, T. Leinmuller, G. Goldacker, and C. Harsch. Security architecture for vehicular communication. In *Proceedings of the 5th International Workshop on Intelligent Transportation (WIT), March*, 2007.

[8] M. Gerlach and F. FOKUS. Trust for Vehicular Applications. In *Proceedings of the Eighth International Symposium on Autonomous Decentralized Systems (ISADS)*, pages 295–304, 2007.

[9] Kukshya, V.; Krishnan, H.; Kellum, C. Design of a system solution for relative positioning of vehicles using vehicle-to-vehicle radio communications during gps outages. *Vehicular Technology Conference 2005*, 2:1313–1317, October 2005.

[10] K. C. Lee, S.-H. Lee, R. Cheung, U. Lee, and M. Gerla. First Experience with CarTorrent in a Real Vehicular Ad Hoc Network Testbed. In *Proceedings of IEEE Workshop on Mobile Networking for Vehicular Environments (MOVE'07), April 2007.*

[11] 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.

[12] B. Parno and A. Perrig. Challenges in securing vehicular networks. In *Proceedings of HotNets-IV*, 2005.

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

[14] M. Raya, P. Papadimitratos, I. Aad, D. Jungels, and J. Hubaux. Eviction of Misbehaving and Faulty Nodes in Vehicular Networks. *Selected Areas in Communications, IEEE Journal on*, 25(8):1557–1568, 2007.

[15] M. Raya, P. Papadimitratos, V. Gligor, J. Hubaux, and S. EPFL. On Data-Centric Trust Establishment in Ephemeral Ad Hoc Networks. In *Proceedings of IEEE Infocom*, 2008.

[16] S. Rizvi, S. Olariu, M. Weigle, and M. Rizvi. A novel approach to reduce traffic chaos in emergency and evacuation scenarios. In *Proceedings of the IEEE Vehicular Technology Conference*, Oct. 2007.

[17] A. Shamir. How to Share a Secret. *Communications of the ACM*, 22(11):612–613, 1979.

[18] Q. Shengbo, D. Keliang, and L. Qingli. An effective gps/dr device and algorithm used in vehicle positioning system. In *Proc. of IEEE ITS Conference*, Oct. 2003.

[19] L. Tang, X. Hong, and P. G. Bradford. Secure Relative Location Determination In Vehicular Network. In *Proceedings of 2nd International Conference on Mobile Ad-hoc and Sensor Networks (MSN 2006), Dec. 2006*, Hong Kong, China.

[20] M. Verma and D. Huang. Attribute based group communication in vanet. Arizona State University, Technical Report. `http://dj.eas.asu.edu/VANET.pdf`, 2008.

[21] J. S. Warner and R. G. Johnston. Think GPS cargo tracking = high security? Think again. Technical report, Los Alamos National Laboratory,2003.

[22] G. Yan, G. Choudhary, M. Weigle, and S. Olariu. Providing vanet security through active position detection (poster). In *Proceedings of ACM VANET 07*, Sept. 2007.

[23] H. Yu, M.Kaminsky, P.B.Gibbons, and A.Flaxman. Sybilguard: Defending against sybil attacks via social networks. In *Proceedings of Sigcomm'06*, September 2006.