Secure V2V and V2I Communication in Intelligent Transportation Using Cloudlets

Maanak Gupta, James Benson, Farhan Patwa, and Ravi Sandhu, *Fellow, IEEE*

Abstract—Intelligent Transportation System (ITS) is a vision which offers safe, secure and smart travel experience to drivers. This futuristic plan aims to enable vehicles, roadside transportation infrastructures, pedestrian smart-phones and other devices to communicate with one another to provide safety and convenience services. Vehicle to Vehicle (V2V) and Vehicle to Infrastructure (V2I) communication in ITS offers ability to exchange speed, heading angle, position and other environment related conditions amongst vehicles and with surrounding smart infrastructures. In this intelligent setup, vehicles and users communicate and exchange data with random untrusted entities (like vehicles, smart traffic lights or pedestrians) whom they don't know or have met before. The concerns of location privacy and secure communication further deter the adoption of this smarter and safe transportation. In this article, we present a secure and trusted V2V and V2I communication approach using edge infrastructures where instead of direct peer to peer communication, we introduce trusted cloudlets to authorize, check and verify the authenticity, integrity and ensure anonymity of messages exchanged in the system. Moving vehicles or road side infrastructure are dynamically connected to nearby cloudlets, where security policies can be implemented to sanitize or stop fake messages and prevent rogue vehicles to exchange messages with other vehicles. We also present a formal attribute-based model for V2V and V2I communication, called AB-ITS, along with proof of concept implementation of the proposed solution in AWS IoT platform. This cloudlet supported architecture complements direct V2V or V2I communication, and serves important use cases such as accident or ice-threat warning and other safety applications. Performance metrics of our proposed architecture are also discussed and compared with existing ITS technologies.

Index Terms—Smart cars, security, privacy, V2V, V2I, intelligent transportation, ABAC, edge computing, cloud, cloudlets, connected vehicles, trusted communication, amazon web services (AWS)

1 Introduction and Motivation

Future smart world will be equipped with technologies and autonomous devices which collaborate among themselves with minimal human interference. Automotive industry is one of the front runners that has quickly embraced this technological change. Connected vehicles (CVs) and smart cars have been introduced, with a plethora of on-board sensors and applications with internet connectivity to offer safety and comfort services to users. Intelligent transportation for smart cities envisions moving entities interacting and exchanging information with other vehicles, infrastructures or on-road pedestrians. Federal and private agencies are defining communication standards and technologies for Intelligent Transportation System (ITS) to ensure safety, and address security and privacy concerns of end users.

Vehicle to Vehicle (V2V) and Vehicle to Infrastructure (V2I) communication are two proposed technological innovations which can change current transportation. V2V will enable vehicles to exchange information about speed, location, position, direction, or brake status with other surrounding vehicles where receiving vehicles will aggregate these messages and make smart decisions. These on-board applications will warn drivers about accidents, over-speed, slow traffic ahead, aggressive driver, blind spot or a road hazard. V2I will enable road side units (RSUs) or traffic infrastructures to transmit information about bridge permissible height, merging traffic, work zone warning or road hazard detection to complement V2V applications. Vehicle to pedestrian (V2P) is also envisioned to cater to pedestrians, such as with visual or physical impairments, and send corresponding alerts to approaching vehicles. These communication technologies will use Dedicated Short Range Communications (DSRC[1]) to exchange data packets, called Basic Safety Messages (BSM[2]), with nearby vehicles and entities between 300-500 meters range. Messages will be sent up to 10 times per second providing a 360-degree view of proximity, with on-board applications using the information for alerts and warnings. US Department of Transportation (DOT) and National Highway Traffic Safety Administration (NHTSA) estimate around 80 percent of non-impaired collisions [1], [2] and 6.9 billion traffic hours can be reduced by using V2V, V2I and V2P.

Vehicles in ITS will exchange information with external entities including toll booths, gas stations, and other vehicles etc, which raises security and privacy issues. Incidents on Jeep and Tesla [3], [4] have demonstrated how connected

- *Maanak Gupta is with the Department of Computer Science, Tennessee Tech University, Cookeville, TN 38501 USA. E-mail: mgupta@tntech.edu.*
- *James Benson, Farhan Patwa, and Ravi Sandhu are with the Institute for Cyber Security and Department of Computer Science, University of Texas at San Antonio, San Antonio, TX 78249 USA.*
  E-mail: {james.benson, farhan.patwa, ravi.sandhu}@utsa.edu.

Manuscript received 11 January 2020; revised 8 September 2020; accepted 20 September 2020. Date of publication 22 September 2020; date of current version 8 August 2022.
(Corresponding author: Maanak Gupta.)
Digital Object Identifier no. 10.1109/TSC.2020.3025993

[1] https://www.fcc.gov/wireless/bureau-divisions/mobility-division/dedicated-short-range-communications-dsrc-service
[2] https://www.its.dot.gov/cv_basics/cv_basics_how_used.htm

vehicles can be controlled remotely by adversaries. These smart cars are equipped with 100's of electronic control units (ECUs) and more than 100 million lines of code, thereby, exposing broad attack surface for critical car systems including transmission control, air-bag, telematics, engine or infotainment systems. Cyber attacks on smart connected vehicles [5], [6], [7], [8] include: unauthorized over the air updates for firmware, stealing user private data, spoofing sensors, coordinated attacks on road side infrastructure or malware injection. Dynamic and mobile nature of V2X (Vehicle to everything) communication makes it additionally difficult to secure the distributed system where vehicles will be exchanging data with random unknown entities on road. Impersonation and fake message from malicious vehicles is a grave concern as the information exchanged is used by other vehicles for alerts and notifications. Vehicle users have privacy concerns about their movement being tracked continuously or data collected from vehicles used to extrapolate personal identifiable information. To address these concerns USDOT proposed a communications security solution for ITS, called the Security Credential Management System (SCMS) [9], [10], that can ensure trusted communications between vehicles and between vehicles and infrastructure.

Attribute-based access control (ABAC) [11], [12], [13], [14] provides fine grained authorization capabilities for resources. This mechanism offers flexibility in a distributed multi-entity environment where the attributes of entities along with contextual information are used to make access and communication authorization decisions. ITS involves messages exchange among entities with no prior association. Attributes of entities are used to authorize communication based on their location, ownership etc. Such security mechanisms can help to prevent fake messages, stop rogue vehicles and ensure privacy aware communication besides enabling location and time sensitive relevance of exchanged information. ABAC has the ability to capture contextual and dynamic environments like IoT and ITS. Access control models like RBAC [15] and ReBAC [16], will not fit well since they are more suitable for enterprise applications, often with single administrative authority. In case of ITS where vehicle and smart infrastructures are controlled by different users/authorities these are not a good fit.

This work presents an attribute-based V2V and V2I communication architecture and model using edge cloudlets. These cloudlets are setup in geographic locations with limited coverage. Vehicles are dynamically assigned to these cloudlets as they move along geographic boundaries based on their GPS coordinates and predicted path. Each cloudlet receives messages from vehicles in its range and appropriately forwards it to other associated vehicles. The main benefit of this indirect V2V and V2I communication is the deployment of security policies at edge cloudlets which can restrict or block fake messages, and ensure trustworthiness in ITS. Moreover these cloudlets also enable message anonymization and user privacy, as the receiving entity cannot detect who is the sender since all messages come through cloudlets. These cloudlets can forward certificate revocation lists (CRLs) to associated vehicles beside blocking the vehicles themselves. Rogue vehicle list can be dynamically updated at the edges, and messages from a vehicle in the rogue list can be blocked. The proposed architecture and attribute-based policies ensure the important security properties of message integrity, originator authenticity and user privacy in ITS communication. This MQTT[3] based approach for messages exchange can go with DSRC to enable use cases with minimal latency (discussed in implementation section) without the need for additional hardware cost[4] and work with WiFi, LTE or 5G. Our proposed approach complements the USDOT proposed SCMS and can be used as an add on to current peer to peer communication.

The key *contributions* of this paper are as follows:

- It provides an overview of the existing technologies used in V2V and V2I communication, highlighting the USDOT proposed SCMS [9], [10] and related work.
- It identifies security and privacy needs in ITS, discussing threat model for the proposed mechanism and need for cloudlet supported communication.
- It proposes a formalized communication with ABAC security model for V2V and V2I called attribute-based intelligent transportation system (AB-ITS).
- It implements the proposed architecture and model using AWS to reflect the plausibility and efficiency, together with brief comparative discussion on performance metrics.

Rest of the paper is as follows: Section 2 discusses related work. Security requirements along with the proposed cloudlet supported ITS architecture is given in Section 3. Section 4 presents formal attribute-based V2V and V2I communication model (AB-ITS). Section 5 describes implementation using AWS, and discusses performance parameters. Section 6 concludes the paper.

2 Related Work

Connected and smart vehicle applications need wireless exchange of V2X messages among unknown entities. The proposed ITS for future cities has underlying technologies, security concerns and related work, which we briefly review in this section.

2.1 Security Credentials Management System

The United States Department of Transportation (USDOT) has suggested a PKI-based security infrastructure system, called Security Credentials Management System or SCMS [9], [10], to ensure trusted V2V and V2I communication among random moving entities. Authorized participating vehicles use digital certificates issued by SCMS to validate and authenticate basic safety messages (BSMs), by attaching these certificates with each message to ensure integrity, confidentiality and privacy of the communication. Vehicles need initial enrollment into SCMS to obtain security certificates from trusted certificate authorities (CA). Each BSM will include vehicle related information digitally signed using private key corresponding to the digital certificate attached with BSM. Different certificate types are used including enrollment, pseudonym and identification for

[3] http://mqtt.org/

[4] NHTSA proposed V2V equipment and communication is between $341 to $350 per vehicle in 2020 [17]

vehicle and enrollment applications for RSUs. Certificates can be cancelled for potential adversaries or reported misbehaving vehicles by CAs by disseminating certificate revocation lists (CRLs). USDOT and NHTSA claim [2] that BSMs will exchange anonymized information and no personal identifiable data will be shared with other entities. SCMS is considered as a central system to be trusted by entities participating to revolutionize transportation.

However, there are some challenges [18], [19] that need to be addressed before the system is deployed. Each vehicle will receive 20 certificates weekly to sign the BSMs [20], which will rotate every 5 minutes. Therefore, a vehicle will use a new set of 20 certificates every 100 minutes. In such a scenario a computer can analyse all the certificates a vehicle used in a day and then use these certificates to track it for a week. Although, PKI based SCMS system ensures who signed the certificate, it is difficult to prove how correct or true the information sent from the vehicle is. A malfunctioning device in the vehicle can result in false BSMs exchanged even though the sender is trusted. Further, the proposed SCMS system will be largest and complex PKI ever built producing 265B to 800B certs/year depending on weekly rate supporting 17M vehicles/year [19]. The revocation of certificates for bad actors would result in pushing CRLs to all enrolled vehicles, which will be time and bandwidth consuming.

2.2 Relevant Background and Technologies

Several IoT architectures [21], [22], [23] have been proposed with middleware layers in multi-layer stack representing physical objects, communication or service layer, cloud and end-user applications. Gupta and Sandhu proposed [24] enhanced access control oriented architecture (E-ACO) particularly relevant to smart cars and intelligent transportation. The work introduced clustered objects (smart objects with multiple sensors like cars) as component of object layer which interact with other objects, similar to V2V and V2I communication. Recently dynamic groups and ABAC model [25] was proposed for smart cars ecosystem which caters to mobile needs of vehicles. However the model is more suitable to cloud assisted applications and a real time V2V and V2I edge supported model is still missing. Research in [26], [27], [28], [29], [30] has discussed challenges, approaches and novel ideas with respect to VANETs (Vehicular Ad Hoc Network) and intelligent transportation. Security schemes in VANETs have been elaborated in [27]. Another work [28] focuses on the cryptographic viewpoint in VANETs to highlight security concerns. Firat *et al.* [29] elaborate on advanced driver assistance systems (ADAS) applications and novel vehicle intelligence (VI) architecture consisting of ADAS modules and VI services to support fully autonomous vehicles. Anonymous authentication schemes and trust management models for vehicular systems have been proposed by [26], [31]. Edge supported and privacy preserving technologies [32] have been developed for internet of vehicles. Benefits of V2V communication and to quantify the benefits of using V2V communication in terms of a reduction in the employable time headway has been discussed in [33]. Other research intends to explore the role of data science in handling security threats and attack detection [34]. Another work towards evaluating connected vehicles in the cloud was introduced in [31] to meet the requirement of modern ITS.

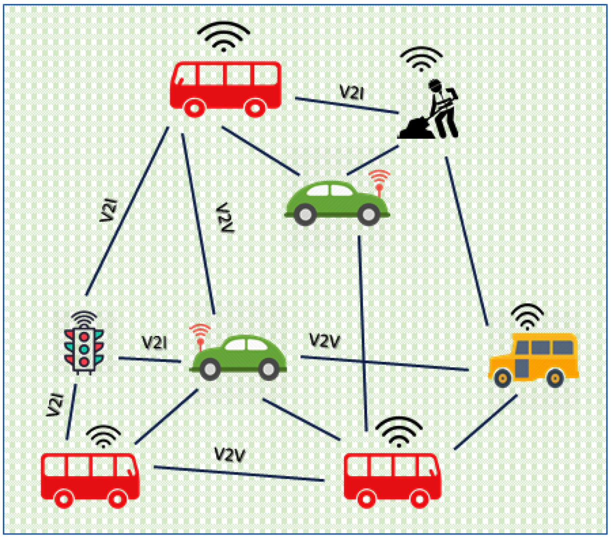


Fig. 1. V2V and V2I Peer to Peer communication.

Federal agencies are working along with industry partners to "fully" proof the ITS before final deployment and use by common public. European Union Agency for Network and Information Security (ENISA) [35] has studied vulnerable assets in smart cars with related threat and risks, and proposed some prevention approaches with recommendations. Cooperative Intelligent Transport Systems (C-ITS) [36], [37] also highlighted the need of data communication integrity and authenticity in V2V and V2I, and proposed PKI based trust model using pseudonym certificates. NHTSA report [38] has thoroughly explored the technical, legal and policy related issues pertinent to V2V communication and studied technological solutions for safety and privacy issues. US Government Accountability Office (GAO) [5] has also discussed security risks and potential attack surfaces in smart vehicles, and proposed solutions to prevent cyber threats.

3 Proposed Cloudlets Supported ITS Architecture

The peer to peer V2V and V2I communication as represented in Fig. 1 is proposed to use SCMS to ensure secure trusted BSMs exchange among entities. However, the vast and complex scale of this PKI based system has user privacy and security concerns which need to be addressed before its deployment. In this section, we will discuss security and privacy requirements of ITS and highlight how the proposed cloudlets supported communication offers the required security and complements current solutions.

3.1 Security and Privacy Needs

ITS involves real time sharing of information like location, direction, vehicle type, etc. which pose security and privacy concerns. Dynamic and distributed ITS will enable interaction with random entities on road with no prior trust established, and the information exchanged will be used by onboard applications to provide safety and warning signals, blind spot warning, accident alerts etc. Basic safety messages (BSMs) are designed to contain no personal identifiable information (PII) and are attached with a certificate issued by certificate authority in SCMS. However, limited number of certificates and number of messages sent per minute can reveal the identity of a targeted vehicle with advanced computer techniques. Untrackability of vehicles and users is paramount to ensure privacy in ITS. The system must not save personal or individual information and use it for law enforcement. Anonymity of sender must always be maintained. Over the air messages exchanged among smart entities must have integrity, and authenticity. Security mechanisms to protect smart cars and their critical systems from unauthorized access, control and tampering are important to strengthen ITS. Integrated approach of DSRC and cellular technologies is needed based on different ITS applications. Cloud and edge supported architectures will provide resiliency and reduce system stress. Encrypted and secure data transfer link is the backbone needed from DSRC, cellular LTE or any communication technologies involved in ITS. However, limited bandwidth and latency issues in cloud connectivity needed for certificate updates and revocation needs attention.

In smart city, location based notifications for connected vehicles must allow user to have personal preferences where a user may want weather warning and not parking advertisements on board. Dynamic policies are required, for example, in case of a traffic jam in an area a policy may ask all drivers to follow route A but considering the heavy traffic on route A, the policy may be changed to move traffic to route B or C. This can be implemented at the edge level and triggered by central administrators. In such a case, whether the administrative subject is authorized to change the policy or trigger an alert, also needs security checks.

3.2 Threat Model

The adversary threat model in this paper is inspired by the USDOT cyber[5] security research focus for a secure connected transportation ecosystem. In particular, some potential threats and vulnerabilities we are focusing on include:

- A registered trusted vehicle with ITS having verified certificates. These vehicles are validated with set of defined criteria at the time of enrollment with central authority (CA) and are considered trusted actors supported by a security certificate. However, it is possible that a vehicle can be compromised by a remote adversary after the enrollment and is able to modify/fabricate the information exchanged in BSMs. This also includes physical tampering of sensors or ECUs by a malicious user.
- Roadside infrastructure is also susceptible to malicious tampering. For example, an adversary can compromise a road-side unit or vehicle to send fake information about traffic or accident, which can trigger unnecessary alerts and may distract drivers.
- It is possible that a sensor in a moving vehicle has malfunctioned and is sending unintentional false messages, which can have negative impact and may issue unwanted and fake alerts to the nearby vehicles. It is important to verify that the exchanged messages are not only from a trusted authorized party, but also if the information sent is correct.

The paper focuses on ensuring trusted communication between vehicles and infrastructures. As connected vehicle applications exchange information among vehicles, roadway infrastructure, traffic management centers, and mobile devices, a security system is needed to ensure that users can trust the validity of information received from other system user whom they have never met and do not know personally. Our proposed ABAC supported policy based approach complements USDOT SCMS solution, and offers additional benefits to prevent fake messages exchange.

3.3 Benefits of Cloudlets Supported Communication

Fig. 2 shows the proposed edge supported architecture for V2V and V2I communication. Trusted edge infrastructures (setup by city administration) will work as a middle man and relay messages to vehicles and other entities inside its geographic range. Instead of peer to peer connection, all vehicles publish to edges, where security policies are checked to ensure validity and integrity of the communication, and relevance of messages, before forwarding to other vehicles. A vehicle can be in range of multiple infrastructures, depending on its location and will be dynamically associated with edges as it moves. All participating vehicles and RSUs still need to enroll with a central authority to be part of the system, to ensure that only trusted vehicles are allowed to exchange messages. Communication technologies used for vehicles to cloudlets can be cellular LTE, WiFi or DSRC. MQTT protocol can be used, as discussed in implementation, will obviate the cost of DSRC equipment needed in vehicles. The proposed architecture is implemented in addition to direct V2V and V2I as supported in NPRM [39] documents which recommend both DSRC and secondary communication for ITS.

Trusted cloudlets installed in wide geographic area offer the needed fog infrastructure functionality required in an IoT environment. Similar to any device which wants to be associated with the ITS (as discussed in USDOT specifications[6]), these edge infrastructures must be enrolled into the system by submitting an enrollment request to a central authority. Once authorized, devices are considered trusted actors in the system. A certification process will ensure that devices meet program requirements and perform as intended. They can address security concerns by deploying and enforcing security policies to ensure trusted communication among smart entities on the road. This proposed architecture offers an alternate edge supported V2V and V2I communication with minimal message latency and in permissible time limits [40], [41]. Vehicle sending and receiving BSM must be associated with an edge infrastructure, which will enforce policies, sanitize messages, prevent fake messages dissemination and offer administrative advantages. Each cloudlet will have a geographic range and vehicles within it will get associated with the edge automatically.

[5] https://www.its.dot.gov/factsheets/cybersecurity.htm

[6] https://www.its.dot.gov/resources/scms.htm

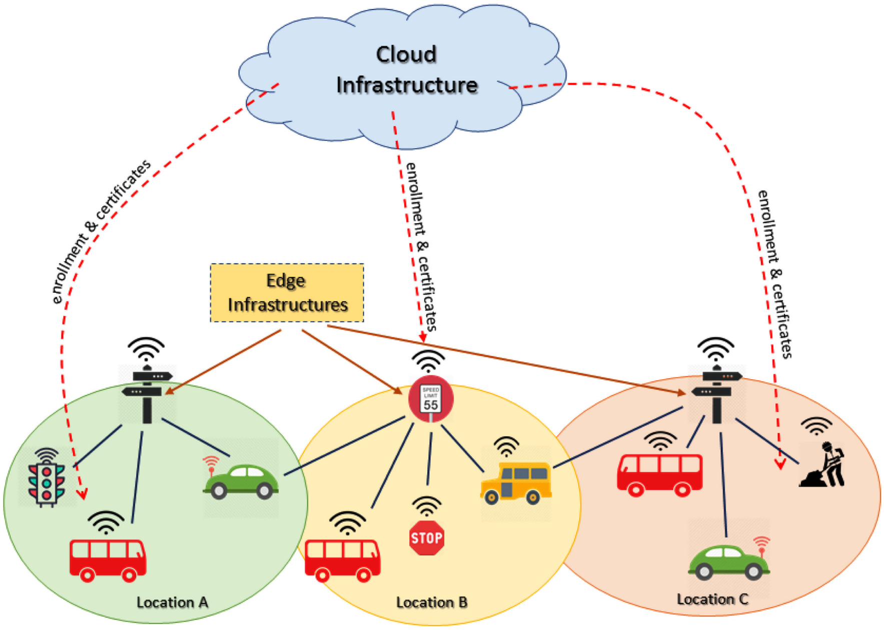


Fig. 2. Proposed trusted cloudlets supported V2V and V2I communication architecture.

Since the range of edge is within a restricted limited area, it also ensures location sensitivity of messages exchanged, as vehicles communicating messages must be associated to a common cloudlet. Message anonymity is ensured, since messages sent by a vehicle are relayed via edge which can remove certificates information. Cloudlet verifies if content of the messages are correct and in tandem with messages received by other vehicles in the system, so as to prevent any relay of fake/compromised messages to other receiving vehicles as discussed in the threat model.

Cloudlets can offer administrative benefits as single notification from edge infrastructure will trigger alerts for all the vehicles which are connected to it in a geographic range. If an agency or a police vehicle wants to send alerts, instead of sending to each individual vehicle, they can send it to a trusted cloudlet, which after checking the policies to ensure the sender is allowed to generate such requests, forwards or stops the message. Also, entities present in a particular area have certain characteristics (for example, stop sign warning, speed limits, deer-threat, flash flood warnings etc.) in common, which can be inherited by getting dynamically associated to edge infrastructures, without the need to generate messages 10 times per second [38] to get this information from other vehicles or RSUs saving network bandwidth.

It is also possible to limit the messages to a specific set of vehicles, for example, in case of a kidnapped child warning, messages can be sent to nearby edge infrastructures and then to only police vehicles in the area, and not to the common public using security policies defined at the cloudlet. Edge infrastructure can also have the capacity to filter unwanted and incorrect messages from the vehicles and infrastructure using a majority rule policy. For example, if an adversary is sending accident message (either deliberately or a malfunction sensor on vehicle) to subvert the traffic whereas other vehicles notify no accident and clear traffic messages, installed trusted edge will have the intelligence and policy to filter such fake messages and forward the correct information to its associated vehicles. This will not be possible in peer to peer V2X (vehicle to anything) architecture immediately, until certificate revocations (by a central authority) are propagated to individual vehicle, which may take time and also require internet connectivity which cannot be guaranteed all times in terrains where the vehicle is moving. Also, instead of sending CRLs to each vehicle, only edge servers can be sent with list of revoked certificates and based on the information, edge can decide if the messages sent by vehicle should be forwarded or not.

Since, this proposed solution complements SCMS [9], [10], it supports and builds upon the following security properties based on the USDOT ITS cyber security[7] focus areas:

Authenticity & Trust. Vehicles exchanging messages as a part of ITS are certified to be trusted based on enrollment request to a central authority. These entities obtain security certificates, and attach it to their messages as part of a digital signature. The certificates prove a device is a trusted actor in the system. This is one time process and vehicles are registered with the cloud service as shown in Fig. 2 as supported by SCMS. However, how to ensure that messages data exchanged is not fake either due to malfunctioning or compromised sensor is how our solution ensures trust in the system, as cloudlets verify every message before forwarding to other vehicles. Cloudlets empower trust in the contents of exchanged messages as well.

Confidentiality & Integrity. Communication between cloudlets, connected devices and cloud is encrypted using Transport Layer Security (TLS) or other protocol supported by SCMS. All data sent to the cloud is sent over an TLS connection using MQTT or HTTPS protocols, as discussed in the implementation section. Our solution ensures that the content of messages is not modified to support the integrity. This is done without computationally expensive cryptography and in near real time by evaluating security policies

[7] https://www.its.dot.gov/factsheets/cybersecurity.htm

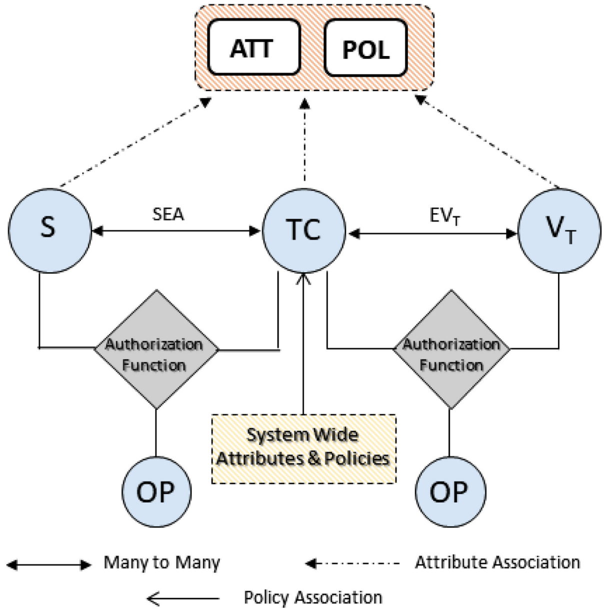


Fig. 3. A conceptual AB-ITS communication model.

which are defined only by system administrators. The confidentiality of vehicles is still maintained since there is no way for the receiving vehicle to find out from where it received the message, as message broadcast is done by the connected cloudlet.

Anonymity & Privacy. The messages and data exchanged among the vehicles and infrastructure comply with the BSM data fields[8] as issued by the USDOT. These messages contain no personal identifiable information (PII) maintaining the anonymity of the users. Similar structure has been used in our implementation, as elaborated in Section 5. The anonymity and privacy of vehicles is maintained with respect to other vehicles which will receive messages, since cloudlets will remove any certificates from the messages sent which will then be forwarded to vehicles.

Our proposed solution supports and extends SCMS system (discussed in Section 2) which enables peer to peer V2V and V2I communication. It extends the functionalities of SCMS infrastructure to support ABAC based security policy solution. We assume that the vehicles are already trusted and have the needed credentials or certificates to exchange messages. In our use-case implementation (Section 5), we register simulated vehicles into the system before they can send messages to cloudlet.

4 Cloudlets Enabled Attribute Based V2V and V2I Communication

Here, we formally define cloudlets supported attributes based intelligent transportation system model, referred to as AB-ITS.

4.1 AB-ITS Communication Model

Conceptual AB-ITS model is shown in Fig. 3 with formal definitions in Table 1. The model has following components: Vehicles (V), Transportation Infrastructure Devices (I), Users (U), Sources (S), Trusted Cloudlets (TC), Target Vehicles (V_T), Operations (OP), Authorization Policies (POL), and Attributes (ATT).

Sources (S). A source initiates operations on cloudlets (discussed below) in the system. A source can be from the set of vehicles (V), transportation infrastructure (I) or administrator users (U). For instance, in case of V2V communication, the source is a vehicle which wants to send messages to other vehicles in its vicinity. Similarly, law enforcement and city administration can initiate theft and accident alerts in a particular area via cloudlets, which are forwarded to all vehicles associated with that cloudlet.

Trusted Cloudlets (TC). Cloudlets are edge infrastructures set up across locations and facilitate secure V2V and V2I communication. These cloudlets have a limited geographic range and all vehicles in that range get associated with one or more TCs automatically based on their moving location coordinates. These devices enroll into the system by submitting an enrollment request to CA. Once authorized, devices are considered trusted actors in the system. A certification process will ensure that devices meet requirements and perform as intended. Any communication between vehicles and other entities including transportation infrastructures (or RSUs) is done via TC, which check security policies to forward or block messages sent by different sources. Also TCs have attributes which are propagated to associated vehicles and can also help setting alerts and warnings based on attribute values.

Target Vehicles ($\mathbf{V_T}$). These vehicles are potential receivers of messages sent by a source, whereby $V_T = V$. Both target vehicle and source must be associated with same TC to enable V2V and V2I communication.

Operations (OP). Operations are actions which are performed by source on TC. Further, TCs also execute operations on associated target vehicles and infrastructures. For example, a source initiating a join operation to get associated with a TC, or trying to send a message to vehicles via TC. Also, TC forwarding a message sent by sources to its member vehicles is another example of operations in ITS. These also include administrative actions performed by an administrative user including updating, deleting or adding attribute values for an attribute or rogue vehicles list in TC.

Authorization Policies (POL) and Attributes (ATT). Sources, TCs, vehicles and other ITS entities can have personal defined individual policies along with system wide authorization policies needed for the overall secure functioning of the ecosystem. Vehicle owners can set individual privacy preferences which enable them to allow or disallow any particular private information from being shared with a third party remotely. City traffic department may set its own rules when to trigger an alert or warnings to vehicles in a sensitive or accident prone area. Administrative policies are also needed to authorize a legitimate user to change attributes, send notifications to TCs or update rogue vehicles list. Entities like vehicles and sources also have individual characteristics, called attributes, which are used to make authorization and communication decisions. For a vehicle, attributes can be: vehicle ID, speed, heading angle, brake, vehicle size, vehicle type or preferred notifications. Vehicles and infrastructure can also inherit attributes from their associated TCs, which can have common attributes like speed limit, road work ahead or blind turn.

[8] https://data.transportation.gov/Automobiles/Wyoming-CV-Pilot-Basic-Safety-Message-One-Day-Samp/9k4m-a3jc

Both attributes and policies are dynamic which can be changed by administrators or vehicle owners based on system needs and personal preferences. The attributes of vehicles like location, speed or heading angle are continuously changing, but other attributes like vehicle size remain static. Policies are also dynamic in nature, as reflected in use-case implementation in the next section, where we defined a security policy with a list of black-listed rogue vehicles which are notified to law enforcement when detected by TCs. This list is dynamic in nature and is continuously updated by administrators, demonstrating how dynamic policies are used and enforced in ITS. It must be noted that in a session the proposed model assumes a static set of policies and attributes which are used to make V2V and V2I communication decision. All relevant polices including system defined and user preferences are evaluated to make the final communication decision.

In our model, TCs evaluate security policies and ensure that untrusted or fake messages are not forwarded to associated vehicles in their geographic coverage boundary. These connected vehicles must initiate association with a TC proactively based on their predicted path, and once they get into the range of the TC, vehicles become a member of that TC. Such communication with TCs can be done using encrypted and secure cellular or WiFi technologies with no added equipment cost.

4.2 Formal Definitions

Table 1 elaborates the formal AB-ITS communication model definitions, which comprise of vehicles (V), transportation infrastructure devices (I), administrative users (U) and edge cloudlets (TC). A source in S initiating an operation op $\in$ OP can be from a set of vehicles, transportation infrastructures or users, and target vehicles $V_T = V$. Attributes are functions defined for sources and edge cloudlets. These functions can be set or atomic valued (specified by attType) and are assigned values from Range(att) for each att $\in$ ATT. Atomic valued attributes are assigned a single value including null (denoted as $\perp$) whereas set valued attribute are assigned a subset of values from the range. Some attributes are also defined system wide, which reflect the state of entire transportation system (like level of threat or city traffic) and are set by administrators. Authorization policies are defined for individual sources and TCs, which are either stated based on personal privacy preferences or are enforced system wide defined by administrators. For example, a driver may not want to receive marketing commercials, so she can set such personal preference by choosing the desired policy, whereas police can define a policy blocking communication from a list of black-listed cars.

Vehicles are dynamically assigned to one or many trusted edge cloudlets based on their current GPS coordinates and predicted path as defined by associated_cloudlets function. The association with edge cloudlets is fixed for transportation infrastructures or administrators which are assigned at the time of system deployment whereas for vehicles it keeps on changing as the vehicles move. Each cloudlet has defined geographic coverage area and when vehicles enter the area, they get associated with the cloudlet. A vehicle may be associated with multiple cloudlets in areas where coverage areas are overlapping, thereby, a vehicle is always associated to at least one cloudlet at all times. These cloudlets mediate the V2V and V2I communication by enforcing security policies, so as to stop fake messages and ensure privacy, as discussed later in the model definitions. Further, sources (including vehicles) inherit attributes from their associated cloudlets, which helps in administration and propagation of common attributes to all associated entities with single administrative action. For instance, at a location where flash flood warning is issued, the edge cloudlet installed there will set attribute flash-flood = ON for all its associated vehicles when they become members of that cloudlet. In case of set valued attribute function, the effective attribute values for att $\in$ ATT of source (defined as $\mathrm{effS_{att}}$), including target vehicles, is the union of direct values assigned to the source for attribute att and the values assigned to att for each associated cloudlets. However, in case of atomic valued attribute, it is necessary to define which attribute values take precedence when multiple edge clouds are associated. In our model, we propose that most recently connected cloudlet with non-null value for the attribute will be inherited by the associated source or vehicles.[9] For example, the speed-limit attribute of most recently associated cloudlet will be populated for all member vehicles, and as the vehicle moves, this value is inherited from next associated edge cloudlet and so on. This inheritance in atomic values attribute only takes place when edge cloudlets have non-null values, whereby with all associated cloudlets having null values, the direct attribute value of the source holds as its effective value also.

Authorization functions are parameterized propositional logic formulae defined to represent access control security policies stated in the policy language defined in Table 1. The function $\mathrm{Auth_{op}}$(s:S, tc:TC) specify conditions under which source s (including vehicles) can perform an operation op $\in$ via cloudlet tc $\in$ TC. These boolean authorization functions are evaluated substituting actual arguments for formal parameters along with direct and effective attributes values of actual arguments. Similar syntax and policy language can be defined for other set of policies including personal vehicle specific policies or system wide policies with attributes of relevant entities substituted in authorization requests evaluation. Authorization decision to allow $s' \in$ S to perform an operation op $\in$ OP on $tc' \in$ TC is determined when the authorization function is evaluated with the actual arguments ($s' \in$ S, $tc' \in$ TC) to be True. Similarly, the decision for operation op from $tc' \in$ TC to $v' \in V_T$ is made by calling the relevant authorization function with actual parameters.

As discussed in authorization property, the model has defined two primitive operations, ‘send’ and ‘forward’ relevant for V2V and V2I communication. A source uses ‘send’ operation (with authorization specified by $\mathrm{Auth_{send}}$(s': S, tc': TC)) to communicate a ‘send message’ to trusted cloudlet, whereas ‘forward’ operation (with authorization specified by $\mathrm{Auth_{forward}}$(tc': TC, v': V_T)) is between trusted cloudlet and target vehicle defining a ‘forward message’. Communication from s' to v' requires a common tc' to which both $s'$and $v'$are associated and the required authorization functions for send and forward messages i.e $\mathrm{Auth_{send}}$(s': S, tc':

[9] There are other approaches also to deal with atomic value inheritance, but for moving vehicles which are dynamically assigned to new cloudlets, we believe this approach is the most appropriate and relevant.

TABLE 1
Formal AB-ITS Communication Model Definitions

Basic Sets and Functions

– V, I, U, TC are finite sets of vehicles, transportation infrastructure devices, (administrative) users, and trusted cloudlets respectively.

– S, $\mathrm{V_T}$, OP are finite sets of sources, target vehicles, and operations respectively, where S = I ∪ V ∪ U and $\mathrm{V_T}$ = V.

– ATT is a finite set of attributes associated with S, TC, and system-wide.

– For each attribute att in ATT, Range(att) is a finite set of atomic values.

– attType: ATT = {set, atomic}, defines attributes to be set or atomic valued.

– Each attribute att in ATT maps entities in S and TC, and system-wide to attribute values. Formally,

$$\text{att} : \text{S} \cup \text{TC} \cup \{\text{system-wide}\} \rightarrow \begin{cases} \mathrm{Range(att)} \ \cup \{\perp\} & \text{if attType(att) = atomic} \\ 2^{\mathrm{Range(att)}} & \text{if attType(att) = set} \end{cases}$$

– POL is a finite set of authorization policies associated with individual entities in S and TC, and system-wide.

– associated_cloudlets : $\mathrm{S} \rightarrow 2^{\mathrm{TC}}$, maps each source (including target vehicles) to a set of trusted cloudlets.
Equivalently, relations SEA = $\{(\mathrm{s, tc}) \mid \mathrm{tc} \in \text{associated\_cloudlets(s)}\}$ and $\mathrm{EV_T}$ = SEA ∩ ($\mathrm{V_T}$ × TC).

Effective Attributes of Sources Including Vehicles

– For each attribute att in ATT such that attType(att) = set :

- $\mathrm{effS_{att}}$: S → $2^{\mathrm{Range(att)}}$, defined as $\mathrm{effS_{att}(s)} = \mathrm{att(s)} \bigcup_{\mathrm{tc} \in \text{associated\_cloudlets(s)}} \mathrm{att(tc)}$.

– For each attribute att in ATT such that attType(att) = atomic :

- $\mathrm{effS_{att}}$: S → Range(att) ∪ {⊥}, defined as

$$\mathrm{effS_{att}(s)} = \begin{cases} \mathrm{att(s)} & \text{if } \forall\ \mathrm{tc} \in \text{associated\_cloudlets(s)}.\ \mathrm{att(tc)} = \perp, \text{otherwise} \\ \mathrm{att(tc)} & \text{where tc was most recently assigned } \mathrm{att(tc)} \neq \perp \text{ amongst all } \mathrm{tc'} \in \text{associated\_cloudlets(s)} \end{cases}$$

Authorization Functions (Policies)

– Authorization Function: For each op ∈ OP, $\mathrm{Auth_{op}(s : S, tc : TC)}$ is a parameterized propositional logic formulae returning true or false, defined using the following policy language:

- $\alpha ::= \alpha \wedge \alpha \mid \alpha \vee \alpha \mid (\alpha) \mid \neg\alpha \mid \exists\ \mathrm{x} \in \mathrm{set}.\alpha \mid \forall\ \mathrm{x} \in \mathrm{set}.\alpha \mid \mathrm{set} \bigtriangleup \mathrm{set} \mid \ \mathrm{atomic} \in \mathrm{set} \mid \mathrm{atomic} \notin \mathrm{set}$
- $\bigtriangleup ::= \subset \ \mid \ \subseteq \ \mid \ \not\subseteq \ \mid \cap \mid \cup$
- $\mathrm{set} ::= \mathrm{effS_{att}(s)} \mid \mathrm{att(i)}$ for att ∈ ATT, i ∈ S ∪ TC ∪ {system-wide}, attType(att) = set
- $\mathrm{atomic} ::= \mathrm{effS_{att}(s)} \mid \mathrm{att(i)} \mid \mathrm{value}$ for att ∈ ATT, i ∈ S ∪ TC ∪ {system-wide}, attType(att) = atomic

– Authorization Function Evaluation: Authorization functions are evaluated by substituting actual arguments for formal parameters along with attribute values of actual arguments, thus reducing the parameterized formula to a propositional logic formula for evaluation.

Authorization Decision

– A source s′∈ S is allowed to perform an operation op ∈ OP on edge cloudlet tc′∈ TC (where s′and tc′are actual arguments), if all the required policies stated in $\mathrm{Auth_{op}}$(s′: S, tc′: TC), are satisfied. Formally, $\mathrm{Auth_{op}}$(s′: S, tc′: TC) = True.

Authorization Communication Property

– To communicate a message between s′∈ S and v′∈ $\mathrm{V_T}$ requires authorization for individual operations {send, forward} ∈ OP where send[s′, tc′] and forward[tc′, v′] are operation signatures meaning send operation is performed by s′to tc′and forward is executed by tc′to v′. The authorization functions evaluated to allow communication between s′and v′include $\mathrm{Auth_{send}}$(s′: S, tc′: TC) and $\mathrm{Auth_{forward}}$(tc′: TC, v′: $\mathrm{V_T}$).

– A source s′∈ S is allowed to communicate a message to vehicle v′∈ $\mathrm{V_T}$ if both the source and vehicle are associated with the same trusted cloudlet tc′∈ TC, and all the required policies are evaluated to make communication authorization decision. Formally, ∃ tc′∈ TC. ($\mathrm{Auth_{send}}$(s′: S, tc′: TC) ∧ $\mathrm{Auth_{forward}}$(tc′: TC, v′: $\mathrm{V_T}$)) ∧ (System-Wide Policies) = True

TC) and $\mathrm{Auth_{forward}}$(tc′: TC, v′: $\mathrm{V_T}$) as well as the system defined security policies evaluate to True. Additional relevant operations and messages can be similarly defined.

The proposed AB-ITS model leverages attributes and GPS coordinates of communicating entities to enable and secure V2V and V2I communication. The introduction of trusted cloudlets provide benefits of enforcing security policies at the edge to stop fake messages, enhance user privacy and integrity of messages before forwarded to other target vehicles. These edge cloudlets ensure low latency and near real time communication much needed in most ITS applications without bandwidth issues. The messages shared among source and vehicles are end to end encrypted and can still use the proposed DSRC wireless technology for communication with cloudlet and then to the vehicles.

5 Implementation in AWS

In this section we present a proof of concept implementation of AB-ITS model in Amazon Web Services (AWS[10]). We

[10] https://aws.amazon.com/

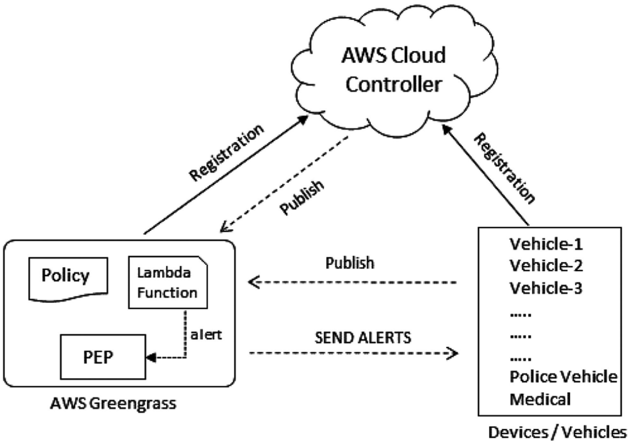


Fig. 4. System architecture.

use AWS IoT service along with AWS Greengrass[11] (to provide edge functionality) to setup a realistic environment where vehicles are simulated as AWS IoT things. In particular, these stand alone services are implemented as a Lambda[12] function using Boto[13] which is AWS SDK for Python. It should be noted that in this implementation no long term GPS data coordinates of vehicles are collected in cloudlets. This reduces privacy concerns of end users and encourages adoption of the proposed model.

5.1 Use Cases Overview

USDOT has an extensive list of ITS applications[14] which we have used to create our use cases. Our implementation addresses trust, security and privacy issues concerning end users which must be satisfied before bringing ITS technology in practice. As most applications are safety related, we have considered accident and ice-on-road (tire slip) alerts as our running use case along with real-time detection and prevention of rogue (or malicious) vehicles on road. In the use cases, we have also shown how different entities (S, TC, V_T etc.) fit in model definitions.

Accidental Safety and Ice-Threat. Moving vehicles (S) can generate warnings for other vehicles (V_T) in their surrounding based on an event which they sensed or encountered. In our use case, we consider ‘ice-threat’ alerts based on a tire slip wherein vehicles are notified a warning, if any nearby vehicle ‘feels’ it and broadcasts, after satisfying security policies implemented at the edge infrastructures (TC). These policies take into account: who is the source of alert, location of vehicle (ATT) and how many other vehicles encountered similar event, before forwarding (OP) these alerts to other nearby approaching vehicles (V_T). It is possible that a single vehicle (S) sends an ice-threat alert to associated cloudlet (TC), while other vehicles in the area sense no such movement. Therefore the edge will be able to filter such malfunctioning or deliberate malicious attempt from the vehicle and also notify law enforcement and put that vehicle in rogue vehicles list. Further, in case of an accident, alert messages will be generated and sent only to police or medical vehicles in the area. Based on the type of alerts and who generates it, policies are defined in the system to ensure trusted, anonymized and relevant notifications.

TABLE 2
AWS Setup Parameter Information

Message Queue Size	2.5 MB
Number of AWS Greengrass Groups	4
Range of Vehicles per groups	1 – 50
Published Range of Messages (per second per vehicle)	1 – 20
Greengrass Server Configuration	8 VCPUs, 4 GB RAM
Simulated Vehicles Server Config.	2 VCPUs, 4 GB RAM
Average Network traffic (50 vehicles)	255 Kbps
Network Capacity of Interface	1.84 Mbps

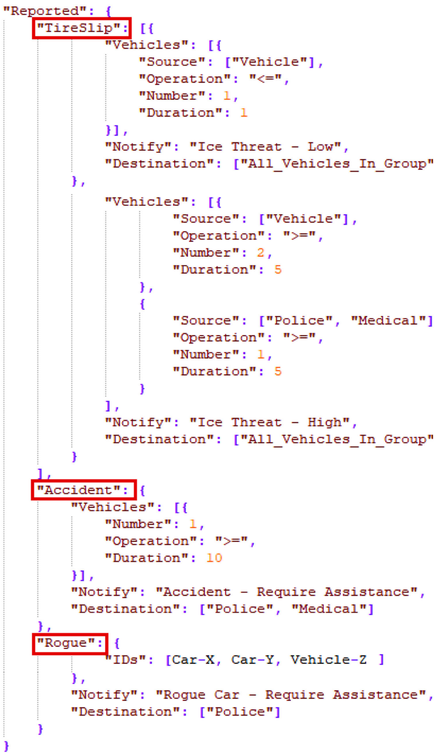
Compromised Rogue Vehicles. Rogue vehicles, either intentionally or due to sensor failure, can send fake messages to other vehicles. Misbehaving and compromised vehicles must be detected and alerts must be issued immediately to discard the information sent by them. In our use case, central cloud authority (S) informs edge infrastructures (TC) with a list of detected rogue vehicles so that when any message is received by an edge from these vehicles, it is not forwarded to other vehicles. Further, law enforcement is informed about the location (ATT) of a rogue vehicle to prevent fake message dissemination. This approach eliminates the need to update and publish revocation list to all vehicles eliminating the bandwidth and connectivity issues.

5.2 Proof of Concept

We will first go over the system configuration along with implemented security policies defined in the cloudlet before we delve into additional details of our developed prototype.

System Architecture. Fig. 4 represents system architecture along with different components implemented for our prototype. Vehicles and static smart entities including edge infrastructures are registered with a central cloud controller to ensure trusted authorized participating entities. The controller also helps in the administrative phase (discussed later) which includes providing a list of cloudlets on designated path of moving vehicle. Once the registration is done and vehicles are sent a list of cloudlets, vehicles publish and subscribe to secure (and reserved) MQTT topics created in each cloudlet which get dynamically assigned based on vehicle GPS coordinates. It is also possible that the moving vehicle keeps on sending coordinates to the cloud and the controller lets them know the IP address of the nearby edge infrastructures to which the vehicle has to associate. These cloudlets (represented as AWS Greengrass) hold the implemented security policies, a lambda function (similar to policy decision point - PDP [12]) for policy evaluation and the policy enforcement point (PEP) to check messages received, anonymize and filter them and based on the type of alert send them to relevant entities. It should be noted that only alert messages go through the enforcement point, whereas no alerts messages are discarded after logging. Table 2 lists different AWS system parameters to provide a better understanding of performance metrics shown later in this section.

[11] https://aws.amazon.com/greengrass/
[12] https://aws.amazon.com/lambda/
[13] https://aws.amazon.com/sdk-for-python/
[14] https://www.its.dot.gov/pilots/cv_pilot_apps.htm/



```
"Reported": {
    "TireSlip": [{
        "Vehicles": [{
            "Source": ["Vehicle"],
            "Operation": "<=",
            "Number": 1,
            "Duration": 1
        }],
        "Notify": "Ice Threat - Low",
        "Destination": ["All_Vehicles_In_Group"
    },
        "Vehicles": [{
                "Source": ["Vehicle"],
                "Operation": ">=",
                "Number": 2,
                "Duration": 5
            },
            {
                "Source": ["Police", "Medical"]
                "Operation": ">=",
                "Number": 1,
                "Duration": 5
            }
        ],
        "Notify": "Ice Threat - High",
        "Destination": ["All_Vehicles_In_Group"
    }
    ],
    "Accident": {
        "Vehicles": [{
            "Number": 1,
            "Operation": ">=",
            "Duration": 10
        }],
        "Notify": "Accident - Require Assistance",
        "Destination": ["Police", "Medical"]
    },
    "Rogue": {
            "IDs": [Car-X, Car-Y, Vehicle-Z ]
        },
        "Notify": "Rogue Car - Require Assistance",
        "Destination": ["Police"]
    }
}
```

Fig. 5. Implemented security policies.

Security Policies. We defined attributes based policies which are enforced at the edge, to check who is allowed to send messages, conditions when the message is forwarded to other vehicles and who are authorized recipients for different types of alerts in the system.

Various attributes can be included in policy but for the sake of simplicity we used only vehicle type to determine the source and destination of messages. As shown in Fig. 5, security policies are listed in JSON format, where three types of alerts are being generated, 'TireSlip', 'Accident' and 'Rogue' vehicle updates, as denoted by red rectangular boxes. We defined separate set of conditions for each alert type. For example, in 'TireSlip' alerts, it is first checked if it is generated ('Source' attribute) by a regular vehicle (specified by attribute value 'Vehicle') or by law enforcement ('Police' or 'Medical'). Policy then checks number of vehicles which created similar alerts (specified by "Number" attribute). Notification to other vehicles depends on how many alerts were generated or who is the source of alert. If the number of alerts is greater than or equal to 2 from regular vehicles, or even a single alert from police or medical vehicle, "Ice-threat High" notifications are sent to other associated vehicles of the cloudlet. However, if an alert is generated by one regular vehicle, "Ice Threat - Low" is sent for all member vehicles. It must be noted that the sender vehicles and the receiving vehicle must be associated with the same cloudlet to exchange notifications, which also ensure relevance of alerts being received. Similarly, for accident use case, notification is only sent to nearby police vehicles and medical with assistance message. Here the source is not defined, since any smart entity including vehicle, or nearby smart road side sensor or a pedestrian can send message to police or medical vehicles. It is also possible that information about the vehicle including color, license plate number or other identifying information can be sent to law enforcement. Another important use case is to enable a central law enforcement that can regularly publish and update the list of rogue vehicles. This list for example, could help locate vehicles that have been stolen or implicated in amber alerts In the last part of our policy for 'Rogue', vehicle IDs `Car-X`, `Car-Y`, `Vehicle-Z` are stated as rogue and any message from these vehicles is not forwarded. This is a dynamic policy as the list is periodically updated by a central authority. Also to extend the use case, it is possible when an edge receives a message from a rogue vehicle, it can forward that information to nearby police along with vehicle information like license number and color. The defined policies are only for alert messages, and other 'no alerts' messages are just checked by the policy and are logged and dropped without forwarding to any vehicle.

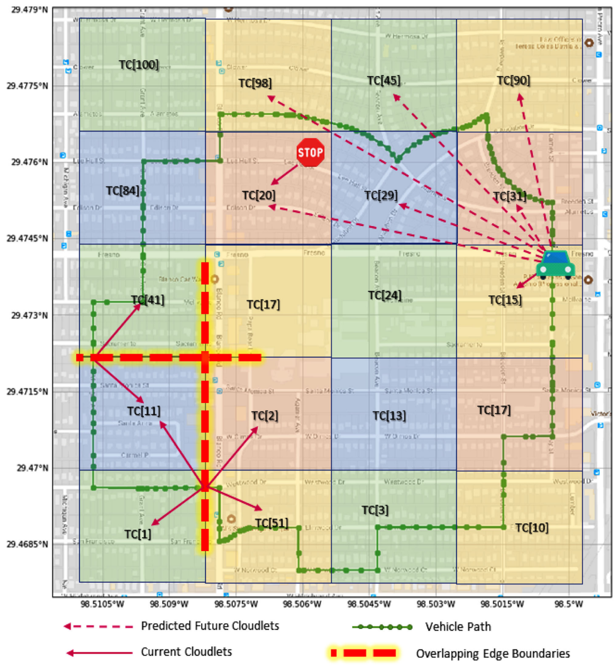


Fig. 6. Moving vehicle cloudlets association.

Implementation Details. Implementation involves two steps: the administrative phase and the operational phase. Administrative phase includes setup of cloudlets by administration, setting up the boundaries for each cloudlet, dynamic assignment of moving vehicles to edge infrastructures, and attributes and alerts inheritance from edges to the member vehicles. To be part of ITS, vehicles and smart infrastructures need to have one time registration with central cloud. The moving vehicles can be provided with a mapped list of edges which will arrive in their designated route to which they are allowed to connect. As the vehicles get dynamically associated to different cloudlets, they are able to publish and subscribe to the reserved topics on each edge infrastructure. The operational phase consists of how these attributes and assignment to cloudlets ensure the relevance of alerts to the vehicles and how the edge deployed security policies are used to mitigate security and privacy concerns of users who are using AB-ITS system.

In our prototype, we demarcated a big geographic location area into several smaller regions and each region has a

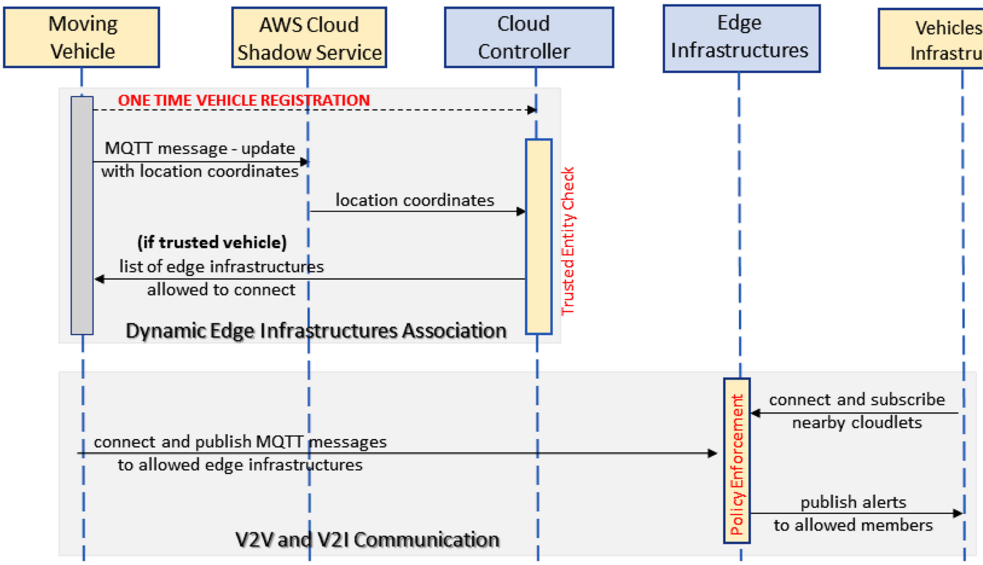

Moving Vehicle
AWS Cloud Shadow Service
Cloud Controller
Edge Infrastructures
Vehicles and Infrastructure
ONE TIME VEHICLE REGISTRATION
MQTT message - update with location coordinates
location coordinates
(if trusted vehicle) list of edge infrastructures allowed to connect
Trusted Entity Check
Dynamic Edge Infrastructures Association
connect and subscribe nearby cloudlets
connect and publish MQTT messages to allowed edge infrastructures
Policy Enforcement
publish alerts to allowed members
V2V and V2I Communication

Fig. 7. Sequence diagram for cloudlets supported V2V and V2I communication.

trusted cloudlet (TC) which serves all the smart entities in the region as shown in Fig. 6. We used a Python script to simulate the movement of vehicles in the system, shown as green dots, which sends MQTT messages containing GPS coordinates to a central cloud. Service in cloud determines which edge cloudlets are in the surrounding area of the vehicle and then assigns the vehicle to the nearby cloudlets. Following is the sample MQTT payload sent by a moving vehicle to its shadow reserved topic `$aws/things/'Vehicle-Name'/shadow/update` in the cloud for dynamic cloudlet assignment:

```
{"state":{"reported":
   {"Latitude":"28.1452683",
    "Longitude":"-97.567259"}}}
```

As the path of vehicle is mostly known, these edge assignments can be pro-active in nature as well, mitigating the concern of cloud latency. In such a case, the cloud controller can send a list of edge infrastructures which will be on the designated path of the vehicle to get them associated when vehicles come in their range. It is also possible that these cloudlets have a wireless range and the vehicles which are in the range get automatically assigned to these cloudlets. A vehicle can associate to multiple cloudlets at a time based on their overlapping location. In Fig. 6, static smart objects like stop warning signs, road work ahead or other infrastructures have fixed allocation to cloudlets, and the dotted lines represent predicted future cloudlets of vehicle along with current cloudlets by solid pink lines.

Once vehicles get assigned to nearby cloudlets, operational phase starts where the vehicles send messages to its shadow reserved topic (which gets created when the vehicle becomes member of a cloudlet) in their associated edges, which enforce security policies to ensure trusted and authorized alerts to nearby vehicles in near real time manner. In all the policies defined, privacy of the sender is well preserved as the messages do not contain any personal identifiable information and are anonymous. Following is a sample MQTT message sent by vehicle:

```
{"state":{"reported":
 {"Longitude":"29.472741982",
  "Latitude":"-98.50038363",
  "Time":"2019-03-19 11:27:40.237734",
  "Velocity":"30","Direction":"north",
  "Elevation":"650","Posit. Accuracy":
  "5","Steering Wheel Angle":"0",
  "Alert":myAlert}}}
```

In this message, beside BSM [42] attributes, an attribute "Alert" also exists, which defines what kind of alert has been sent from the vehicle to cloudlets. For our use cases, it can be an "Accident", "Tireslip", or "Null" value where Null signifies no alert. Once the message is received by cloudlet, and is checked against the policies, the edge infrastructure forwards the following Tireslip alert message to a generic topic `test/devices` to which the vehicles subscribe when they become member of the edge.

```
{"message":"Ice Threat - Low',
 'myEvent':'2019-03-19 10:56:15.921834"'}
```

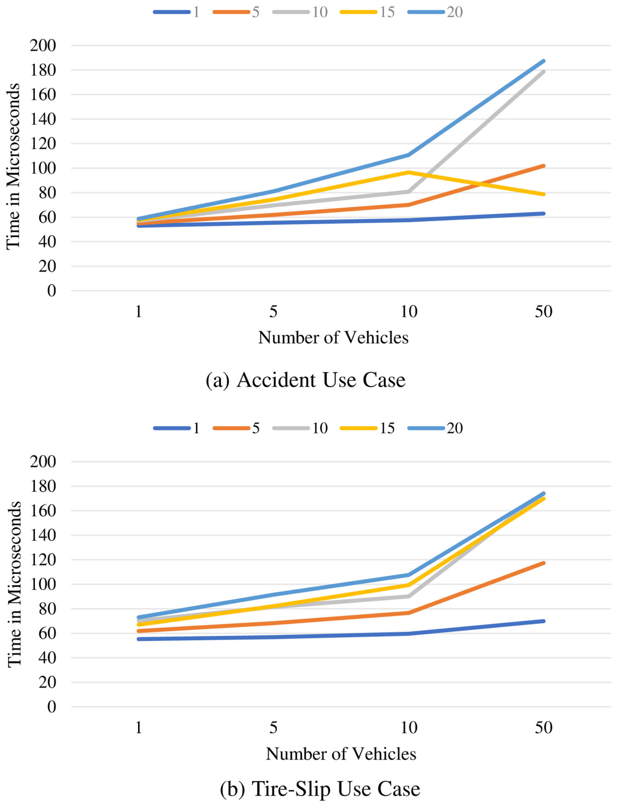
In case of accident alert following message:

```
{"message":"Accident- Require Assistance',
 'myEvent':'2019-03-19 11:27:40.237734"'}
```

is sent to topic `test/medical` and `test/police` to which nearby medical and police vehicles are subscribed respectively. Note that event time has also been added to messages, to ensure when the message is not obsolete. Similarly, for updating the rogue vehicle list from the transportation authority via central cloud to the edge infrastructures, message

```
{"Alert":myAlert, "myVehicle":myVehicle}
```

is sent to `test/Rogue-Vehicle` topic. In this message, 'myAlert' variable can be `ADD`, `DELETE` or `LIST` operation, and 'myVehicle' can hold the vehicles to be added or deleted. In case of list operation, 'myVehicle' attribute value is NULL. The complete sequence of events for the administrative and operational phase in cloudlet supported ITS is shown in Fig. 7.



(a) Accident Use Case

(b) Tire-Slip Use Case

Fig. 8. Policy evaluation time.

TABLE 3
Total Trip Time for Accident

Vehicles Msg. per Sec	1	5	10	50
1	71.72	23.53	32.45	39.85
5	18.94	79.69	78.87	69.11
10	30.73	73.73	28.57	83.89
15	18.01	22.31	30.06	∼
20	18.04	34.40	65.82	∼
Average	31.49	46.73	47.15	64.28
Standard Deviation	23.13	27.85	23.49	22.42

TABLE 4
Total Trip Time for TireSlip

Vehicles Msg. per Sec	1	5	10	50
1	47.44	56.24	89.78	55.72
5	104.23	99.27	56.76	85.26
10	43.38	44.07	51.49	∼
15	66.43	44.04	51.32	∼
20	42.76	45.74	85.40	∼
Average	60.85	57.87	66.95	70.49
Standard Deviation	26.10	23.69	19.03	20.89

5.3 Performance Metrics, Discussion, and Limitations

We evaluated the performance of our proposed AB-ITS model in AWS and provide metrics for the use cases in proof of concept. We first calculate the execution time for the proposed policy enforcer to evaluate the attribute based security polices (shown in Fig. 5) against the number of vehicles associated with a cloudlet and scaling the number of messages sent per vehicle per second. In Fig. 8a and 8b, as the number of vehicles increase (along x axis) with more messages being sent, the enforcer takes more time to evaluate the polices and impact performance. This enforced policy engine in cloudlet has the worse case execution time less than 200 microseconds, for any number of messages sent per second (from 1 to 20) by vehicles which could range from 1 to 50. In case of no-alerts, this execution time will be zero as the policies will not be evaluated. Total trip time performance of our model includes time at which vehicle generates an alert till it is received by target vehicles which includes the policy evaluation time. As shown in Table 3 and 4, the total trip time is within the permissible limits (∼100 ms [40], [41]) for most of the case scenarios. However, the trip time goes beyond the limits when 50 vehicles get associated to single edge cloudlet at one time. The variation in total trip time is due to network traffic and latency, but the average and standard deviation infer that the performance is very comparable to peer to peer ITS. The extra overhead induced by policy execution (in microseconds) is very negligible as compared to the total trip time (in milliseconds). In our approach MQTT protocol has been used, therefore, if some one does not want to use DSRC due to cost of transmitter and receiver, our approach can still work with the traditional IoT MQTT based communication based on LTE, 5G or WiFi connectivity.

We understand that there may be hundreds of vehicles during heavy traffic time, therefore, to scale the system and accommodate all vehicles we can install more cloudlets and infrastructure devices in busy areas that will reduce the number of vehicles which will get associated with single cloudlet at a time. This implementation in AWS showcases practical viability and use of fine grained polices in context of ITS, without the need to capture data points from real world traffic. It must be noted that, AWS Greengrass has limit of 200 devices per Greengrass group, which means maximum number of vehicles which can be associated can not be more than 200. We can add more cloudlets in the system which can cater to higher population of vehicles and smart entities. Some *limitations* of our approach include the infrastructure and operational cost in deployment of cloudlets (which could be multiple to remove bottleneck). It is expected that to realize ITS, city and administration will need investment from different stakeholders. Further, since messages are passed through cloudlets, authorities setting up these infrastructure may have precise approximation of location of vehicles. However, it can be mitigated using homomorphic encryption or similar privacy preserving approaches. It is also assumed that cloudlets are trusted to relay correct information. In case, cloudlets are compromised, the system can no longer guarantee security properties.

6 Summary

This research proposes a cloudlet supoorted secure V2V and V2I communication in ITS, which ensures trusted and reliable messages exchange among moving entities on road.

We introduce the novel notion of dynamic edge associations in which the smart entities get connected to different pre-installed cloudlets on road, which help them relay the BSMs and perform the needed filtering and reduces privacy concerns of the users. These cloudlets can anonymize the messages, ensure trustworthiness and ensure their relevance to entities which receive them. We also present the formal model which specifies attributes based polices for V2V and V2I communication. Several use cases of ITS have been discussed along with implementation in Amazon Web Services (AWS). Performance has been evaluated against time taken to evaluate the polices in cloudlets and the total trip time from moment message is generated till it gets received and relayed by cloudlets.

Acknowledgments

This work is supported in part by NSF Grant HRD-1736209.

References

[1] *U.S. Department of Transportation Announces up to $42 Million in Next Generation Connected Vehicle Technologies*, Accessed: Jul. 3, 2018, 2015. [Online]. Available: https://www.its.dot.gov/press/2015/ngv_tech_announcement.htm

[2] *Connected Vehicles and Your Privacy*, Accessed: Jul. 3, 2018, 2015. [Online]. Available: https://www.its.dot.gov/factsheets/pdf/Privacy_factsheet.pdf

[3] Wired, *Hackers Remotely Kill a Jeep on the Highway-With Me in It*, 2015. [Online]. Available: https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

[4] USAToday, *Chinese Group Hacks a Tesla for the Second Year in a Row*, 2017. [Online]. Available: https://www.usatoday.com/story/tech/2017/07/28/chinese-group-hacks-tesla-second-year-row/518430001/

[5] U. GAO, "Vehicle cybersecurity," *GAO-16–350*, Mar. 2016. [Online]. Available: https://www.gao.gov/assets/680/676064.pdf

[6] NHTSA, "NHTSA and vehicle cyberSecurity," *NHTSA Report*, 2016. [Online]. Available: https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/nhtsavehiclecybersecurity2016.pdf

[7] NHTSA, "Cybersecurity best practices for modern vehicles," National Highway Traffic Safety Administration's, Washington, DC, Rep. no. DOT HS 812 333, Oct. 2016.

[8] A. Elmaghraby and M. Losavio, "Cyber security challenges in smart cities: Safety, security and privacy," *J. Advanced Res.*, vol. 5, pp. 491–497, 2014.

[9] USDOT, *Securty Credential Management System (SCMS) Proof of Concept (POC)*, Accessed: Jul. 8, 2018, 2016. [Online]. Available: https://www.its.dot.gov/factsheets/pdf/CV_SCMS.pdf

[10] USDOT, *Securty Credential Management System*, Accessed: Jul. 8, 2018, 2016. [Online]. Available: https://www.its.dot.gov/resources/scms.htm

[11] X. Jin *et al.*, "A unified attribute-based access control model covering DAC, MAC and RBAC," in *Proc. IFIP Annu. Conf. Data Appl. Secur. Privacy*, 2012, pp. 41–55.

[12] V. C. Hu *et al.*, "Guide to attribute based access control (ABAC) definition and considerations," *Nat. Inst. Standards Technol. Special Pub.*, vol. 800, no. 162, 2014.

[13] M. Gupta and R. Sandhu, "The GURA_G administrative model for user and group attribute assignment," in *Proc. Int. Conf. Netw. Syst. Secur.*, 2016, pp. 318–332.

[14] V. C. Hu, D. R. Kuhn, and D. F. Ferraiolo, "Attribute-based access control," *IEEE Comput.*, vol. 48, no. 2, pp. 85–88, Feb. 2015.

[15] R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman, "Role-based access control models," *Computer*, vol. 29, no. 2, pp. 38–47, 1996.

[16] Y. Cheng, J. Park, and R. Sandhu, "Relationship-based access control for online social networks: Beyond user-to-user relationships," in *Proc. IEEE Int. Conf. Privacy, Secur. Risk Trust*, 2012, pp. 646–655.

[17] *20 Questions About Connected Vehicles*, Accessed: Aug. 10, 2018, 2018. [Online]. Available: https://www.its.dot.gov/cv_basics/cv_basics_20qs.htm

[18] J. Williams, "Danger ahead: The government's plan for vehicle-to-vehicle communication threatens privacy, security, and common sense," Accessed: Jul. 9, 2018, 2017. [Online]. Available: https://www.eff.org/deeplinks/2017/05/danger-ahead-governments-plan-vehicle-vehicle-communication-threatens-privacy

[19] B. Lattin, *Key Technical and Policy Design Challenges for Security Credential Management Systems (SCMS)*, Accessed: Jul. 9, 2018, 2017. [Online]. Available: http://itsworldcongress2017.org/wp-content/uploads/2017/11/SIS40_Bill_Lattin.pdf

[20] *Vehicle-To-Vehicle Communication Technology For Light Vehicles*, Accessed: Jul. 3, 2018, 2016.[Online]. Available: https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/v2v_pria_121216_clean.pdf

[21] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," *Comput. Netw.*, vol. 54, no. 15, pp. 2787–2805, 2010.

[22] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future Gener. Comput. Syst.*, vol. 29, no. 7, pp. 1645–1660, 2013.

[23] A. Alshehri and R. Sandhu, "Access control models for cloud-enabled Internet of Things: A proposed architecture and research agenda," in *Proc. IEEE 2nd Int. Conf. Collaboration Internet Comput.*, 2016, pp. 530–538.

[24] M. Gupta and R. Sandhu, "Authorization framework for secure cloud assisted connected cars and vehicular Internet of Things," in *Proc. 23nd ACM Symp. Access Control Models Technol.*, 2018, pp. 193–204.

[25] M. Gupta, J. Benson, F. Patwa, and R. Sandhu, "Dynamic groups and attribute-based access control for next-generation smart cars," in *Proc. 9th ACM Conf. Data Appl. Secur. Privacy*, 2019, pp. 61–72. [Online]. Available: http://doi.acm.org/10.1145/3292006.3300048

[26] Z. Lu, G. Qu, and Z. Liu, "A survey on recent advances in vehicular network security, trust, and privacy," *IEEE Trans. Intell. Transp. Syst.*, vol. 20, no. 2, pp. 760–776, Feb. 2019.

[27] I. Ali *et al.*, "Authentication and privacy schemes for vehicular ad hoc networks (VANETs): A survey," *Veh. Commun.*, vol. 16, pp. 45–61, Feb. 2019.

[28] M. N. Mejri, J. Ben-Othman, and M. Hamdi, "Survey on VANET security challenges and possible cryptographic solutions," *Veh. Commun.*, vol. 1, no. 2, pp. 53–66, 2014.

[29] Y. F. Payalan and M. A. Guvensan, "Towards next-generation vehicles featuring the vehicle intelligence," *IEEE Trans. Intell. Transp. Syst.*, vol. 21, no. 1, pp. 30–47, Jan. 2020.

[30] A. Bazzi, B. M. Masini, A. Zanella, and I. Thibault, "On the performance of IEEE 802.11p and LTE-V2V for the cooperative awareness of connected vehicles," *IEEE Trans. Veh. Technol.*, vol. 66, no. 11, pp. 10 419–10 432, Nov. 2017.

[31] M. Aladwan *et al.*, "TrustE-VC: Trustworthy evaluation framework for industrial connected vehicles in the cloud," *IEEE Trans. Ind. Inform.*, vol. 16, no. 9, pp. 6203–6213, Sep. 2020.

[32] S. Ghane, A. Jolfaei, L. Kulik, K. Ramamohanarao, and D. Puthal, "Preserving privacy in the internet of connected vehicles," *IEEE Trans. Intell. Transp. Syst.*, to be published, doi: 10.1109/TITS.2020.2964410.

[33] S. Darbha, S. Konduri, and P. R. Pagilla, "Benefits of V2V communication for autonomous and connected vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 20, no. 5, pp. 1954–1963, May 2019.

[34] U. Ahmad, H. Song, A. Bilal, M. Alazab, and A. Jolfaei, "Securing smart vehicles from relay attacks using machine learning," *J. Supercomputing*, vol. 76, pp. 2665–2682, 2020.

[35] ENISA, "Cyber security and resilience of smart cars: Good practices and recommendations," 2017, Accessed: Jan. 27, 2018. 2017. [Online]. Available: https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars

[36] E. Union, "Certificate policy for deployment and operation of european cooperative intelligent transport systems," 2017. [Online]. Available: https://ec.europa.eu/transport/sites/transport/files/c-its_certificate_policy_release_1.pdf

[37] E. Union, "Security policy & governance framework for deployment and operation of european cooperative intelligent transport systems," 2017. [Online]. Available: https://ec.europa.eu/transport/sites/transport/files/c-its_security_policy_release_1.pdf

[38] J. Harding *et al.*, "Vehicle-to-vehicle communications: Readiness of V2V technology for application," Washington, DC: National Highway Traffic Safety Administration, Rep. no. DOT HS 812 014, 2014.

[39] *Notice of Proposed Rulemaking (NPRM)- Federal Motor Vehicle Safety Standards; Vehicle-To-Vehicle Communication*, Accessed: Mar. 3, 2018, 2017. [Online]. Available: https://goo.gl/DzSYxN

[40] Q. Xu *et al.*, "Vehicle-to-vehicle safety messaging in DSRC," in *Proc. 1st ACM Int. Workshop Veh. Ad Hoc Netw.*, 2004, pp. 19–28.

[41] Z. Xu *et al.*, "DSRC versus 4G-LTE for connected vehicle applications: A study on field experiments of vehicular communication performance," *J. Advanced Transp.*, vol. 435, p. 10, 2017.

[42] *Basic Safety Message*, Accessed: Aug. 10, 2018, 2018. [Online]. Available: https://www.its.dot.gov/cv_basics/cv_basics_how_used.htm

Maanak Gupta received the BTech degree in computer science and engineering from Kuruskhetra University, India, the MS degree in information systems from Northeastern University, Boston, Massachusetts, and the MS and PhD degrees in computer science from the University of Texas at San Antonio (UTSA), San Antonio, Texas. He is currently an assistant professor in computer science at Tennessee Technological University, Cookeville, Tennessee. He has also worked as a postdoctoral fellow at the Institute for Cyber Security (ICS) at UTSA. His primary area of research includes security and privacy in cyber space focused in studying foundational aspects of access control and their application in technologies including cyber physical systems, cloud computing, IoT and Big data. He has worked in developing novel security mechanisms, models and architectures for next generation smart cars, smart cities, intelligent transportation systems and smart farming.

James Benson received the BSc and MSc physics degrees from Clarkson University, Potsdam, New York, in 2007 and 2009 respectively, and the MSc degree in electrical engineering from the University of Texas at San Antonio (UTSA), San Antonio, Texas, in 2016. He has worked at the Texas Renewable Energy Institute (TSERI) and Open Cloud Institute (OCI) at UTSA assisting with data analytics and various research projects. He is currently working as a Technology Research Analyst II with the Institute for Cyber Security (ICS) and the Center for Security and Privacy Enhanced Cloud Computing (C-SPECC) at UTSA. His research interests include cyber physical systems, cloud computing, and automation.

Farhan Patwa received the BSc and MSc degrees in electrical engineering from the University of Texas at Arlington, Arlington, Texas. He is a systems engineer with more than 20 years of professional experience working in the telecom industry, cloud computing and software security solutions. He has worked for Nortel and Ericsson leading projects for high capacity test of their 3G and 4G wireless telecom products. He currently works for Wind River Systems, designing embedded security solutions. He also works part-time as an associate director and chief architect at the Institute for Cyber Security, University of Texas at San Antonio, San Antonio, Texas.

Ravi Sandhu (Fellow, IEEE) is currently the founding executive director and chief scientist at the Institute for Cyber Security, University of Texas at San Antonio, San Antonio, Texas, where he holds the Lutcher Brown Endowed chair in Cyber Security. He is a fellow of the ACM and AAAS and an inventor on 30 patents. He was the past editor-in-chief of the *IEEE Transactions on Dependable and Secure Computing*, past founding editor-in-chief of the *ACM Transactions on Information and System Security* and a past chair of ACM SIGSAC. He founded ACM CCS, SACMAT and CODASPY, and has been a leader in numerous other security conferences. His research has focused on security models and architectures, including the seminal role-based access control model. His papers have accumulated more than 40,000 Google Scholar citations, including more than 9,000 citations for the RBAC96 paper. He is a fellow of the ACM, IEEE, and AAAS and an inventor on 30 patents.