Situation-Aware Trust Architecture for Vehicular Networks

Dijiang Huang, Arizona State University

Xiaoyan Hong, University of Alabama

Mario Gerla, UCLA

ABSTRACT

We present a new trust architecture — Situation-Aware Trust — to address several important trust issues in vehicular networks. SAT includes three main components: an attribute-based policy control model for highly dynamic communication environments a proactive trust model to build trust among vehicles, and prevent the breakage of existing trust, and an email-based social network trust system to enhance trust and to allow the set up of a decentralized trust framework. To deploy SAT, we utilize identity-based cryptography to integrate entity trust, data trust, security policy enforcement, and social network trust, allocating a unique identity, and a set of attributes for each entity. We conclude by presenting research challenges and potential research directions that extend this work.

INTRODUCTION

Vehicular ad hoc networks (VANETs) will enable vehicle-to-vehicle and vehicle-to-roadside communications and are expected to greatly enhance driving safety and improve roadway system efficiency. However, widespread deployment and penetration will heavily depend on users' perception of the VANETs as a readily available, secure, reliable, and trustworthy infrastructure for providing accurate traffic and road system data. The state-of-the-art research on VANET trust has mainly focused on building entity-level trust and data-centric trust [1]. The former is based on shared and public key management solutions, where messages must be authenticated to prevent external attackers from injecting, altering and replaying messages, as well as to prevent eavesdropping and location tracking. The latter is to assess the credibility of the reported data. Recent research publications have studied the use of both entity and data trust for authentication while preserving privacy and accountability, in robust broadcasting or multi-hop message disseminations [2].

Solutions based on entity-level trust and data-centric trust still face many challenges raised by the complex vehicular communications system that includes dynamic user groups, stringent real-time constraints, and heterogeneous communication environments, which make existing entity trust and data trust methods ineffective. Considering the broadcast nature of the medium, multi-hop routing, and multiple communication paradigms (from broadcast with specific geographic zones to multicast within a large organization); also considering the short duration of vehicle to vehicle sessions — usually a few seconds — the establishment of VANETs trust in a timely fashion becomes critical. Existing entity or data trust is usually based on an individual user, security-on-demand approach. This method cannot deal efficiently with trust establishment in a highly dynamic and ephemeral communication environment. For example, while conventional message encryption can be a solution for access control, it requires a few rounds of message exchanges for secure key establishment among entities and trust verifications on data items, greatly slowing down the response time. The issue is especially serious in view of VANET safety applications' real-time constraints. Furthermore, existing VANET trust management solutions have very limited capability to support secure data access control and in particular, group-based secure access considering the broadcast nature of VANETs.

To highlight our research motivations, we present the following three illustrative scenarios. *Scenario 1*: following an emergency (say, a fire, a chemical spill or a bomb threat) in a certain area of the city, police headquarters broadcast an alert message to enable qualified vehicles (e.g., patrol cars, fire trucks, ambulances) in selected locations near the scene of the accident to take over the control of traffic lights in order to facilitate rescue and carry out orderly vehicle evacuation. The light control can be performed using a challenge-response protocol: if the vehicle can decrypt and answer the challenge, then it can control the traffic lights. The vehicle must also validate its location with respect to scene of accident, in order to prevent the control message from being read by other vehicles in the wrong locations. This situation is representative of a class of VANETs applications that require to validate — with low processing latency — both the roles (e.g., police patrol car) and the locations (near a designated intersection) of the

0163-6804/10/$25.00 © 2010 IEEE

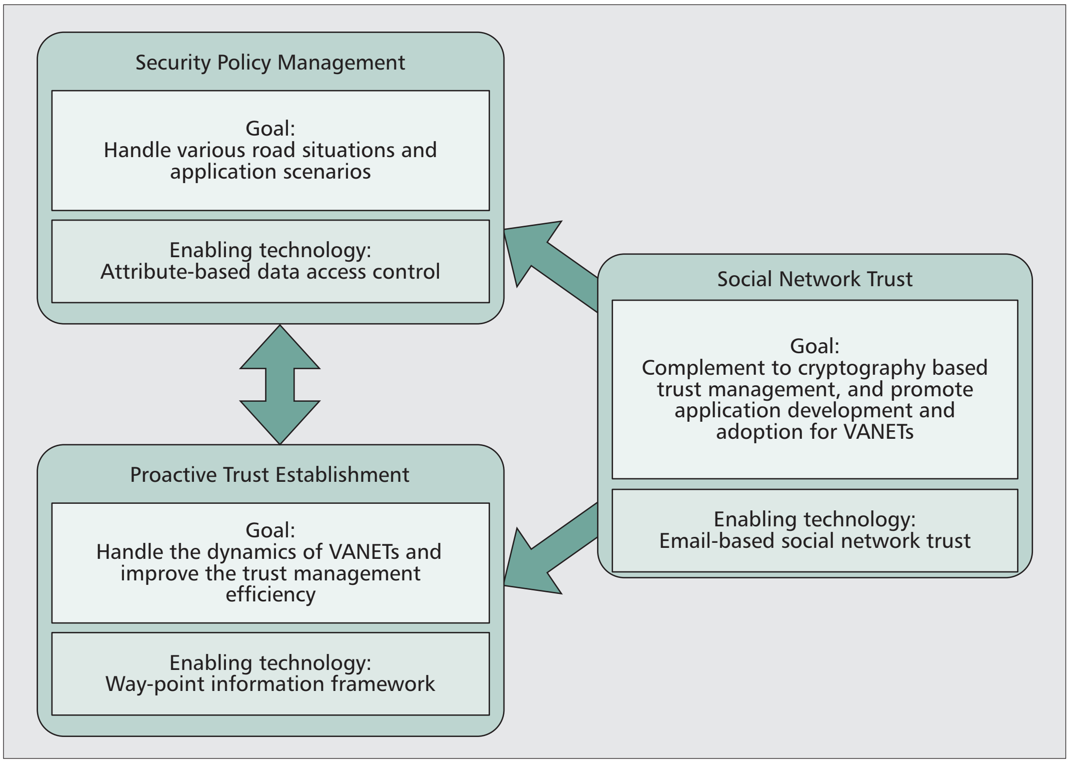
Security Policy Management
Goal:
Handle various road situations and application scenarios
Enabling technology:
Attribute-based data access control
Social Network Trust
Goal:
Complement to cryptography based trust management, and promote application development and adoption for VANETs
Enabling technology:
Email-based social network trust
Proactive Trust Establishment
Goal:
Handle the dynamics of VANETs and improve the trust management efficiency
Enabling technology:
Way-point information framework

Figure 1. *System components, goals, and enabling techniques of SAT architecture.*

These quite different examples (location vs. affiliations vs. social network trust) all point to the need of exploring an efficient and predictive trust system to reduce on-the-scene trust setup latency. To this end, we present a new trust architecture, situation-aware trust (SAT).

associated entities. Note that these validations require a long chain of message exchanges using existing schemes, thus leading to long response delay. *Scenario 2*: a peer-to-peer information system provides services to its community of drivers. For example, a taxicab has learned that customers of a major convention will be waiting after the banquet for cabs at a Hotel on Washington St., 10am 8/25/2009. It informs fellow cab drivers of the same company of this opportunity. It wants to broadcast this information only to drivers belonging to his company, and as a further restriction, only to the drivers who, given their current location, are expected to reach Washington St. in time. This example is representative of applications where data access control is based on the organizational affiliation bounded by the effective intervention time period. It requires group shared keys to be established dynamically and on the fly. Using the earlier proposed schemes, it will require multiple steps of message exchange with long delay. Scenario 3: a social network trust network can be viewed as an overlay layer on top of the vehicular communication networks. Suppose social network trust is established between driver *A* and driver *B* through a social network. They can use their social network associated credentials, e.g., cryptographic keys, to establish secure channels between them when needed. This situation suggests that some trust relationships may already exist and can be explored to help reducing the latency of establishing trust and keys in the two previous scenarios.

These quite different examples (location vs. affiliations vs. social network trust) all point to the need of exploring an efficient and predictive trust system to reduce on-the-scene trust setup latency. To this end, we present a new trust architecture, *situation-aware trust* (SAT) [3], for VANETs to address the trust management issues identified by the above scenarios. SAT includes the following three key architectural design components:

- Security Policy Management to address a number of trust situations and application scenarios on-road
- Proactive Trust Establishment to manage VANET dynamics and build inter-vehicle trust in a timely fashion
- Social Network Trust to incorporate people factors in the VANETs trust establishment in addition to cryptography based trust management solutions, in which more applications can be developed and adopted using VANET communication environments.

Compared to previous trust management in VANETs, SAT adds new enabling techniques to achieve the described system components: using an attribute-based data access control scheme to handle dynamic changes of VANET applications complying with various data access security policies, building a way-point information framework to support cryptographic tools and communication protocols for proactive trust management, and applying email-based social network trust to support and enhance current secure VANET communications. Figure 1 describes the architecture of SAT.

In summary, the goal of SAT is to build a new trust model using architecture and cryptographic tools that provide predictive trust information and quick and flexible key management, thus improving driving experience. SAT is inspired by the observation that there exist many different requirements for secure communica-

Similar to many secure mobile communication systems, SAT needs to address various active and passive attacks. For example, active adversaries can forge and inject malicious packets, or modify and replay previously captured packets; passive adversaries can also learn information from captured packets.

tion and data correctness with respect to a certain group of vehicles in a certain application situation; an event that affects a certain region with immediate processing needs, or a service that has a clear organizational boundary for its users. In the following sections, we provide detailed descriptions of SAT.

RATIONAL AND PRINCIPLES OF SAT

EFFICIENT CRYPTOGRAPHIC APPROACH FOR VANETS DATA ACCESS CONTROL

In SAT, we use a cryptography-based approach that allows data access control by defining attributes of receivers. Attributes describe the properties of corresponding entities or data as studied in entity trust and data trust. Attributes are treated as multiple public key components using attribute-based cryptography [4] and they can be used to identify common properties for a group of vehicles, which can enforce data access control policies for a group of vehicles. Particularly, we call the group of entities that satisfy the attributes specified in a policy statement as a *policy group*. For example, the policy group qualifier can be taxicabs in a company, police cars in a city, a type of events (e.g., accidents, congestions), a set of common interests shared among vehicles, a set of security or service requirements, a set of road/environment constraints (e.g., street name, time duration, driving direction), or a combination thereof. Attributes can be further classified as static and dynamic attributes, depending on how frequently the attributes change in VANETs. Typically, dynamic attributes are tied to road segments and effective time duration.

PROACTIVE TRUST ESTABLISHMENT IN VANETS

Existing VANET trust management solutions (e.g., 1609.2) assume that certificates are issued before the actual communication act. SAT provides an assistant framework to distribute certificates to vehicles before the actual communications among vehicles and RSUs. On the other hand, SAT also provides a framework to reduce unnecessary trust establishment actions among vehicles encountered on the road. Particularly, knowing the attributes of an encountering vehicle can help in deciding whether establishing the trust is required. To this end, SAT uses a proactive approach to establish trust with intended vehicles before they meet. This approach requires that each vehicle predicts the potential meeting peers by distributing its moving trajectory to others.

USING SOCIAL NETWORK TRUST FOR VANETS

SAT adopts social network trust as part of SAT architecture to bootstrap trust, which can also add incentives for users to adopt VANET-based services. SAT particularly investigates email-based social network trust [5]. Such a trust and related usable values can be made usable for message communication through automated agents installed within the on-board vehicle communication units. The interaction can be triggered when a passenger uses his/her email services. Extracting social network trust from email services has many attractive advantages with respect to other social networks:

- Email services usually provide a natural and intrinsic layer of protection, e.g., scrutinizing the untrusted emails through spam filter and manually setup filtering rules.
- Email management systems usually have already encapsulated some services that help to establish email-based social network trust. For examples, managing labels or folders to classify emails, statistic information such as email exchange frequency, priority level, email receiving dates, etc.
- Email IDs are unique, which can be easily integrated with identity-based cryptography system.
- Email trust can potentially provide a very large trust database covering majority of population, which can maximally benefit for general users.

SECURITY ANALYSIS OF SAT

Similar to many secure mobile communication systems, SAT needs to address various active and passive attacks. For example, active adversaries can forge and inject malicious packets, or modify and replay previously captured packets; passive adversaries can also learn information from captured packets. Traditional cryptography based security services, e.g., Public Key Infrastructure (PKI), can be used to protect VANET communication through authentication, confidentiality, and integrity security solutions. However, SAT is designed to assist these solutions to counter the above described security threats in a more effective way by proactively exploiting the strategies and solutions proposed in the early work that use PKI for security and privacy for traditional entity trust and data-centric trust [1, 2]. Moreover, SAT integrates policy-based data access control that cannot be effectively addressed using PKI-based solutions.

SAT ARCHITECTURE

In this section, we first describe the system model of SAT. Then, we present the basic construction of secure attribute-based policy enforcement and group key management. Followed by the traffic management model to support proactive trust management, we present the integration of email-based social network trust in SAT.

SAT SYSTEM AND TRUST MODEL

The SAT system model includes vehicles, Road-Side Infrastructure (RSI), and Internet. The RSI is composed by Road-Side Units (RSUs), interconnections among RSUs, and servers running control and management functions. Particularly, we assume a global trusted agent that is in charge of the basic credentials distribution, e.g., keys are pre-installed through the global trusted agent when a vehicle is manufactured or registered. Additionally, multiple local trust agents can also be deployed when each is responsible for situation detection, monitoring and local trust management through RSUs in their designated geographical areas. Both the global trusted agent and local trusted agents are inter-connected and can be reached by vehicles through RSUs. Vehicles are equipped with wireless communication devices to establish connections among vehicles and to RSI. We also assume that inputs from GPS devices or digital navigation systems are available to provide locations or travel trajectories. The vehicles include hardware and software that supports general vehicle-to-vehicle (V2V) or vehicle-to-infrastructure (V2I) communication. They also have tamper resistance devices to store critical data such as equipment identifier (EID) and cryptographic keys. The existing PKI-based secure communication package can be installed as well [2].

Constructing Policy Groups for Vehicular Networks

Attribute-based cryptography [4] greatly improves the efficiency of secure communication among multiple vehicles. The efficiency is due to the nature of using attributes that provide two major benefits. First, specifying desired attributes naturally incorporates data access control policies into the data encryption. The attributes specified in a data access tree structure, which will be illustrated later, are actually the data access control policies enforced on the ciphertext. Second, the attribute-based cryptography is suitable in a vehicular broadcasting environment, where the message intended receivers cannot be predefined through a group establishment procedure due to the mobility. Thus, using attribute-based approaches, we can confine data access based on various roles of vehicles. Such a policy specific action makes the use of creating cryptography-binding policy groups [6]. For examples, cars can be classified based on their functions or roles (e.g., police cars, ambulances, general civilian vehicles, and commercial vehicles); and cars can also be classified as they are designed for special functions or particular networking applications. Attributes can also be dynamic according to on-road situations, such as location, times, and events, which are considered to form a policy group. Additionally, there are many static attributes such as car types, affiliations that can help to construct an on-the fly dynamic communication data access in an efficient way [7]. Each static attribute is associated with a unique private key that is derived from a global trusted party, e.g., Motor Vehicle Division (MVD). The dynamic attributes and corresponding private keys can be derived from a local trusted party, e.g., a local server connected through an RSU. In this way, a decentralized trust framework is formed by global and local trusted parties. As a result, defining a policy group is to define a collection of multiple attributes and their logic connections (usually are AND and/or OR gates)to allow data decryption by legitimated vehicles.

We present a policy tree example based on the second illustrative scenario presented in Introduction to highlight the salient features of SAT to construct a cryptography-binding policy group for dynamic data access control. Figure 2 left details a policy tree that defines the policy formed by AND gates for the taxi car example where location and time are mapped to a real scenario. To differentiate the static and dynamic attributes, a sub tree for dynamic attributes is re-created by connecting through another AND gate to the static part (Fig. 2, right). This policy tree represents the following policy enforcement:

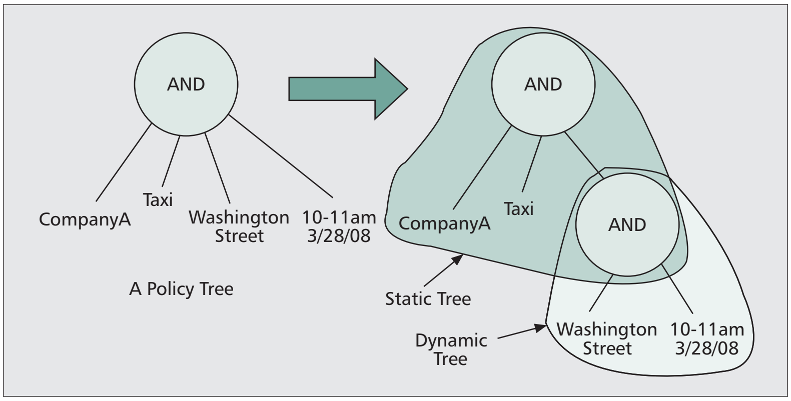

Figure 2. *A policy tree example.*

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

The cryptographic method backing up the above data access is for each attribute to be considered as a public key component. Thus, the data access tree is a set of public key components and logic operators. The outcome of the policy tree is the generation of the Data Encrypting Key (DEK) S for encryption and decryption. This tree is sent with the ciphertext. The associated private key components should be available at each associated vehicle. Whoever receives this message will first to determine if it is an eligible receiver, i.e., it must satisfy the policy tree, and then it can compute the DEK S using its stored private key components with respect to each attribute in the tree. As a result, only vehicles having the right set of the private keys can legitimately decrypt the ciphertext.

In Fig. 3, we present an example based on Ciphertext-Policy Attribute-Based Encryption (CP-ABE) [4]. In this example, attributes $A1$–$A4$ are arranged as leaves nodes of the attribute tree, where each attributes is corresponding to a set of secret key components $S1$–$S4$ assigned to users $u1$–$u3$. We note that the private key components assigned $u1$–$u3$ are different even if they own the same attribute. We use different colors to highlight the difference of private key components. Thus, $u1$ has private key components {*red*: $S1$, $S2$, $S3$, $S4$}, $u2$ has private key components {*green*: $S1$, $S2$, $S4$}, and $u3$ has private key components {*blue*: $S1$, $S2$, $S3$}. The internal nodes of the attribute tree are logical gates, such as *AND*, *OR*, which are implemented using threshold secret sharing scheme [8]. The secret S can be reconstructed by using two secrets S' and S''. At the bottom level the encryption is performed using identity-based encryption (IBE) [9], which considers each attribute as a public key. $S1$–$S4$ are considered as the private keys for the corresponding attributes. To satisfy the *AND* gate, the decrypter must have all the secrets to recon-

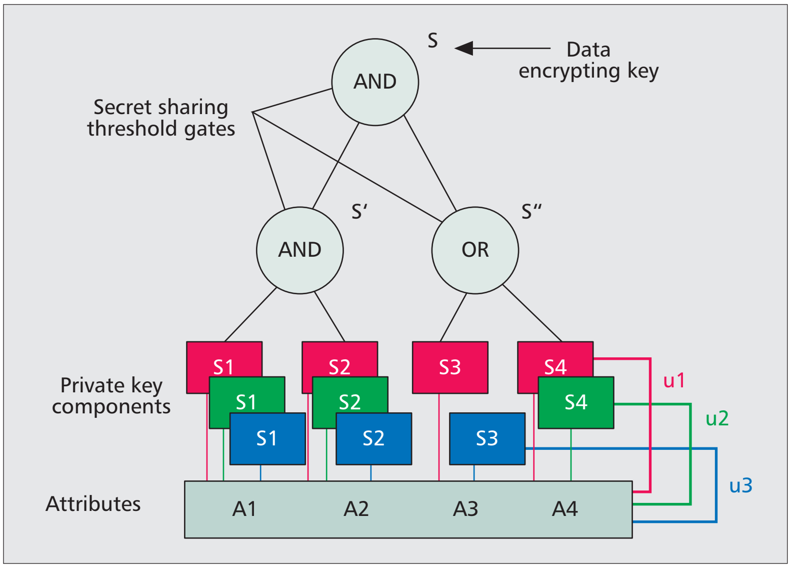

Figure 3. *Attribute-based encryption.*

struct the higher level secret; to satisfy the *OR* gate, the decrypter is only required to have one of secrets at the lower level to reconstruct the parent-level secret. In this way, the encryption algorithm of CP-ABE is performed in a top-down manner by constructing the ciphertext to the bottom level of the attribute tree; and the decryption algorithm of CP-ABE is performed in a bottom-up manner using the users' pre-distributed secrets to reconstruct the higher level secrets until derive the root-level secret (i.e., the DEK). In this presented example, based on the pre-distributed secrets, $u1$–$u3$ can decrypt the secret S and thus they can access the data encrypted by using the DEK S.

We must note that, using the presented approach, it is efficient to enable multiple vehicles to access the message even if the message sender does not know whether the receivers can receive the message or not. This approach brings the major benefit of flexibility in that the sender does not need to negotiate a group key with the intended receivers to send a message. However, this also brings up a new problem, i.e., how to create an attribute tree to effectively cover the most intended receivers in VANETs. We will address this question in the next section.

Establish Proactive SAT Trust in VANETs

By dividing the information needed to access messages into static and dynamic attributes, SAT is able to identify various cases that the trust information needed for each vehicle to collect and propagate. More important, it is able to help vehicles to predict future possible trust relations on the road. The way-point information framework (WIF) [10] is a mechanism that SAT uses to address the tight time constraints to establish trust.

The data unit in WIF, namely, the way-point information is composed by trajectory information bounded by approximated time stamps, which can be derived from an embedded digital navigation system. A typical way-point record includes two types of information:

- Static attributes: Vehicle type, preferred security policies, etc., which are derived from the global trusted agent
- Vehicle moving properties: Moving direction, average speed, etc., which can help local trust agents to predict the location of the vehicle at a given time.

By knowing the way-point information from each vehicle, a local trust agent can generate appropriate dynamic attributes and help vehicles to construct a policy group using both static and dynamic attributes.

WIF can be applied using one or both of the following approaches: a decentralized traffic prediction system with the help of RSI or a purely distributed way-point information system model when RSI is not available.

WIF with RSI Support — The inputs from a navigator computation give the best paths to given destinations, and predict future times and locations based on the travel speed, direction, and possibly global traffic information obtained from the global and local trusted agents.

Clearly, road traffic conditions affect the accuracy of way-point computations. Thus, we associate a probability distribution to way-point values. The way-point information is lightweight and concise. It is only transmitted in every a few minutes. RSI must maintain a set of local servers (or agents) to collect and process way-point information. This can be done very efficiently using a Distributed Hash Table (DHT). The DHT, or the Navigator Server (NS), maintains up to date information on road traffic conditions. Typically, the global traffic database is constructed by vehicles reporting their way-point information to the NS.

A local agent generates the policy tree by inspecting its traffic data base. Each vehicle gets the dynamic attributes over a given time span by interacting with the local agent that knows the vehicle trajectory (from navigator) and the traffic database.

WIF without Support by RSI — To handle RSI failures due to disaster, blackout, and unpredictable damages to RSI devices, a distributed way-point information system model is required in order to improve the failure resiliency of the SAT model. We devise a backup system using Way-point Geographic Hash tables (WGHT) to store and retrieve the way-point information. Our solution is inspired by the Grid's Location Services (GLS) implementation described in [11]. In WGHT, a distributed hash table (DHT) is established upon the vehicles. Basically, each vehicle is considered as a server. The search across various servers of the WGHT overlay is accomplished using geographic routing, which is made possible by relying on GPS support. In SAT, we introduce a novel concept of *virtual peer*. The virtual peer is one of the vehicles in an area that is associated with a local policy agent. The virtual peers in the WGHT store the way-point information for vehicles. Many of these areas and virtual peers create an overlay in multi-hop vehicular networks. Thus a group of vehicles will serve as a redundant distributed storage server to store the way-point information. A distributed information handoff scheme is needed to make sure the way-point information is kept (and can be found) within the same geographic area while vehicles move out and move in.

SAT Performance Gain — The latency to establish trust among vehicles is the most important performance issue. SAT addresses this requirement by implementing a pre-trust-establishment phase before two vehicles need to communicate. In general, the latency in SAT is mainly from two sources:

- Preparing policy trees that satisfy the originator's security requirements
- Performing ABE algorithms to generate cipher-text

The predictability of SAT through WIF allows the reduction of latency by allowing each vehicle to pre-fetch its dynamic attributes and hence pre-compute the policy trees and ciphertext (recall static attributes are always available to vehicles). The performance gain using this approach can be analyzed considering the following cases:

- When accurate dynamic attribute predictions are possible, the policy tree can be pre-computed to bypass the traditional handshaking during the V2V communication. Broadcasting messages can be within tens of milliseconds with only message encryption latency due to the ABE computation.
- When only partial dynamic attributes predictions are available, the system can still benefit greatly from partial policy tree computations. When the predictions become more accurate, vehicles can add their computation readily.
- Most of vehicles in a given zone will either have complete predictions or partial results.

This locality feature can add to the overall performance gain and improve the scalability.

The predictability of SAT through WIF allows the reduction of latency by allowing each vehicle to pre-fetch its dynamic attributes and hence pre-compute the policy trees and ciphertext (recall static attributes are always available to vehicles).

Introducing Social Network Trust in VANETs

SAT incorporates E-Mail-based Trust (EMT) to complement cryptography-based solutions. In general, social network trust can be applied in the following two scenarios: the use of shared keys or public key certificates is not available, and data trust cannot be easily evaluated through traditional methods, such as using majority rule, watch dog solutions, etc. We must note that SAT utilizes social network trust to bootstrap the inter-vehicle trust. SAT is not restricted by scope of EMT. Here, we use EMT as an illustrative example. SAT is based on the social network trust established among email contacts through their email-based activities. Particularly, in SAT, we address the following three email-based social network trust functions:

- Measuring trust between an email user and his/her contacts;
- Protecting email users' privacy during the social network trust establishment procedure; and
- Interfacing email-based social network trust into VANETs related security functions.

To address the first function, each user will run an email trust checking agent (TCA) software. It performs the following two main operations: sending trust checking requests and performing trust checking and ranking. After two users exchange their email addresses, the TCA will perform trust checking based on each other's email addresses through a trusted EMT server. Current trust model using EMT services is similar to the existing on-line web services, such as Amazon, in which each user needs to tell his/her private information to service providers. Thus, to use EMT services, a user needs to register in an EMT server (a prototype is developed in [5]). The EMT server performs statistic analysis of the email *inbox* to ascertain its trust level based on statistical analysis on several email exchanging activities, e.g., email exchange frequency, inbound ratio, outbound ratio, etc. In general, more frequent, recent, and balanced email exchanges represent higher trust level.

To address the second function, as shown in Fig. 4, we present email domains based on their usage scopes, i.e., personal emails, business emails, and public emails that can be used as anonymized email IDs. Each block represents a trust domain with respect to the user's email addresses with trust-ranked contacts. For examples, the trust levels in a private trust domain can be classified as: *highly trusted*, *trusted*, and *un-trusted*. For the working domain, similar trust structure or more scrutinized hierarchical trust models can be defined. For the public domain, we consider the EMT server as a trusted party and it cannot be compromised or expose users' private information. During the registration procedure, a user needs to provide a mapping between his public email address (serves as a pseudonym) and email addresses in the private or working domains. Moreover, the EMT service will access email servers in each domain to retrieve statistical email data of corresponding registered email accounts.

For the third function, obtaining email-based trust is initiated by a TCA residing in the vehicle's onboard unit or a passenger's cell phone. Each TCA broadcasts the user's public email ID periodically to look for trusted peers. Upon receiving an email ID, the receiving TCA runs a trust search protocol through the EMT server to evaluate the trust level of the received email ID. Based on the email trust social graph built at the EMT server, the trust evaluation results are returned to the vehicle or the user's device. Cryptography and secure policies can be integrated by considering the email ID as an attribute. This requires the corresponding private key component be pre-installed through the global trust agent. In this way, the data encrypting key can be finally calculated using the proposed policy tree scheme.

Deployment and Implementation Considerations

SAT is composed by several interrelated key components including policy enforced data access control mechanism, proactive and predictive way-point information collection and distri-

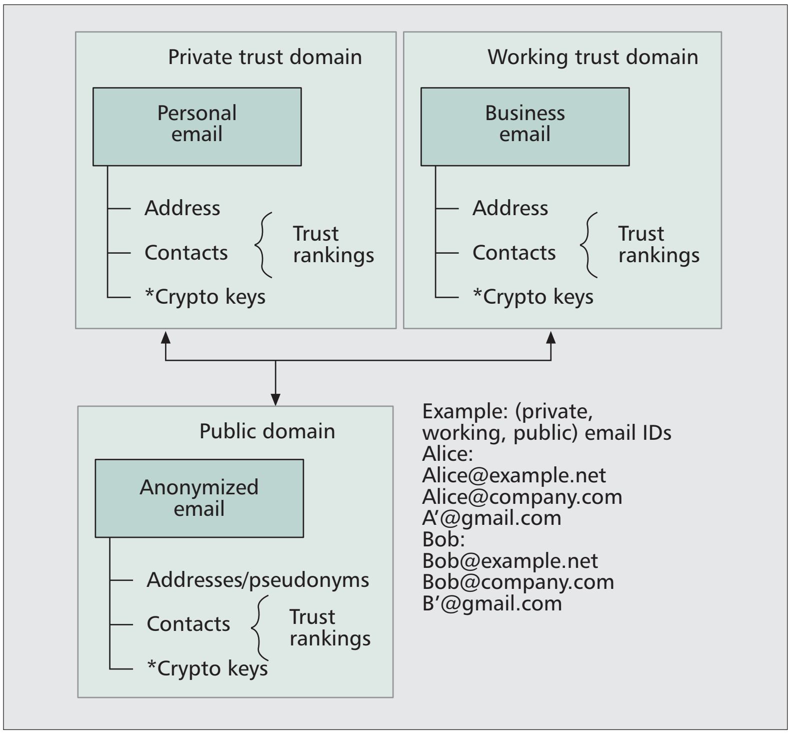

Figure 4. *EMT architecture.*

bution framework, and social network trust model. The proposed new trust infrastructure is driven by new development of technologies. Many wireless technologies are ready for VANETs. For example, Dedicated Short-Range Communications (DSRC) and IEEE 802.11p are ready to support short range and low latency communication; 3G and WiMax can support reliable and fast data delivery; the functionalities of digital navigation systems become more accurate and widely used. In [12], a novel mobile cloud framework is presented to utilize cloud computing techniques to promote the development of various mobile services for mobile users. Particularly, the trust management services, e.g., certificate services, social network trust services, credential management services, dynamic/static attributes, and corresponding private key management services, proactive and predictive trust management services, way-point information collection and distribution services, and way-point information database services, can be handled by emerging cloud computing technologies.

Apart from emerging VANET and cloud technologies, the applications based on inter-vehicle communication have proliferated recently, ranging from critical safety driving to commercial services, such as location-based advertising, content delivery, urban sensing, and storage. Various vehicle social networks have been implemented, e.g., RoadSpeak [13]. However, the major obstacle that prevents social network technologies from being adopted for VANETs is a lack of efficient and user-friendly interfaces to VANET applications. A tremendous software development effort is required to bridge the gap between theory and applications of social networks to real VANET applications. Moreover, social network trust usually exhibits a certain preference based on the nature of the analyzed social domain. When the derived social network trust is applied to another application domain, the social network trust may not fit well into the new application domain. Thus, it is critical to analyze the similarity between the social network trust and a given application domain to minimize the divergence of applying the social network trust.

The proposed SAT architecture resides on various network devices, including vehicles, roadside units and servers sitting inside the wired infrastructures. At system level, the Security Policy Management (SPM) and Vehicle Trust Processing (VTP) are two required components. The SPM component consists of a global trusted agent and local trusted agents to distribute cryptographic keys, and to manage static and dynamic security policies. The global and local agents connect to vehicles through the way-point information framework. The VTP component runs on each vehicle. It handles sensing, event perception, analysis and SAT related network protocols. It supports the interactions among the global and local agents, and runs the SAT prediction protocols. Its networking services include cryptographic operations and communication protocols. As the two components interact, the security policy is determined and access permits can be verified.

With the development of vehicular technologies, installing cryptographic keys in vehicles can be practically possible in near future. But the major issue for implementing and deploying the SAT techniques is the availability of trust infrastructure required to host the proposed local trust agents and global trusted agents. Some cryptographic credentials can be established offline with long lived validity; others, more dynamic credentials are obtained as the car joins the VANET and travels through the urban grid. On the other hand, the PKI based secure vehicle communication techniques for securing vehicular communication [1, 2] can be used underlying the primitives for SAT.

Conclusions

Vehicular Situation-Aware Trust (SAT) architecture targets to build a fundamental trust platform to handle various road situations. To this end, we present a policy enforcement system utilizing identity and attributed-based cryptography to achieve group-based data access control. We also presented away point information collection and dissemination framework to address the communication and computation latency issues due to the highly dynamic nature of VANETs. Lastly, we present how to incorporate social network trust model for vehicular systems, which can greatly improve the incentive of users to adopt new vehicular technologies and applications. In the future, great efforts are needed on both the in-vehicular system and RSI to enable SAT. These efforts include deploying global and local trust agents using cloud computing techniques, tackling the privacy issues of using social network trust, and conducting field test.

REFERENCES

[1] P. Papadimitratos *et al.*, "Secure Vehicular Communication Systems: Design and Architecture," *IEEE Commun. Mag.*, vol. 46, no. 11, 2008, pp. 100–9.

[2] F. Kargl *et al.*, "Secure Vehicular Communication Systems: Implementation, Performance, and Research Challenges," *IEEE Commun. Mag.*, vol. 46, no. 11, 2008, pp. 110–18.

[3] X. Hong *et al.*, "Sat: Building New Trust Architecture for Vehicular Networks," *Proc. 3rd ACM MobiArch*, 2008, pp. 31–36.

[4] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy Attribute-Based Encryption," *Proc. IEEE Symp. Security & Privacy*, 2007, pp. 321–34.

[5] D. Huang *et al.*, "Establishing Email-Based Social Network Trust for Vehicular Networks," *Proc. IEEE CCNC*, 2010, pp. 1–5.

[6] D. Huang, W.-T. Tsai, and Y-hsin Tseng, "Policy Management for Secure Data Access Control in Vehicular Networks," J. *Net. Sys. Management*, 2010.

[7] N. Chen *et al.*, "Secure, Selective Group Broadcast in Vehicular Networks using Dynamic Attribute Based Encryption," *Proc. 9th IFIP Annual Mediterranean Ad Hoc Net. Wksp.*, 2010.

[8] A. Shamir, "How to Share a Secret," *Commun. ACM*, vol. 22, no. 11, 1979, pp. 612–13.

[9] D. Boneh and M. Franklin, "Identity-Based Encryption from the Weil Pairing," *Proc. 21st Annual Int'l. Cryptology Conf. Advances Cryptology*, 2001, pp. 213–29.

[10] Y. Qin, D. Huang, and V. Nagarajan, "Towards Delay Tolerant Attribute Based Group Communications in VANETs," ASU Tech. Rep., 2010; http://dj.eas.asu.edu/snac/document/WIF.pdf.

[11] J. Li *et al.*, "A Scalable Location Service for Geographic Ad Hoc Routing," *Proc. 6th ACM MobiCom*, 2000, pp. 120–30.

[12] D. Huang *et al.*, "Mobicloud: Building Secure Mobile Cloud Framework for Mobile Computing and Communication," *Proc. 5th IEEE Int'l. Symp. Service-Oriented Sys. Eng.*, 2010.

[13] S. Smaldone *et al.*, "Roadspeak: Enabling Voice Chat on Roadways using Vehicular Social Networks," *Proc. 1st IEEE Int'l. Wksp. Social Net. Sys.*, 2008, pp. 43–48.

BIOGRAPHIES

DIJIANG HUANG [M] (dijiang@asu.edu) received his B.S. degree from Beijing University of Posts & Telecommunications, China 1995. He received his M.S., and Ph.D. degrees from the University of Missouri-Kansas City, in 2001 and 2004, respectively. He is an Assistant Professor in the School of Computing Informatics and Decision Systems Engineering (SCIDSE) at the Arizona State University. His current research interests are computer networking, security, and privacy. He is a recipient of Office of Naval Research (ONR) Young Investigator Award 2010.

XIAOYAN HONG [M] (hxy@cs.ua.edu) is an associate professor in the Department of Computer Science at the University of Alabama. She received her Ph.D. degree in Computer Science from the University of California, Los Angeles in 2003. Her research interests include mobile and wireless networks, challenged networks and future Internet. Her current research focuses on mobility, routing, bio-inspired communications, and wireless network trust and privacy.

MARIO GERLA [F'02] (gerla@cs.ucla.edu) is a Professor in the Computer Science at UCLA. He holds an Engineering degree from Politecnico di Milano, Italy and a Ph.D. degree from UCLA. At UCLA, he was part of the team that developed the early ARPANET protocols under the guidance of Prof. Leonard Kleinrock. He joined the UCLA Faculty in 1976. At UCLA he has designed and implemented network protocols including ad hoc wireless clustering, multicast (ODMRP and CODECast), and Internet transport (TCP Westwood). He has lead the $12M, 6 year ONR MINUTEMAN project, designing the next generation scalable airborne Internet for tactical and homeland defense scenarios. He is now leading two advanced wireless network projects under ARMY and IBM funding. His team is developing a Vehicular Testbed for safe navigation, urban sensing, and intelligent transport. A parallel research activity explores personal communications for cooperative, networked medical monitoring (see www.cs.ucla.edu/NRL for recent publications).

In the future, great efforts are needed on both the in-vehicular system and RSI to enable SAT. These efforts include deploying global and local trust agents using cloud computing techniques, tackling the privacy issues of using social network trust, and conducting field test.