Challenges and Opportunities for Securing Intelligent Transportation System

Meiyuan Zhao, Jesse Walker, and Chieh-Chih Wang

***Abstract*—There has been considerable work addressing security in vehicular network systems for intelligent transportation system (ITS) usages. We examine the proposed security framework and solutions in this space. Our analysis leads to several key observations. The current security work misses many practical ITS usage and security requirements, since it fails to consider practical economic models and critical ITS functional requirements as a control system. Consequently, the standardized ITS communication message authenticity solutions have little utility relative to addressing the real threats. Furthermore, we analyzed the missing requirements for public key infrastructure support for secure vehicular communication. Based on our analysis, we call for future research directions in analyzing practical problems and designing solutions to secure vehicular communication in order to achieve its full potential.**

***Index Terms*—Control systems, message authentication, vehicle safety, wireless networks.**

I. Introduction

THE INTELLIGENT transportation system (ITS) targets utilization of ubiquitous sensing and wireless networking capabilities for intelligent management of the transportation system. There is considerable existing work addressing security for vehicular network systems. Despite the inclusion of these works in many globally harmonized standardization efforts, we believe the resulting systems lack utility, because the real security issues in practical usages are not addressed. Much of the existing work transports IT security models into the vehicular system. This translation is appropriate for only some functions, as security is not a static universal property, but rather depends just as much on functional, economic, political, and social characteristics of the system being secured as technical considerations.

In order to identify realistic security requirements for vehicular networks, this paper examines a number of intended usages of the ITS functionality, analyzes effectiveness of designed security framework and protocols, and makes recommendations for building viable security mechanisms. We made three major contributions as summarized below.

- Conduct detailed analysis on the existing message authenticity mechanisms and demonstrate the failure to address real world ITS security issues in practical usages.
- Examine missing requirements for public key infrastructure support in securing ITS communication.
- Call for a focus on real world ITS usages, their unique requirements, and designing solutions to meet these requirements and to adapt to continuous changes and evolution of ITS.

In the rest of this paper, Section II introduces the ITS and current security solutions. Section III revisits the intended usages of ITS. Section IV examines the authenticity requirements and analyzes the utility of proposed security mechanisms for intended ITS safety usage. Section V analyzes PKI architectural issues. Section VI presents discussion on further ITS security challenges. Section VII concludes this study and calls for actions.

II. Intelligent Transportation System Security

The intelligent transportation system (ITS) promises systematic solutions to enable intelligent decision making for improved transportation safety and traffic efficiency. Similar to other control systems, the ITS must function correctly to limit damage or loss of life or property even under system failure modes, such as attack or communications failure. This section briefly introduces the ITS system model, and discusses existing academic and industry work pertaining to threat analysis and security solutions.

A. ITS and Communication Model

The core components of an intelligent transportation system are ubiquitous road environmental sensing and a vehicular communication system. The sensing information, such as road conditions, driving status, and traffic information, is processed and shared by vehicles and roadside infrastructure units (RSUs). The communications medium among vehicles is based on RF technologies specifically designed for vehicular communication. Below is a common system model of ITS communication, in the existing ITS standardized specifications, including ETSI TC ITS [9] and IEEE 1609 DSRC/WAVE [17].

In the vehicular communication system, the network nodes—vehicles and RSUs—send broadcast beacon messages to share transportation sensing information. The beacons may be sent periodically or on-demand, transmitted in one or multiple hops. Typically, the vehicle sends one beacon message every 100–1000 ms. Such communication is commonly referred to as vehicle-to-vehicle (V2V) or vehicle-to-infrastructure (V2I). For information to be shared among dedicated

Manuscript received November 02, 2012; revised December 31, 2012; accepted January 04, 2013. Date of publication February 25, 2013; date of current version March 07, 2013. This paper was recommended by Guest Editor F. Koushanfar.

M. Zhao is with Intel Labs, Santa Clara, CA 95054 USA (e-mail: meiyuan.zhao@intel.com).

J. Walker is with Intel Labs, Hillsboro, OR 97124 USA (e-mail: jesse.walker@intel.com).

C.-C. Wang is with the Department of Computer Science and Information Engineering, National Taiwan University, Taipei 10617, Taiwan (e-mail: bobwang@ntu.edu.tw).

Digital Object Identifier 10.1109/JETCAS.2013.2243633

entities, the messages could also be sent via Geocast [24], multicast, or unicast. The RSUs are connected to the infrastructure via dedicated communication channel.

The vehicles use beacons to share information about themselves, such as location, speed, and direction, and road condition events. The example road condition events could be accident location, change lane/merge traffic warning, brake light warning, emergency vehicle warning, etc. RSUs send broadcast warning messages mainly about road condition and environmental hazards. Sometimes, services provided to the vehicle, such as vehicle maintenance reminder or e-Toll, may require a session to be established between the vehicle and a RSU using unicast messages.

B. Existing ITS Security Works

Incorporating a comprehensive security architecture into ITS is perceived as critical for its practical deployment. The proposed mechanisms focus primarily on security and privacy protection for the vehicular communication protocols.

There are a few efforts analyzing the risk of the vehicular communication systems. Koushanfar *et al.* [22] surveyed the issues around emergent cyber cars and highlighted the important security challenges insider the vehicles as well as in various vehicle communication channels. Papadimitratos *et al.* [27] conducted an analysis to identify threats, and further a set of critical security requirements applicable to ITS communication protocols. The authors define a set of principles guiding the design of secure vehicular communication. However, the general guidelines are not specifically dedicated to usages. ETSI TC ITS conducted its own threat analysis [8]. This study identifies similar set of threats and security requirements. The authors dedicate their effort, however, on mapping appropriate security requirements to specific usage cases. In both studies, message authenticity and integrity stands out as critical requirements for almost all usages. We will argue later that the requirement for real-time public-key based authentication is not feasible in some practical usage cases.

A number of works proposed security mechanisms on vehicular communication, primarily focusing on message authentication [9], [10], [12], [17], [23], [31]. The commonly-used approach to providing broadcast authenticity is to apply the sender's public key signature to messages it generates. This approach is adopted by ITS standardization efforts, including ETSI [9] and IEEE 1609.2 [17]. In the vehicles there could dedicated hardware to support needed cryptographic and security capability. For instance, EVITA project [10] suggested integrate several hardware security modules (HSM) as security co-processors in the vehicle internal architecture to support security functions, including securing vehicular communication. To support effective secure storage and key generation for vehicles, some hardware features, such as a PUFs framework [1], could be utilized to enable secure key generation, component identification, and security storage.

To support digital signature mechanisms, most approaches assume a public key infrastructure (PKI). In such a model, there exist a set of certification authorities (CAs) in the ITS backend. The CAs are responsible for registering entities in the ITS, and issuing and managing security credentials for ITS network nodes. Hierarchical ITS PKI structures are proposed, with a root CA and a set of subordinate CAs. A valid certification path from the end entity to the root CA establishes its identity validity. The sender's certificate should be verified first via its certification path before verifying signature on its message. The prior work on security infrastructure support for ITS focused on two aspects: efficient certificate validation or revocation, and enabling privacy protection. Recognizing the extra communication and processing overhead by the certification validation, several proposed approaches attempt to remove the requirement that the sender's certificate has to be attached with each signed message, as long as the relying parties have ways to retrieve and validate the certificate status [18], [30]. Furthermore, the certificate revocation status should be distributed to relying parties to enable effective certificate status validation [13], [19], [33]. We will argue later that current ITS PKI has fundamental architectural issues that prevent it from supporting practical ITS usages.

There is also a large body of work on vehicular communication privacy, worrying that ITS messages could reveal private information about the vehicle and driver [1], [14], [17], [33]. Many works, proposed to use pseudonyms as "implicit certificate" in the beacons. Such an approach saves communication bandwidth and attempts to hide sender's identity [1]. However, the recipient still needs to verify the sender's authenticity in order to verify its messages. Other works attempt to address this using various key assignment techniques [33]. Note that nonrepudiation/authenticity and anonymity are contradictory goals. We believe a viable privacy preserving solution should attempt to satisfy only appropriate usages, in which non-repudiation is not the intended essential security requirement.

III. ITS Communication Usages

Existing ITS risk analysis works have outlined *authenticity* and *anonymity* as primary security requirements. It is important to note that security requirements are driven by target usages. As we noted above, the anonymity required for some usages is at odds with nonrepudiation required for other purpose. Different usages require different kinds of signatures (e.g., anonymous versus nonrepudiable). In this section, we revisit the intended ITS usages and applications. Understanding intended usages helps us derive corresponding security requirements specific to these usages.

Collision avoidance has been the primary motivation for ITS design. CAMP-VSC2 Consortium launched studies specifically for this purpose [3]. A much broader scope of applications were identified by ETSI TC ITS [6]. The definition is summarized in Table I. The basic applications are categorized in four classes: active road safety, cooperative traffic efficiency, cooperative local service, and global Internet services. The active road safety and cooperative traffic efficiency goals mainly rely on frequent V2V and V2I broadcast communications. The latter two classes are enabled mostly by unicast vehicular communication.

Existing threat analysis studies [8] derive security requirements primarily based on the form of communication. For instance, the usages relying on V2V safety broadcast beacons are considered together. Similarly, periodic beaconing of environmental condition is used to group another set of usages. As the

TABLE I
BASIC SET OF ITS APPLICATIONS

Class	Application	Example Use Cases
Active road safety (Driving Assistance)	Cooperative awareness	Emergency vehicle warning; Slow vehicle indication; Intersection collision warning; Motorcycle approaching indication
	Road hazard warning	Emergency electronic brake lights; Stationary vehicle warning; Signal violation warning; Collision risk warning; Warning: hazardous location, precipitation, road adhesion, visibility
Cooperative traffic efficiency	Speed management	Regulatory / contextual speed limits notification; Traffic light optimal speed
	Cooperative navigation	Traffic information and recommended itinerary; Enhanced route navigation; Limited access and detour notification;
Cooperative local services	Location based services	Point of Interest notification; Automatic access control and parking management; ITS local electronic commerce
Global internet services	Community services	Insurance and financial services; Fleet management; Loading zone management
	ITS entity life cycle management	Vehicle SW / data provisioning and update; Vehicle and RSU data calibration

result, the target of the analysis only focuses on ITS messages. We argue, however, that the control system nature should instead be the primary concern, i.e., the security requirements should be derived from the intended usage, not from the implementation approach.

Due to the limited scope of existing risk analysis works, the resulting mitigation proposals only focus on ensuring protection of ITS messages to satisfy the defined security requirements. This means only the entities involved in transmitting and processing ITS messages are considered in the solution. These entities are primarily vehicles, RSUs, and backend ITS authority/server. Consequently, despite original motivation to address a wide range of usages, the currently defined security mechanisms solve problems mostly related to active safety class of usages.

In order to identify suitable security solution for intended real world usages, we next examine the authenticity requirement and their utility more closely. We further conduct in-depth analysis on PKI support in the current security framework and identify several critical missing requirements.

IV. REVISITING MESSAGE AUTHENTICITY

The global ITS standardization effort has widely assumed that the V2X message authenticity is one of the essential security requirements [3], [9], [17]. Given the broadcast nature of ITS messages, the proposed solutions follow a similar system model: each vehicle or RSU digitally signs messages it generates before transmission. A receiver of the messages then verifies the digital signature and validity of the signing key to establish authenticity and integrity of the received messages.

We argue that the mechanism of real-time message verification has little utility for enhancing the security of a vehicular communication system when receiver of these messages is expected to take real-time actions for safety or traffic efficiency. On the other hand, we argue that message authenticity and nonrepudiation, are in fact essential for nonreal time usages, such as producing evidence for legal dispute resolution.

A. Adversarial Model

The *Dolev-Yao (DY)* adversarial model [5] or one of its children is the most common approach to analyzing the security of communications protocols. A DY adversary can obtain any message transmitted across the network, delete any such message that traverse the network, initiate a "conversation" with any network participant, and insert messages of his choice into any message flow. In the wireless networking threat analysis, the DY model is appropriate given the open nature of the wireless communication. A real life adversary could launch any of the following actions on vehicular communication messages.

Message Deletion: Remove messages from the wireless communication medium before delivery, e.g., through jamming.

Message Modification: Intercept messages from the communication channel, modify their content, and then transmit the modified message back into the channel.

Message Forgery: Create messages of choice and inject them into the channel. Message modification is a special case of forgery.

Message Replay: Record messages on the channel, and then retransmit them at a later time. The replay may occur in a different channel than the one that carried the original.

These are basic attacks against a communications channel. Other attacks exist that utilize these basic actions: message delay, rushing, reordering, etc. More complex attack actions could also be conducted by collusion among attackers. We choose to analyze only these four threats, as these are more basic threats to be mitigated. We will show later, proposed ITS message authenticity mechanisms fail to address important issues raised by these threats.

B. Risk Analysis

To analyze the risks, we focus on control system consequences. Control systems possess different requirements than traditional IT networking systems. In a control system, like the vehicular communication system, the primary concern shifts from integrity, availability, and confidentiality to the preservation of *human lives*, *property*, and *safety*. As discussed above, most of the ITS usages focus on driving safety with the goal of reducing collisions. We recognize this goal and analyze the consequences of attacks with collision avoidance in mind. In particular, we attempt to understand whether the threats to ITS messages lead to worse results compared with the situation where no ITS service is available for the vehicles. For instance, if the goal is to reduce collisions, we examine if an attack on ITS messages could lead to more collisions compared with the case where there is no vehicular communication enabled or deployed.

We choose the leading active safety awareness applications as the usage case for our analysis. Mostly V2V messages from this category are broadcast to share critical real-time status. Status information is sent in message as "event," together with vehicle's location, speed, and direction information. The vehicle receiving such message is expected to either take immediate action by itself, or send nonsuppressible and intrusive warning to the driver. The detailed specification of message format can be found in [9]. Detailed definition and discussion on the human factors for these cases are in [7]. Readers interested in detailed risk and mitigation analysis on other usages are referred to [35].

Furthermore, we divide the concern to analyze consequences for *precollision* versus *postcollision* situations. Specifically, "precollision" refers to the situation where the ITS messages are sent and processed to potentially avoid collision, expecting real-time actions taken by vehicle or driver as the perceived danger dictates. For "postcollision" situation, the focus is on collecting evidence to document what happened. ITS messages are part of the evidence. Therefore the threats to message authenticity and integrity are the focus of the analysis.

In addition to the consequences of the attacks, we also discuss the effectiveness of proposed mitigation mechanism, namely, digitally signing and verifying ITS messages in real-time.

1) Risks in Precollision Situation:

Threat #1: Message Deletion: A message deletion is indistinguishable from the case where legacy vehicles do not implement the ITS vehicular communication at all, or a message is destroyed through normal operation of the channel, e.g., interference due to the hidden node problem. The vehicle system won't take action in such situations.

Threat #2: Message Modification: All fields in a broadcast message are subject to message modification attack. Modified contents may lead to two possible outcomes.

Case 1: The modified message could suggest the danger level is below the threshold of any collision avoidance algorithm. The attacker could change the location, speed, direction, or timestamp value in the message to make the content irrelevant to the message recipient. Or the attacker could also remove the warning event(s) from the message. Nonetheless, this kind of modification leads to the similar effect as deleting the message.

Case 2: The modified message falsely suggests a high danger level that could lead to unnecessary collision avoidance action. For instance, the false location/speed/direction information could lead the victim vehicle or its driver to brake suddenly. As suggested in [7], if the vehicle is convinced the collision danger is high, it could take immediate action and the driver may not overrule the action. In this case, the attack can successfully cause unnecessary actions, which may increase the chance of collision.

Threat #3: Message Forgery: The attacker may forge warning and send to vehicles via broadcast. Consequences are identical to Threat #2.

Threat #4: Message Replay: If it is not treated as collision warning by a recipient vehicle, a replayed message only consumes communication channel bandwidth. If the wireless channel is consumed by sufficient number of "normal" replays, real "live" warnings could be blocked due to congestion, one of the stock attacks to cause message deletion.

If replayed message is treated as valid warning by the recipient vehicle, the consequence is identical to forging warning messages as in threat #2 and #3.

2) Mitigation Analysis in Precollision Situation: Digital signatures are effective for detecting message forgery and modification. Hence, if forgery and modification of warnings were the only threats, digital signatures might be an effective mitigation. However, this approach is problematic for several reasons.

First and foremost, being a control system, the ITS must minimize the loss or damage to life and property, even without any message input. The transportation infrastructure will likely always support legacy vehicles that lack the latest ITS communication. Messages will always be lost or damaged in transit, as no radio medium can offer an ideal, completely reliable communication medium. For the same reason, a vehicle must necessarily ignore messages at variance with its own measurements of the driving environment. This suggests that real-time forgery detection is not the sole security requirement governing the communication function.

There are other reasons to reject real-time signature verification. Performance overhead of public key signature operations is computationally expensive. There are two aspects to this performance overhead: space and operation latency.

To further understand the space overhead, let us examine the cryptographic contents in a signed message, which include the following:

a) the signature itself;
b) the verification key;
c) the signer's identity bound to the signing key;
d) a second signature over the signing key and identity by a certifier, attributing the signing key to the correct party;
e) the signing key of the certifier;
f) the identity of the certifier.

A signing key and signature based on, say, EC-DSA over a 224-bit elliptic curve requires at least 56 bytes to encode, an approach taken in the IEEE 1609.2 standard [17]. Suppose the identities are expressed using an 8-byte abbreviated form, the example cryptographic contents above can require at least 240 bytes of precious message payload just for two public keys, two public key signatures, and two identities. This per-beacon overhead is significant. To see this, at 10 Hz each vehicle will generate 10 warning messages per second. As we have seen, each signed warning message will include at least 240 bytes for signatures, keys, and identities, which translates to at least 1920 bits of bandwidth for each message. Since each vehicle generates 10 warning messages per second, the radio channel must dedicate at least 19 Kb/s bandwidth per vehicle to convey the integrity information alone. The ITS will be most useful in urban settings, where there is a high density of vehicles. In such a scenario, we might expect hundreds of vehicles to be within radio range of one another in many cases. It is dubious that many of the proposed broadcast channels deliver sufficient bandwidth to support the data load imposed just by the signature scheme. Analyses conducted for U.S. National Highway Traffic Safety Administration (NHTSA) [3] confirm the same concern.

A second problem is a single public key signature or verification requires literally millions of instructions. Each vehicle could in principle receive literally hundreds or thousands of broadcast messages from other vehicles and the infrastructure each second. Verifying authenticity of each message requires verifying at least two signatures from each message: the signature of the sender, and the certifier's signature. It has been estimated [18] the architecture can require a vehicle to process up to 8800 signatures per second, with 20 Hz beacon message frequency. Hence, this approach imposes a signature verification processing load on each vehicle comparable with or even exceeding that of entire e-commerce data centers, where 2000 signatures/second is a heavy load [29]. Because of this, the IEEE 1609.2 standard suggests using the verification-on-demand (VoD) [23] approach to reduce the number of required signature verifications. Adopting VoD scheme, the receiver of the message determines the threat level as the result of processing the message. It only verifies the message authenticity if the threat level is higher than a defined threshold value. Kargl *et al.* [19] suggested similar approach to selectively verify signatures based on message context.

The VoD method suggests a potential viable path to support secure vehicular communication. That is, ITS message authenticity is taken into account with a larger context, where there are other sources of information could be more important to help determine the safety urgency. To extend this further, a few studies took a different route to evaluate event validity in vehicular communication via multiple sources of information [16], [20]. In these schemes, a valid signature on the message is no longer the sole source of information. In addition, other entities' observation and reports, as well as the vehicle's local sensing information can all be utilized. Such validation may be viewed as "*plausibility test*," where messages with plausible event/warning deserve further validation. If the warning is far from the consensus situation derived from the vehicle's local sensing view, it could be determined as not plausible, hence should be ignored. This seems to be a viable direction to follow and should attract more research attention for validation algorithm design and evaluation.

Finally, the use of broadcast makes timestamping the most obvious candidate to defend against replays, but timestamping requires global synchronization to a common secure clock.

Given the extra overhead for real-time signature verification, the question here is whether the vehicle can afford the extra delay given that it has to take action immediately to avoid collision. As we have already noted, a vehicle must determine the action it takes anyway, independent of any warning messages received. Signature-based broadcast message authenticity to defend against forged warning in real time appears to have limited utility in collision avoidance.

3) Postcollision Situation Analysis: Computational overhead and network bandwidth is not an issue postcollision, because time and bandwidth exists to collect any available evidence. After a collision or a traffic incident occurs, a question of liability arises. There are at least two interesting scenarios relevant to ITS messages.

If a critical warning message was maliciously deleted and the collision occurred, the omission of such warning from a trustworthy log, where ITS messages are stored, can be deduced as part of evidence gathering during a postaccident investigation. However, as unreliable as the wireless channel is, a party suspected liable cannot argue the omission of such warning messages as a defense. Again, being a control system, we expect the vehicle to operate properly even without any external information at all.

On the other hand, the "false warning" messages could lead to unnecessary collisions since the victim vehicle or driver took actions based on false information. In this case, evidence showing the transmitted or received information is faulty could be important. We are not qualified to reason about all the legal consequences. However, if vehicular communication messages are to be used as evidence, message signing is paramount. In this case, digital signatures are useful only if they provide nonrepudiation and nonanonymity.

It is also worth noting that legal dispute resolution after an incident may need multiple signatures. An accident might be due to infrastructure failure (the Department of Transportation is at fault), improper vehicular maintenance (the owner is at fault), vehicular failure (the manufacturer is at fault), driver error (the operator is at fault), an impaired driver (either the owner or the operator might be at fault, although some impairments like stroke or heart attack are no one's fault), etc. In any event, the notion of a single signature seems to be simplistic to address the real need. Instead, design work is needed to support the recovery of all pertinent evidence when needed. Due to the overhead of public signature schemes, however, it seems more realistic to suppose communication messages generated by a vehicle have a single, nonrepudiable signature, and signatures on other supporting evidence are captured in data logs that provide trustworthiness.

C. Discussion

Going beyond the concern of message authenticity and integrity, some usages may have more concerns on information *availability* instead. Noted from Table I, several usages in traffic efficiency category expect vehicles to periodically exchange driving status information, such as location, speed, and direction information. Kloiber *et al.* [21] conducted a simulation study to evaluate one such application, cooperative cruise control, with respect to the beaconing frequency. They discovered that the application relies heavily on message availability. Based on their experiments, certain beaconing frequency, e.g., 8–10 Hz, should be reached in order for vehicles to constantly keep track of neighboring vehicles. On the other hand, beaconing frequency higher than expected optimal value can hurt function reliability, because of saturated communication channel and much higher message collision rate. Given this property, message deletion and replay may be effective attack approaches to defeat the traffic efficiency function. These two attacks are relatively easy to launch, and digital signature approach does not mitigate the risks.

It is also worth noting that nonrepudiation and anonymity are conflicting requirements. There is increased concern that vehicular communications can leak about personal identifiable information. Attempting, however, to use one protocol to satisfy conflicting requirements is fundamentally flawed. Given our analysis that real-time signature verification has little utility we could potentially satisfy the privacy requirement by encrypting the hash of sender's public key under a key that could be decrypted only through due process to uncover and collect evidence. We plan to conduct further work on this topic in the future.

V. PKI Architectural Issues

A. DSRC PKI Framework

The public key infrastructure (PKI) defined in [17] supports the security framework that enables the secure communication protocol for ITS entities, mainly vehicles and RSUs. The entities hold their certificates that bind their public keys to their ITS domain. A certification authority (CA) is responsible for issuing and managing member certificate for each member entity in the domain. The DSRC security framework suggests a hierarchical structure of the authorities where the root CA is pre-established as trusted authority by all members and defined in the form of its self-signed certificate. The root CA could further issue certificates for other CAs, each of which is responsible for their own members as could be defined by a set of policies. Overall, the validity of a member is established via a certificate chain, linking the member's public key back to the trusted root CA. All entities are required to validate the signing certificate before they can validate the signed messages by the member.

IEEE 1609.2 security framework defines certificate format for CAs and members that certifies EC-DSA public keys. The attention is paid closely to reduce the certificate size for space efficiency. In such a design, the target certificate size is under 200 bytes. In addition, pseudonyms of certificate holders are defined to address privacy concerns. The entities are not directly identified and tracked via their member certificates.

In the case of certificate revocation due to member compromise or key pair update, the CA also supports the function of creating and disseminating certificate revocation list (CRL). Each CRL contains the identifiers of the revoked certificates by the CA. The CRL is signed by the issuing CA. All relying parties must check the subject certificate against the issuer's CRL. Certificate validation fails with a revoked certificate in the subject certificate's certificate chain.

B. ITS PKI Architectural Issues

For each ITS domain, the intended usages require careful assessment of deploying practical PKI framework. There are several issues that deserve in-depth analysis.

First of all, the PKI support for ITS may potentially need to manage certificates for large numbers of entities. For instance, a hypothetic national ITS system for U.S. would require certification for all vehicles operated in the region and all possible RSUs to be deployed to enable the infrastructure. There could be hundreds of millions of entities in total. The tremendous scale of the problem leads to challenges in managing and updating the system that was never faced before in traditional IT systems.

Second, more importantly, the security infrastructure should be capable of dealing with the dynamics of the transportation systems.

The primary focus in our analysis is on missing requirements and considerations regarding three issues in the ITS PKI design: 1) support vehicles crossing regulatory boundary; 2) deal with certification authority update; 3) support control system requirements in case of ITS cyber system failures. The rest of this section discusses each of these issues in detail.

C. Crossing Regulatory Boundaries

A *regulatory domain* refers to one ITS operational domain that is managed and operated by its own root-of-trust authorities. One ITS regulatory domain mandates a set of algorithms, protocols, operations, and policies. It may be relevant to a geographic region, such as a city, a state, or even a country. Some other regulatory domains could be defined based on intended functionality. The same region could have multiple overlapping regulatory domains.

Within a regulatory domain, all registered ITS entities, including vehicles, are required to comply with all its rules, so that they can interoperate with each other. It is possible that vehicles cross regulatory boundaries of ITS domains during normal operation, e.g., between the European Union and Russia. Hence when a vehicle crosses the boundary and enter a new domain, it should comply with a new set of rules and policies as mandated in the new domain.

The current framework has several issues complicate the case of supporting multiple regulatory domains: 1) mandatory cryptographic algorithms limit algorithm agility; 2) single root of trust is dictated by design; 3) no registration procedure defined, to permit a new trust anchor and crypto parameters to be established at a crossing point between regulatory domains.

Cryptographic Algorithms: The currently DSRC/WAVE security framework mandates EC-DSA as public key signature algorithm on every participating vehicles (OBUs) and RSUs. Moreover, the framework only uses two sets of elliptic curve parameters with EC-DSA: NIST curves p-224 and p-256 [11]. The future U.S. ITS deployment is expected to adopt DSRC/WAVE security framework, hence all entities will support these algorithms by default. Unfortunately, other regulatory domains may not support these algorithms. EC-DSA with different curve parameters, or even completely different and noninteroperable algorithms could be mandated. Vehicles operated in U.S. ITS that only support mandatory algorithms by DSRC/WAVE security framework will not be able to interact with entities in a different regulatory domain mandating noninteroperable algorithms. For instance, devices in PRC are mandated to use SM2 [34] as the public key signature algorithm, which is noninteroperable with EC-DSA. In a hypothetic ITS in PRC, it is illegal to operate a vehicle that does not utilize the SM2 algorithm mandated within PRC regulatory domain. Other countries, such as Japan, also have their own supported algorithms. In the future, there may be more nations that will mandate their own cryptographic systems.

In order for vehicles operate with ITS when crossing regulatory boundaries, the following two requirements must be satisfied. They are missing in the current PKI design.

Missing Requirement R1: Vehicles must implement the cryptographic systems mandated by each regulatory domain in which the vehicle is intended to operate.

Missing Requirement R2: Consequently, the vehicles must be able to support multiple cryptographic algorithms and key pairs, each of which supports a regulatory domain in which the vehicle is intended to register and operate.

The support for multiple cryptographic systems could be established when the vehicle is manufactured. Or else, a mechanism could be invoked for the vehicle in need of updating its cryptographic capability. The vehicle could generate its own key pair internally, or get its key pairs provisioned by its manufacturer. There could be other possible methods that enable initial configuration. Explicit definition of mechanisms for extensible algorithm support must be defined for practical PKI deployment.

Root-of-Trust Authorities: In order to validate messages sent by other ITS entities, the vehicle must first establish trust on the root CA in the regulatory domain, as the trust anchor. In the current PKI design, the single root-of-trust is assumed to minimize complexity of validating member certificates. Given the expectation that vehicles will cross regulatory boundaries, the PKI design and configuration should assume that vehicles support multiple domains. Different regulatory domains will use different root signing authorities, if for no other reason than they use noninteroperable cryptographic systems. To support proper certificate validation, two requirements are missing from current framework.

Missing Requirement R3: Vehicles must be able to be securely provisioned with root certificates (as trust anchors) for each regulatory domain in which they are expected to be driven.

Missing Requirement R4: Vehicles expected to send secure V2V/V2I messages must be certified by the root CA in each regulatory domain in which they are expected to be driven.

We expect the vehicle manufacturer or the initial vehicle registration agency could provision the basic trusted root CA for the vehicle to begin the ITS operations. We expect other mechanisms that the vehicle could utilize to acquire knowledge of additional root CAs for a new domain and establish trust on them.

ITS Member Registration: The vehicle's signing key must be recognized by other vehicles, which means the vehicle must be enrolled as a member before it can sends secure ITS messages in a domain. The process for a vehicle to enroll in an ITS could be complex in the real-world practice. It is tightly coupled with regulatory processes. The current PKI framework defines the information exchanged between the enrollee and the registration authority. The specification sets the registration procedure as out of scope, leaving the details as an exercise. This is proper, since different regulatory domains are likely to use different procedures. To begin registration, however, parties should invoke procedures to acquire registration information. The validity of both the enrollee and the registration authority must be mutually verified before an active registration protocol could complete. Hence, we identify two more requirements to be satisfied as prerequisite for real-time member registration.

Missing Requirement R5: Vehicles must be able to acquire knowledge of newly encountered root registration authority for intended enrollment.

Missing Requirement R6: ITS registration authority must be able to identify enrolling vehicles in a nonrepudiable way.

There may be different ways for the enrollee to acquire knowledge on the local registration authority. For instance, the vehicle manufacturer could pre-provision the trusted root registration authorities on each vehicle at its manufacturing time. The vehicle may also identify such root CA information in real time from public announcement. Nonetheless, the PKI system should satisfy the information acquisition requirement to support flexible member registration other than static configuration.

Likewise, the registration authority should also be able to validate the enrollee's identity via its identity evidence. Such identify evidence, if accepted, should be nonrepudiable since it is the basis of trust on the enrollee. The issuing CA of the identity evidence should be trusted by the registration authority before the two parties can further proceed with the registration procedure. Typically, the root manufacturer CA of the automaker is assumed to issue manufacture certificates for its vehicles. In this case, the knowledge of root CAs by vehicle manufacturers should be made known to ITS registration authorities. Alternatively, if the enrollee chooses to present its home ITS member certificate for registration in the new domain, the registration authority is expected to trust the enrollee's home ITS root CA.

D. Updating Root Certification Authorities

Besides crossing boundaries, the second issue in the existing PKI design is the complexity of updating root CAs. It is worth calling out that the design of PKI framework should satisfy the requirement for updating root CAs.

Missing Requirement R7: Root-of-trust update should be enabled.

It is suggested [10] that the vehicle establishes its manufacturer's root certificate as the root-of-trust for system update, and updating its root certificate store. Hence hardware protection is required to securely store root manufacturer key. The countermeasure should resist at least simple hardware attacks, such as replacing the vehicle's hardware component storing its keys. Such attacks could cause the victim system's root key be maliciously replaced with any public key of attacker's choice. Hence, the attacker could completely compromise the victim's security system and any security protocol that utilizes the victim's root key as the root-of-trust.

Since the root CA key will need to be replaced, the ITS protocols need to define provisions to accommodate this. In a traditional IT system, updating a root authority requires similar actions on authorities, PCs, and users as on vehicles in an ITS, but it could lead to far more complexity and difficulties in ITS due to: 1) massive scale; 2) much longer vehicle lifetime; 3) the highly distributed and mobile nature of the ITS—not all ITS system components will receive the update simultaneously.

The scale of an ITS domain could be massive. A national ITS in U.S. could potentially have hundreds of millions of entities, each maintaining their valid certificates. A top vehicle manufacturer could sale one million new vehicles in U.S. alone each year. A manufacturer root CA could be responsible for up to one hundred million vehicles on road in U.S. When the CA updates its key pair, all of these vehicles should be updated with newly issued vehicle manufacture certificates. When the ITS root CA is updated, all vehicles configured with this root CA as one of its trust anchors must be updated as well. This process could potentially impact all hundreds of millions of entities in an ITS domain.

Furthermore, there is a critical mismatch regarding the lifetime of the vehicles versus the security lifetime provided by the system design and cryptographic algorithm strength. In PC industry, a key lifetime of 5–10 years is commensurate with platform usage. In the transportation, however, vehicles can operate for decades. The security of current mandated cryptographic systems could be long broken by then. Updating root of trust is a delicate process, especially on the entities that have longer lifetime than the security lifetime of the current cryptographic algorithms. One design choice would be to update root-of-trust only in a physically secure environment. A regular "health checkup" by the manufacturers on their vehicles with proper physical access to the vehicles would potentially provide great utility to maintain sound security status on their vehicles. For those vehicles on road having trouble getting proper update, enabling a security infrastructure that only supports certain years of lifetime (e.g., 20 years) would be something to consider. Of course, after its lifetime, the systems will have to live with the consequences.

E. Support Control System Operational Principles

Cyber/physical system interaction security is the fundamental issue for ITS security framework. Like the message authenticity protocol, the PKI framework faces the same requirement to deal with control system consequences.

MISSING REQUIREMENT R8: ITS operation policy and function should be defined with great care to handle security validation failure consequences on the vehicles and ITS as control system.

Let us pick an example for analysis. Suppose a vehicle is crossing the regulatory boundary to a new domain, in which it cannot support the cryptographic algorithm or the root authority in the new domain. What should the vehicle react to this situation? The primary goal of ITS system as a control system is to maintain reliability and integrity of its operations regardless the input to the system. Given this principle, it seems that the vehicle should continue to operate as if it does not have communication capability at all, just like a legacy vehicle control system. The other extreme could be that the regulatory domain dictates such vehicles to stop operating completely. Similarly, when the vehicle encounters noninteroperable root CAs, the system may allow the vehicle to act like a legacy vehicle without communication capability or require the vehicle to halt until the new root-of-trust is properly provisioned on the vehicle.

The root cause of these uncertainties is the undefined relationship between the cyber security framework and the transportation control system. Hence, it is paramount that the ITS security framework clearly identifies these interactions and specifies policies/guidelines to invoke proper actions for these cyber/physical security conditions.

VI. ENABLING PRACTICAL ITS SECURITY

The issue of ITS security failure arises because the community has focused on solving the wrong security problems for ITS applications. In their work, the security techniques from classical computer communication security appear to have been transformed directly into ITS space without adequate consideration of what security requirements need to be satisfied. Furthermore, ITS usages have important economic and regulatory constraints that demand the security architecture to satisfy unique requirements. We call for the emphasis on understanding practical usages and the corresponding security requirements needed to support the usages. It is much more valuable to solve the real life ITS security problems than extending techniques from traditional IT space with algorithmic and protocol design tricks.

TABLE II
EXAMPLE ANTICIPATED USAGES

1. Vehicle manufacturing	8. Vehicle joins ITS communication
2. Vehicle title registration or transfer	9. Establish and maintain records to be utilized to resolve property disputes
3. Driver licensing	10. Drive a vehicle across jurisdiction boundary
4. Authorize vehicle driver	11. Data recovery for legal dispute resolution
5. Insuring a vehicle	12. Parking in the city
6. Vehicle FW update	13. Vehicle rental service
7. Vehicle repair	14. eCall service for emergency

A. Practical Usages and Requirements

Our analysis has shown clearly that security design starts from understanding usages and requirements. Here, we further shed light by examining other realistic ITS applications, beyond safety. The vehicle and services it receives are still the center of the concern. However, we take a step back to examine how the vehicle is set up and maintained to participate in ITS communication in the first place. Table II lists a few example usages that are worthy of further consideration.

This list is not exhaustive or exclusive. It offers some interesting insights on diverse economic, social, and regulatory models behind these usages. We call out example usages 1–7 explicitly to raise the issue of complexity of enabling an ITS. There are many steps the vehicle owners and drivers need to take before the vehicle could join the ITS secure communication. The usage as simple as establishing vehicle ownership and digital certificate could require nontrivial interactions among the manufacturer, the vehicle, the new owner, the transportation agency, the insurance company, and many other parties. Appendix demonstrates this complexity via the hypothetic vehicle title transfer usage.

Furthermore, a fully functioning ITS system may require a more complex and flexible infrastructure than what has been envisaged in the current research literature and standards. The framework should support entities beyond vehicles and RSUs, such as people in different roles, various manufacturers, government agencies, different governments, and many kinds of involved business. Example usages 9–11 suggest heavy involvement by various government agencies. Example usages 12–15 further indicate that various business entities also play important roles in an ITS domain. We call the community to devote extensive efforts in identifying and examining practical ITS usages that support real-world transportation related practice.

Our analysis also calls for attention on deriving functional and security requirements based on identified practical usages before designing for solutions. In addition, it is very important that not only the requirements are clearly identified but also cyber system security requirements are considered separately with control system design principles and requirements. The intelligent transportation system is a cyber system designed to support transportation related operations. Hence, the control system requirements determine the ITS design. Further careful analysis and design should take care of appropriate cyber/physical interactions and consequences.

B. Design for Change

We have made the critical observations that ITS framework faces many unusual dynamics. Vehicles could frequently cross regulatory boundaries. The mandatory algorithm and keys for the vehicle change accordingly. The ITS operations should always deal with the situation where the infrastructure is not available in some regions or legacy vehicles that do not have communication capability are on the road with other ITS-enabled vehicles. Furthermore, the long lifetime of vehicles introduces challenges to maintain and update cryptographic systems. The cryptographic strength will evolve over time, so will the security requirements.

Hence, the design of a secure ITS architecture should allow flexibility as well as extensibility. It is desirable that the enabled primitives, functions, protocols, and services can all be evolved over time and across regions.

VII. Conclusion

With ITS vision, vehicles are projected to be fully connected using all their sensors and communication capabilities in the future. We examined the risks faced by the current ITS security architecture and studied the proposed mitigations and PKI framework. We made several key observations. First of all, much existing work fails to address practical economic models, regulatory limitations, and social preferences. Second, the proposed mechanisms that require real-time verification have little utility to address the real risks to ITS communication. Lastly, the PKI envisaged for ITS failed to satisfy a series of missing requirements for vehicles to cross regulatory boundary, for root CAs to be updated, and to interact with physical transportation and vehicular system.

We took an important first step in suggesting a path to practical ITS security. We call for actions to identify practical usages, derive realistic requirements, and to design systems with great care to deal with changes as usages, domains, requirements, and algorithm strength could evolve over time.

Appendix

The transfer of vehicle ownership might hypothetically proceed as follows, to transport the separation of duties required for real life into the ITS world.

1) A seller and buyer introduce themselves to a notary.
2) The seller presents proof-of-ownership (the title) issued by the title authority, which the buyer verifies. The notary witnesses this.
3) The seller presents a selling price, which the buyer accepts. The notary witnesses this agreement.
4) The buyer presents some sort of voucher in payment for the vehicle. The seller validates this voucher. The notary witnesses this.
5) Once the buyer and seller have verified the material presented by each other, they execute the sale. This means that both of them sign a bill-of-sale. The notary witnesses this step.
6) The notary certifies steps 1–5.
7) The title transfer step occurs now. The documents pertaining to the sale (including the notary's certification) is transferred to the vehicular title authority.
8) The vehicular title authority verifies the seller's title to the vehicle.
9) The vehicle title authority verifies the buyer's voucher.
10) The vehicle title authority verifies the seller's, buyer's, and notary's identities.
11) The vehicle title authority verifies the bill-of-sale, including the signatures.
12) The vehicle title authority verifies the notary's certification.
13) There is often a public notice-of-sale with a comment period, to let someone object to the sale. Sometimes this is replaced with a records search, looking for liens or other claims against the seller's or buyer's assets. The vehicular title authority can perform this search.
14) If there is no cause to block the title transfer, the vehicle title authority issues a title to the buyer and cancels the title of the seller.
15) The vehicle updates its owner to reflect the title.

References

[1] F. Armknecht, R. Maes, A.-R. Sadeghi, F.-X. Standaert, and C. Wachsmann, "A formalization of the security features of physical functions," in *IEEE Symp. Security Privacy*, May 2011, pp. 397–412.

[2] G. Calandriello, P. Papadimitratos, J.-P. Hubaux, and A. Lioy, "Efficient and robust pseudonymous authentication in vanet," in *Proc. 4th ACM Int. Workshop Vehicular Ad Hoc Networks (VANET'07)*, pp. 19–28.

[3] Vehicle safety communications—Applications (VSC-A) final report NHTSA Pub. DOT HS 811 492A, 2011, vol. 3, CAMP-VSC2 Consort..

[4] S. Checkoway, D. Mccoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, and T. Kohno, "Comprehensive experimental analyses of automotive attack surfaces," in *USENIX Security*, 2011.

[5] D. Dolev and A. Yao, "On the security of public key protocols," *IEEE Trans. Inf. Theory*, vol. 29, no. 2, pp. 198–208, Mar. 1983.

[6] Intelligent transport systems (ITS); Vehicular communications; Basic set of applications; definitions V1.1.1 (2009-06), Tech. Rep., ETSI TR 102 638.

[7] Human factors (HF); Intelligent transport systems (ITS); ICT in cars V1.1.1 (2010-04), ETSI TR 102 762.

[8] Intelligent transport system (ITS), security, threat, vulnerability and risk analysis (TVRA) V1.1.1 (2010–03), ETSI TR 102 893.

[9] Intelligent transport systems (ITS), security, ITS communications security architecture and security management V0.0.13 (2012-03), ETSI TS 102 940:.

[10] EVITA Consortium, "The EVITA project: E-safety vehicle intrusion protected applications," 2011 [Online]. Available: http://www.evita-project.org

[11] *Digital signature standard (DSS)*, FIPS PUB 186-3, 2009, Fed. Inf. Process. Standards Publ. NIST.

[12] M. Gerlach, A. Festag, T. Leinmuller, G. Goldacker, and C. Harsch, "Security architecture for vehicular communication," presented at the WIT, Hamburg, Germany, 2006.

[13] J. J. Haas, Y.-C. Hu, and K. P. Laberteaux, "Efficient certificate revocation list organization and distribution," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 3, pp. 594–604, Mar. 2011.

[14] J. J. Haas, Y.-C. Hu, and K. P. Laberteaux, "The impact of key assignment on VANET privacy," 2009, Security and communication networks, (DOI) 10.1002/sec.143.

[15] R. Housley, W. Polk, W. Ford, and D. Solo, "Internet X.509 public key infrastructure certificate and certificate revocation list (CRL) profile," 2002, IETF RFC 3280.

[16] H.-C. Hsiao, A. Studer, R. Dubey, E. Shi, and A. Perrig, "Efficient and secure threshold-based event validation for VANETs," in *ACM Conf. Wireless Netw. Security*, Hamburg, Germany, Jun. 15–17, 2011, pp. 163 –174.

[17] *IEEE Trial-Use Standard for Wireless Access in Vehicular Environment-Security Services for Applications and Management Messages*, IEEE Standard 1609.2-2006.

[18] F. Kargl, P. Papadimitratos, L. Buttyan, M. Müter, B. Wiedersheim, E. Schoch, T.-V. Thong, G. Calandriello, A. Held, A. Kung, and J.-P. Hubaux, "Secure vehicular communications: Implementation, performance, and research challenges," *IEEE Commun. Mag.*, vol. 46, no. 11, pp. 110–118, Nov. 2008.

[19] F. Kargl, E. Schoch, B. Wiedersheim, and T. Leinmüller, "Secure and efficient beaconing for vehicular networks," in *5th ACM Int. Workshop VehiculAr Inter-NETworking*, San Francisco, CA, USA, Sep. 2008, pp. 82–83.

[20] T. Kim, A. Studer, R. Dubey, X. Zhang, A. Perrig, F. Bai, B. Bellur, and A. Iyer, "VANET alert endorsement using multi-source filters," in *Workshop Vehicular Ad Hoc Networks*, Chicago, IL, USA, Sep. 24, 2010, pp. 51–60.

[21] B. Kloiber, T. Strang, M. Rockl, and F. de Pante-Muller, "Performance of CAM based safety applications using ITS-G5A MAC in high dense scenarios," in *Proc. IEEE Intell. Veh. Symp.*, 2011, pp. 654–660.

[22] F. Koushanfar, A. Sadeghi, and H. Seudie, EDA for secure and dependable cybercars: Challenges and opportunities DAC 2012: 220–228.

[23] H. Krishnan and A. Weimerskirch, "Verify-on-demand—A practical and scalable approach for broadcast authentication in vehicle-to-vehicle communication," presented at the SAE 2011, World Congress, Detroit, MI, Apr. 12–14, 2011.

[24] C. Maihöfer, T. Leinmüller, and E. Schoch, "Abiding geocast: Time-stable geocast for ad hoc networks," in *Proc. 2nd ACM Int. Workshop Vehicular Ad Hoc Networks*, pp. 20–29.

[25] National Highway Traffic Safety Administration, Pre-crash scenario typology for crash avoidance research DOT HS 810 767, Apr. 2007.

[26] P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung, and J.-P. Hubaux, "Secure vehicular communications: Design and architecture," *IEEE Commun. Mag.*, vol. 46, no. 11, pp. 100–109, Nov. 2008.

[27] P. Papadimistratos, V. Gligor, and J.-P. Hubaux, "Securing vehicular communications—Assumptions, requirements, and principles," presented at the 4th Workshop Embedded Security Cars, Berlin, Germany, 2006.

[28] P. Papadimitratos and A. Jovanovic, "Protection and fundamental vulnerability of GNSS," presented at the Int. Workshop Satellite Space Commun., Toulouse, France, Oct. 2008.

[29] Personal communication received from a major credit card company.

[30] N. M. Rabadi, "Implicit certificates support in IEEE 1609 security services for wireless access in vehicular environment (WAVE)," in *IEEE 7th Int. Conf. Mobile Adhoc Sensor Syst. (MASS)*, 2010, pp. 531–537.

[31] SeVeCom, "Secure vehicular communications: Security architecture and mechanisms for V2V/V2I, deliverable 2.1," [Online]. Available: http://www.sevecom.org

[32] E. Schoch, F. Kargl, T. Leinmüller, and M. Weber, "Communication patterns in VANETs," *IEEE Commun. Magazine.*, vol. 46, no. 11, pp. 119–125, Nov. 2008.

[33] A. Studer, E. Shi, F. Bai, and A. Perrig, "TACKing together efficient authentication, revocation, and privacy in VANETs," in *Proc. 6th Annu. IEEE Commun. Soc. Conf. Sensor, Mesh Ad Hoc Commun. Netw.*, Jun. 2009, pp. 1–9.

[34] X. Wang *et al.*, Public key cryptography algorithm SM2 based on elliptic curves Chinese Commercial Cryptography Administration Office, Spec. No. GM/T 0003-2012, Mar. 2012.

[35] M. Zhao, J. Walker, and C.-C. Wang, "Security challenges for the intelligent transportation system," presented at the 1st Int. Conf. Security Internet of Things (SECURIT), Kerala, India, Aug. 2012.

Meiyuan Zhao received the Ph.D. degree from Dartmouth College, Hanover, NH, USA, in 2005.

She is a Senior Research Scientist at Intel Labs working on improving the security and usability of the Intel next-generation platforms. She is currently focusing on enable security and trust management for vehicle embedded system, vehicular communications, control systems, machine-to-machine systems. Her research interests include network security, trust management, embedded security, sensor networks, swarm intelligence, peer-to-peer networks, routing protocols, and distributed systems.

Jesse Walker received the Ph.D. degree in mathematics from the University of Texas, Austin, TX, USA.

He is a security researcher in Intel Labs. He reviews crypto for all Intel products. He was one of the designers of SHA-3 finalist Skein, and created the conceptual architecture for Intel's new hardware random number generator. He was the technical editor for the IEEE 802.11 security enhancements, and was the first person to publicly identify the security vulnerabilities in WEP, the original 802.11 WLAN protocol.

Chieh-Chih Wang received the B.S. and M.S. degrees in engineering science and ocean engineering from National Taiwan University, Taipei, Taiwan, in 1994 and 1996, respectively, and the Ph.D. degree in robotics from the School of Computer Science, Carnegie Mellon University, Pittsburgh, PA, USA, in 2004.

From 2004 to 2005, he was an Australian Research Council (ARC) Research Fellow of the ARC Centre of Excellence for Autonomous Systems and the Australian Centre for Field Robotics at the University of Sydney. In 2005, he joined the Department of Computer Science and Information Engineering, National Taiwan University, where he is an Associate Professor and is pursuing his academic interests in robotics, machine perception, and machine learning.

Dr. Wang received the best conference paper awards at the 2003 IEEE International Conference on Robotics and Automation (ICRA) and at the 2010 Conference on Technologies and Applications of Artificial Intelligence (TAAI), and the best reviewer award at the 2007 Asian Conference on Computer Vision (ACCV).