# ART: An Attack-Resistant Trust Management Scheme for Securing Vehicular Ad Hoc Networks

tej memane

# ART: An Attack-Resistant Trust Management Scheme for Securing Vehicular Ad Hoc Networks

Wenjia Li, *Member, IEEE*, and Houbing Song, *Senior Member, IEEE*

***Abstract*—Vehicular ad hoc networks (VANETs) have the potential to transform the way people travel through the creation of a safe interoperable wireless communications network that includes cars, buses, traffic signals, cell phones, and other devices. However, VANETs are vulnerable to security threats due to increasing reliance on communication, computing, and control technologies. The unique security and privacy challenges posed by VANETs include integrity (data trust), confidentiality, nonrepudiation, access control, real-time operational constraints/demands, availability, and privacy protection. The trustworthiness of VANETs could be improved by addressing holistically both data trust, which is defined as the assessment of whether or not and to what extent the reported traffic data are trustworthy, and node trust, which is defined as how trustworthy the nodes in VANETs are. In this paper, an attack-resistant trust management scheme (ART) is proposed for VANETs that is able to detect and cope with malicious attacks and also evaluate the trustworthiness of both data and mobile nodes in VANETs. Specially, data trust is evaluated based on the data sensed and collected from multiple vehicles; node trust is assessed in two dimensions, i.e., functional trust and recommendation trust, which indicate how likely a node can fulfill its functionality and how trustworthy the recommendations from a node for other nodes will be, respectively. The effectiveness and efficiency of the proposed ART scheme is validated through extensive experiments. The proposed trust management theme is applicable to a wide range of VANET applications to improve traffic safety, mobility, and environmental protection with enhanced trustworthiness.**

***Index Terms*—Vehicular ad hoc networks (VANETs), trust management, security, misbehavior detection.**

## I. Introduction

In recent years, the growing needs for increased safety and efficiency of road transportation system have promoted automobile manufacturers to integrate wireless communications and networking into vehicles. The wirelessly networked vehicles naturally form Vehicular Ad-hoc Networks (VANETs), in which vehicles cooperate to relay various data messages through multi-hop paths, without the need of centralized administration. VANETs have the potential to transform the way people travel through the creation of a safe, interoperable wireless communications network.

Manuscript received May 30, 2015; revised October 3, 2015; accepted October 8, 2015. Date of publication November 12, 2015; date of current version March 25, 2016. The Associate Editor for this paper was C. Olaverri-Monreal.

W. Li is with the Department of Computer Science, New York Institute of Technology, New York, NY 10023 USA (e-mail: wli20@nyit.edu).

H. Song is with the Department of Electrical and Computer Engineering, West Virginia University, Montgomery, WV 25136 USA (e-mail: Houbing.Song@mail.wvu.edu).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

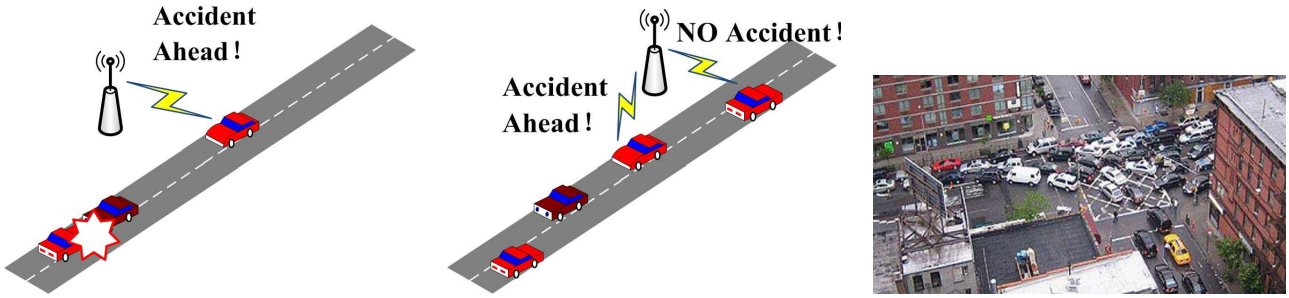
Digital Object Identifier 10.1109/TITS.2015.2494017

In VANETs, various nodes, such as vehicles and Roadside Units (RSUs), are generally equipped with sensing, processing, and wireless communication capabilities. Both Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communications enable safety applications that provide warnings regarding road accidents, traffic conditions (e.g., congestion, emergency braking, icy road) and other relevant transportation events. However, VANETs are vulnerable to threats due to increasing reliance on communication, computing and control technologies. The unique security and privacy challenges posed by VANETs include integrity (data trust), confidentiality, nonrepudiation, access control, real-time operational constraints/demands, availability, and privacy protection [1]–[5].

One typical application of VANETs is the Traffic Estimation and Prediction System (TrEPS), which generally provides the predictive information needed for proactive traffic control and traveler information [6]. TrEPS will facilitate and enhance planning analysis, operational evaluation, and real-time advanced transportation systems operation. For example, TrEPS can provide input to traffic managers who decide where and when to post specific messages on variable message signs, such as ***AVOID CONGESTION—EXIT HERE FOR ALTERNATE ROUTE***.

To help TrEPS more accurately evaluate the current traffic conditions and better make predictions, multiple emerging information sources have been taken into consideration, such as real-time location sensor data collected and transmitted by Android smartphones or Apple iPhone [7], community-based traffic and road condition reporting service based on crowd sensing [8], etc. All these emerging information sources need networking support, such as VANETs, to efficiently share and disseminate the collected traffic information. However, sometimes the TrEPS may encounter confusing or even conflicting traffic information reported by multiple sources, which is demonstrated in Fig. 1.

From Fig. 1(a), we find that the sensor in a vehicle detects an accident ahead, and then it reports this accident to the system. Therefore, the traffic alert shown in Fig. 1(a) is true. In contrast, Fig. 1(b) shows two conflicting traffic alerts. Given that there is no accident in this scenario, the vehicle that reports accident to the system is either *faulty* or *malicious*. If the trustworthiness of the sensor data cannot be properly evaluated, then it is possible to produce traffic jams or even life-threatening road accidents because most of the vehicles will be *incorrectly* redirected to the same route if the fake traffic alerts remain undetected and thus effective in VANETs, as is shown in Fig. 1(c). Therefore, it is important to secure VANETs so that they can better support intelligent transportation applications such as TrEPS.




(a) (b) (c)

Fig. 1. True alerts vs. false alerts in VANETs for traffic monitoring. (a) True traffic alert. (b) Conflicting traffic alerts. (c) Outcome of false traffic alerts.

When compared with the traditional wired networks, VANETs themselves are more vulnerable to malicious attacks because of their unique features, such as highly dynamic network topology, limited power supply and error-prone transmission media. For instance, the wireless communication links among vehicles are prone to both passive eavesdropping and active tampering. Moreover, there are other types of more sophisticated attacks that are difficult to detect [5], [9]–[11].

Thus, it is critical to detect and cope with malicious attacks in VANETs so that the safety of vehicles, drivers, and passengers as well as the efficiency of the transportation system can be better guaranteed. We believe that the trustworthiness of VANETs could be improved by addressing both data trust and node trust holistically.

In this paper, an attack-resistant trust management scheme called *ART* is proposed to cope with malicious attacks and evaluate the trustworthiness of data as well as nodes in VANETs. In the ART scheme, we model and evaluate the trustworthiness of data and node as two separate metrics, namely *data trust* and *node trust*, respectively. In particular, *data trust* is used to assess whether or not and to what extent the reported traffic data are trustworthy. On the other hand, *node trust* indicates how trustworthy the nodes in VANETs are. Moreover, the ART scheme can detect malicious nodes in VANETs. To evaluate the performance of the proposed ART scheme, extensive experiments have been conducted. Experimental results show that the proposed ART scheme is able to accurately evaluate the trustworthiness of data and nodes in VANETs, and it is also resistant to various malicious attacks.

In summary, the major contributions of this work are listed as follows.

- First, an attack-resistant trust management scheme is studied in this paper, which can effectively detect and cope with different types of malicious behaviors in VANETs.
- Second, the trustworthiness of traffic data (*data trust*) is evaluated based on the data sensed and collected from multiple vehicles.
- Third, the trustworthiness of vehicle nodes is assessed in two dimensions. In other words, a vector that is composed of two elements is used to describe the trustworthiness of each node. The two dimensions of *node trust* are *functional trust* and *recommendation trust*, which indicate how likely a node can fulfill its functionality and how trustworthy the recommendations from a node for other nodes will be, respectively.
- Finally, extensive experiments have been conducted, and experimental results show that the proposed ART scheme can effectively evaluate the trustworthiness of both sensed data and mobile nodes in VANETs.

The rest of this paper is organized as follows. In Section II, the related work on misbehavior detection and trust management is reviewed. Section III describes the basics of the research problem in details. In Section IV, the ART scheme is described in details. Section V presents the experimental study that has been conducted. Finally, the conclusion is drawn in Section VI.

## II. Related Work

In recent years, there has been significant research interest in the topics of misbehavior detection as well as trust management for ad hoc networks.

### A. Misbehavior Detection for Ad hoc Networks

Note that the term *misbehavior* generally refers to abnormal behavior that deviates from the set of behaviors that each node is supposed to conduct in ad hoc networks [12]. According to [13], there are four types of misbehaviors in ad hoc networks, namely failed node behaviors, badly failed node behaviors, selfish attacks, and malicious attacks. These four types of node misbehaviors are classified with respect to the node's intent and action. More specifically, selfish attacks are intentional passive misbehaviors, where nodes choose not to fully participate in the packet forwarding functionality to conserve their resources, such as battery power; malicious attacks are intentional active misbehaviors, where the malicious node aims to purposely interrupt network operations. The existence of selfishness and malicious behaviors has remarkably motivated research in the area of misbehavior detection for mobile ad hoc networks (MANETs).

Alternatively, there have been some attacks which primarily focus on the data that are transmitted and shared among nodes in ad hoc networks. Thus, another goal of misbehavior detection approaches is to ensure that data has not been modified in transit, that is, they should make sure that what was sent is the same as what was received. More specifically, some of the widely-studied data trust attacks are masquerading attack, replay attack, message tampering attack, hidden vehicle attack, and illusion attack [14]–[16].

Intrusion Detection System (IDS) is normally regarded as an important solution for detecting various node misbehaviors in ad hoc networks. Several approaches have been proposed to build IDS probes on eac individual peer due to the lack of a fixed infrastructure, such as [17]–[19]. In these approaches, there is one IDS probe installed on each node, and each IDS probe is assumed to be always monitoring the network traffic, which is obviously not energy efficient given the limited battery power that each node has in MANETs. In contrast, Huang *et al.* [20] proposed a cooperative intrusion detection framework in which clusters are formed and the nodes in each cluster fulfill the intrusion detection task in turn. This cluster-based approach can noticeably reduce the power consumption for each node.

Routing misbehaviors are another major security threats that have been extensively studied in ad hoc networks. In addition to externally intruding into ad hoc networks, an adversary may also choose to compromise some nodes in ad hoc networks, and make use of them to disturb the routing services so as to make part of or the entire network unreachable. Marti *et al.* [21] introduced two related techniques, namely *watchdog* and *pathrater*, to detect and isolate misbehaving nodes, which are nodes that do not forward packets. There are also some other solutions that aim to cope with various routing misbehaviors [22]–[24].

### B. Trust Establishment and Management in Ad hoc Networks

The main purpose of trust management is to assess various behaviors of other nodes and build a reputation for each node based on the behavior assessment. The reputation can be utilized to determine trustworthiness for other nodes, make choices on which nodes to cooperate with, and even take action to punish an untrustworthy node if necessary.

In general, the trust management system usually relies on two sorts of observations to evaluate the node behaviors. The first kind of observation is named as *first-hand* observation, or in other words, direct observation [25]. First-hand observation is the observation that is directly made by the node itself, and the first-hand observation can be collected either passively or actively. If a node promiscuously observes its neighbors' actions, the local information is collected passively. In contrast, the reputation management system can also rely on some explicit evidences to assess the neighbor behaviors, such as an acknowledgement packet during the route discovery process. The other kind of observation is called *second-hand* observation or indirect observation. Second-hand observation is generally obtained by exchanging first-hand observations with other nodes in the network. The main disadvantages of second-hand observations are related to overhead, false report and collusion [26], [27].

In [28], Buchegger *et al.* proposed a protocol, namely CONFIDANT (Cooperation Of Nodes, Fairness In Dynamic Ad-hoc NeTworks), to encourage the node cooperation and punish misbehaving nodes. CONFIDANT has four components in each node: a Monitor, a Reputation System, a Trust Manager, and a Path Manager. The Monitor is used to observe and identify abnormal routing behaviors. The Reputation System calculates the reputation for each node in accordance with its observed behaviors. The Trust Manager exchanges alerts with other trust managers regarding node misbehaviors. The Path Manager maintains path rankings, and properly responses to various routing messages. A possible drawback of CONFIDANT is that an attacker may intentionally spread false alerts to other nodes that a node is misbehaving while it is actually a well-behaved node. Therefore, it is important for a node in CONFIDANT to validate an alert it receives before it accepts the alert.

Michiardi *et al.* [29] presented a mechanism called CORE to identify selfish nodes, and then compel them to cooperate in the following routing activities. Similar to CONFIDANT, CORE uses both a surveillance system and a reputation system to observe and evaluate node behaviors. Nevertheless, while CONFIDANT allows nodes exchange both positive and negative observations of their neighbors, only positive observations are exchanged amongst the nodes in CORE. In this way, malicious nodes cannot spread fake charges to frame the well-behaved nodes, and consequently avoid denial of service (DoS) attacks toward the well-behaved nodes. The reputation system maintains reputations for each node, and the reputations are adjusted upon receiving of new evidences. Since selfish nodes reject to cooperate in some cases, their reputations are lower than other nodes. To encourage node cooperation and punish selfishness, if a node with low reputation sends a routing request, then the request will be ignored and the bad reputation node cannot use the network.

Patwardhan *et al.* [30] studied an approach in which the reputation of a node is determined by data validation. In this approach, a few nodes, which are named as Anchor nodes here, are assumed to be pre-authenticated, and thus the data they provide are regarded as trustworthy. Data can be validated by either agreement among peers or direct communication with an anchor node. Malicious node can be identified if the data they present is invalidated by the validation algorithm.

In addition, there have been some other research efforts that aim to enhance the security, trust and privacy of VANETs [31]–[37].

Most of the existing trust management methods for ad hoc networks focus on assessing the trustworthiness of mobile nodes by collecting various evidences and analyzing the prior behavioral history of the nodes. However, little attention has been paid to evaluate the trustworthiness of the data shared among these nodes as well. Given that the data reliability and trustworthiness in transportation systems are extremely important as well, we aim to evaluate the trustworthiness of both mobile nodes and data in this work.

## III. Problem Definition

In this section, the research problem that is addressed in this paper will be described in more details, including the network model as well as the adversary model.

### A. Network Model

A VANET generally refers to a wireless network of heterogeneous sensors or other computing devices that are deployed in vehicles. This type of network enables continuous monitoring and sharing of road conditions and status of the transportation systems.

All of the nodes in VANETs are equipped with the same wireless communication interface, such as IEEE 802.11p. The nodes are limited in energy as well as computational and storage capabilities.

### B. Adversary Model

First of all, the RSUs are assumed to be trustworthy since they are usually better protected. The connected vehicles, on the other hand, are generally more susceptible to various attacks, and they can be compromised at any time after the VANET is formed.

The adversary can be an outsider located in the wireless range of the vehicles, or the adversary can first compromise one or more vehicles and behave as an insider later. The adversary is able to eavesdrop, jam, modify, forge, or drop the wireless communication between any devices in range. The main goals of the adversary may include intercepting the normal data transmission, forging or modifying data, framing the benign devices by deliberately submitting fake recommendations, etc. More specifically, the following malicious attacks are considered in this paper.

- Simple Attack (SA): An attacker may manipulate the compromised nodes not to follow normal network protocols and not to provide necessary services for other nodes, such as forwarding data packets or propagating route discovery requests. However, the compromised node will not provide any fake trust opinions when it is asked about other node's trustworthiness.
- Bad Mouth Attack (BMA): In addition to conduct simple attack, the attacker can also spread fake trust opinions and try to frame the benign nodes so that the truly malicious nodes can remain undetected. This attack aims to disrupt the accurate trust evaluation and make it harder to successfully identify the malicious attackers.
- Zigzag (On-and-off) Attack (ZA): Sometimes sly attackers can alter their malicious behavior patterns so that it is even harder for the trust management scheme to detect them. For instance, they can conduct malicious behaviors for some time and then stop for a while (in that case the malicious behaviors are conducted in an on-and-off manner). In addition, the sly attackers can also exhibit different behaviors to different audiences, which can lead to inconsistent trust opinions to the same node among different audiences. Due to the insufficient evidence to accuse the malicious attacker, it is generally more difficult to identify such sly attackers.

## IV. The Attack-Resistant Trust Management Scheme (ART) for VANETs

In this section, the proposed ART scheme is presented in details. The ART scheme addresses two types of trustworthiness in VANETs: *data trust* and *node trust*.

### A. Preliminaries

In general, the *trustworthiness* of a node $N_k$ can be defined as a vector $\Theta_k = (\theta_k^{(1)}, \theta_k^{(2)}, \ldots, \theta_k^{(n)})$, in which $\theta_k^{(i)}$ stands for the $i$-th dimension of the trustworthiness for the node $N_k$. Each dimension of the trustworthiness $\theta_k^{(i)}$ corresponds to one or a certain category of behavior(s) $B_k^{(i)}$ (such as packet forwarding or true recommendation sharing), and $\theta_k^{(i)}$ can properly reflect the probability with which the node will conduct $B_k^{(i)}$ in an appropriate manner. $\theta_k^{(i)}$ can be assigned any real value in the range of [0,1], i.e., $\forall\, i \in \{1, 2, \ldots, n\}$, $\theta_k^{(i)} \in [0, 1]$. The higher the value of $\theta_k^{(i)}$, the node $N_k$ is more likely to conduct $B_k^{(i)}$ properly.

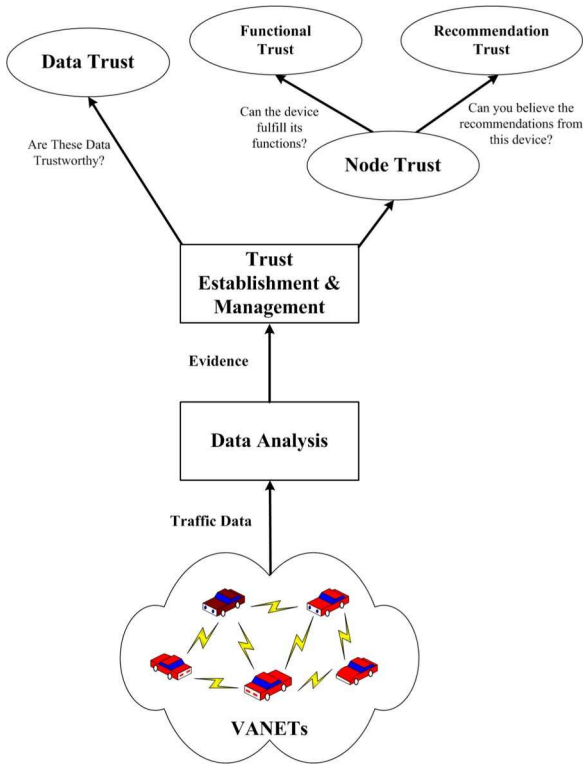



Fig. 2. Overview of the ART scheme.

Each dimension of the trustworthiness $\theta_k^{(i)}$ for the node $N_k$ is defined as a function of the misbehaviors $M_k^{(i)}$ that are related to $B_k^{(i)}$ and have been observed by the neighbors of the device $N_k$. Different dimensions of the trustworthiness may correspond to different functions, and the selection of different functions should coincide with the basic features of $M_k^{(i)}$, such as severity of the outcome, occurrence frequency, and context in which they occur.

In particular, the trustworthiness of a device is represented in a vector $\Theta_k = (\theta_k^{(1)}, \theta_k^{(2)})$, and each element in the vector stands for *functional trust* and *recommendation trust*, respectively. In the future, if it is necessary to introduce new element to the trust vector, the new element can be added easily.

### B. Scheme Overview

The ART scheme is composed of two phases, namely *data analysis* and *trust management*. The schematic diagram of the ART scheme is depicted in Fig. 2.

In the ART scheme, we first collect traffic data from VANETs for data analysis. Second, we summarize the findings from the data analysis as evidences for trust management schemes to evaluate the trustworthiness. The details of the evidence combination are presented in Section IV-C. Then these evidences will be used to assess the trustworthiness of data and nodes. The trustworthiness of nodes further consists of functional trust and recommendation trust. The details of the evaluation of trust recommendation using collaborative filtering are provided in Section IV-D.

### C. Evidence Combination

Evidence combination is very important for the proposed ART scheme. Because some of the traffic data are not reliable, it is critical to find an evidence combination technique to properly fuse together multiple pieces of evidence in presence of both trustworthy and untrustworthy data. Thus, it is necessary to combine multiple pieces of evidences so that both data trust and functional trust can be properly evaluated.

In this work, Dempster–Shafer theory of evidence (DST) [38] is used to fuse together multiple piece of evidences even if some of them might not be accurate. In DST, probability is replaced by an uncertainty interval bounded by belief $(bel)$ and plausibility $(pls)$. Belief is the lower bound of this interval and represents supporting evidence. Plausibility is the upper bound of the interval and represents non-refuting evidence. For instance, if a node $N_k$ observes that one of its neighbors, say node $N_j$, has dropped packets with probability $p$, then node $N_k$ has $p$ degree of belief in the packet dropping behavior of node $N_j$ and 0 degree of belief in its absence. The belief value with respect to an event $\alpha_i$ and observed by node $N_k$ can be computed as the following.

$$bel_{N_k}(\alpha_i) = \sum_{e:\alpha_e \in \alpha_i} m_{N_k}(\alpha_e). \tag{1}$$

Here $\alpha_e$ are all the basic events that compose the event $\alpha_i$, and $m_{N_k}(\alpha_e)$ stands for the view of the event $\alpha_e$ by node $N_k$. In this case, since node $N_k$ merely get one single report of node $N_j$ from itself, i.e., $\alpha_i \subset \alpha_i$. Therefore, we can derive that $bel_{N_k}(\alpha_i) = m_{N_k}(\alpha_i)$. Note that $\bar{\alpha_i}$ denotes the non-occurrence of the event $\alpha_i$. Since the equation $pls(\alpha_i) = 1 - bel(\bar{\alpha_i})$ holds for belief and plausibility, we can further derive the following: $bel_{N_k}(N_j) = m_{N_k}(N_j) = p$ and $pls_{N_k}(N_j) = 1 - bel_{N_k}(\bar{N_j}) = 1 - p$.

Given that belief indicates the lower bound of the uncertainty interval and represents supportive evidence, we define the combined packet dropping level of node $N_j$ as the following.

$$pd_{N_j} = bel(N_j) = m(N_j) = \bigoplus_{k=1}^{K} m_{N_k}(N_j). \tag{2}$$

Here $m_{N_k}(N_j)$ denotes the view of node $N_k$ on another node $N_j$. We can combine reports from different nodes by applying the Dempster's rule, which is defined as following.

$$m_1(N_j) \bigoplus m_2(N_j) = \frac{\sum_{q,r:\alpha_q \cap \alpha_r = N_j} m_1(\alpha_q) m_2(\alpha_r)}{1 - \sum_{q,r:\alpha_q \cap \alpha_r = \Phi} m_1(\alpha_q) m_2(\alpha_r)}. \tag{3}$$

More specifically, we use the Dempster's rule to combine the local evidences collected by a mobile node itself and the external evidences shared by other mobile nodes. The DST-based evidence combination algorithm is shown in Algorithm 1. Note that $n_i$ stands for the $i$-th node in VANET. $V_i$ denotes the initial evidence that is collected by $n_i$, and $V_i'$ denotes the updated evidence that is possessed by $n_i$.

**Algorithm 1** Update of Local Evidence for node $i$ Using the Dempster–Shafer Theory (DST)

**Input of** $n_i : V_i$
**Output of** $n_i : V_i'$
**Upon reception of** $V_k$ from node $n_k$:
**if** $V_i \neq V_k$ **then**

1) merge $V_i$ and $V_k$ according to the following rules:
   - if node $m$ is in **BOTH** $V_i$ **AND** $V_k$, then calculate the updated value $U_i$ of the corresponding columns for node $m$ in BOTH $V_i$ and $V_k$ using the Dempster's rule of combination, and store $U_i$ to an intermediate list $TEMP_i$ as an entry.
   - if node $m$ is in **EITHER** $V_i$ **OR** $V_j$, but **NOT BOTH**, then add a virtual entry of node $m$ to the view that previously does not contain $m$, and set all the columns of this virtual entry as 0. Then calculate the updated value $U_i$ of the corresponding columns for node $m$ in BOTH $V_i$ and $V_k$ using the Dempster's rule of combination, and store $U_i$ to an intermediate list $TEMP_i$ as an entry.
2) calculate the top $k$ outliers from $TEMP_i$, and assign these $k$ top outliers to $V_i'$.
3) broadcast $V_i'$ to all of its immediate neighbors (i.e., number of hop $= 1$).

**else** keep $V_i$ unchanged, and do not send any message out.
**end if**

### D. Evaluation of Trust Recommendations Using Collaborative Filtering

It is well understood that it is not always feasible for two vehicle nodes to communicate directly with each other in VANETs. In this case, it is essential for one vehicle node to relay data for others. However, sometimes a node may refuse to relay data either because of its limited battery power or other resources, or the node may have been compromised by adversaries. Therefore, it is critical to know whether or not another vehicle is trustworthy to interact with. If a vehicle has never interacted with others before, then the trust recommendations that it receives from others become the only data that it can rely on to evaluate the trustworthiness of other nodes.

Suppose that $N = [N_1, N_2, \ldots, N_q]$ denotes the set of $q$ nodes in the VANETs. The vector $V_A = [\bar{v}_{A_1}, \bar{v}_{A_2}, \ldots, \bar{v}_{A_q}]$ denotes the recommendation trust ratings that node $A$ makes for each $N_i$ in $N$. Similarly, the recommendation trust ratings that node $B$ keeps for each node can be denoted as $V_B = [\bar{v}_{B_1}, \bar{v}_{B_2}, \ldots, \bar{v}_{B_q}]$. The credibility of recommendations of node B can be computed

by the similarity of the trust rating information between node A and Node B. In this paper, the Cosine-based similarity metric is used to measure how similar the two vectors are [39].

More specifically, the trust ratings of every node are viewed as a vector in the $k$ dimensional space. If a node does not evaluate a node, then the default rating is used. The similarity between two nodes is measured by computing the cosine of the angle between these two vectors. Formally, in the ratings matrix, similarity between nodes i and j, denoted by $\cos(i,j)$ is given by the following, in which "•" stands for the dot product of two vectors.

$$\cos(\vec{i}, \vec{j}) = \frac{\vec{i} \bullet \vec{j}}{\| \vec{i} \| * \| \vec{j} \|}. \tag{4}$$

In this paper, the user-based collaborative filtering is used to help determine the recommendation trust of other nodes [40], [41]. More specifically, the value of the unknown trust rating $r_{A,B}$ for node $A$ and another node $B$ is usually computed as an aggregate of the ratings of some other (usually, the $K$ most similar) users for the same node $B$, which is shown as follows.

$$r_{A,B} = aggr_{N_i \in \hat{N}} r_{N_i,B} \tag{5}$$

where $\hat{N}$ denotes the set of nodes that possess most similar recommendation trust ratings to node $A$ and that have interacted with node $B$ before and have consequently obtained knowledge regarding the trustworthiness of node $B$.

In other words, nodes which have similar trust preferences on some nodes may also have similar preferences on others. Thus, this method provides recommendations or predictions to the target node based on the opinions of other like-minded nodes.

In particular, the recommendation trust is determined using the following steps.

- *Trust rating formation*: in this stage, the trust ratings of each node $N_i$ for other node $N_j$ are formed as a $q \times q$ matrix $R$.
- *Trusted neighbor selection*: in this stage, all the similarities between nodes in the model are computed, and the top $K$ most similar nodes are selected. Note that the functional trust of each selected node will also be inspected to make sure that only recommendations from the nodes which can fulfill their tasks as expected will be trusted.
- *Predicted trust calculation*: in this stage, the predicted trust rating of node $i$ on node $k$, $T_{ik}$, is calculated. Let $S_i$ be the set of most similar nodes for node $i$. $\bar{R}_i = \sum_k R_{i,k}$ and $\bar{R}_j = \sum_k R_{j,k}$ stand for the overall trust ratings of node $i$ and node $j$, respectively. Based on Resnick's standard prediction formula [42], $T_{ik}$ is calculated as follows.

$$T_{ik} = \bar{R}_i + \frac{\sum_{j \in S_i} \cos(i,j) * (R_{j,k} - \bar{R}_j)}{\sum_{j \in S_i} |\cos(i,j)|}. \tag{6}$$

## V. Performance Evaluation

In this section, the performance of the proposed ART scheme is evaluated and the experimental results are presented.

TABLE I
Simulation Parameters

| $Parameter$ | $Value$ |
|---|---|
| Simulation area | $600m \times 600m$ |
| Num. of nodes | 50, 100, 200 |
| Transmission range | $120m$ |
| Node placement | *Random* |
| Num. of malicious nodes | 5, 10, 15, 20, 25, 30, 35, 40 |
| Node Motion Speed | 5m/s, 10m/s, 20m/s |
| Simulation time | 900s |

We use GloMoSim 2.03 [43] as the simulation platform, and Table I lists the parameters used in the simulation scenarios. we use the weighted voting method as the Baseline method when we evaluate the performance of the ART scheme, because the weighted voting method has been extensively used in many previous trust management schemes for wireless networks, such as [28], [44], [45].

We use the following two parameters to evaluate the accuracy of the ART scheme: Precision (P) and Recall (R), which are both widely used in machine learning and information retrieval to assess the accuracy [46]. In this paper, we use both P and R values to evaluate how accurate the proposed ART scheme is when it is used to identify untrustworthy nodes in VANETs. These two parameters are defined as follows.

$$P = \frac{\text{Num of Truly Malicious Nodes Caught}}{\text{Total Num of Untrustworthy Nodes Caught}} \tag{7}$$

$$R = \frac{\text{Num of Truly Malicious Nodes Caught}}{\text{Total Num of Truly Malicious Nodes}}. \tag{8}$$

Each simulation scenario has 30 runs with different random seeds, which ensure a unique initial node placement for each run. Each experimental result is the average over the 30 runs for each simulation scenario. The simulation results are shown in Figs. 3–5.

Fig. 3(a) shows that the ART scheme always achieves a higher precision score than the baseline method when the node density varies. Moreover, when the node density is higher, both methods yield a better precision. This is true because it is more likely to receive true data from others when there are a higher number of well-behaved nodes. Similarly, Fig. 3(b) shows that the ART scheme also outperforms the baseline method in terms of recall. Also, the recall value is higher when the node density is higher. From Fig. 3(c), it is obvious that the ART scheme introduces similar communication overhead as the baseline method does, which indicates that the proposed ART scheme is cost-effective in terms of the communication overhead. For instance, when there are 50 nodes in the network, both ART and baseline approach introduce around 6% of communication overhead. On the other hand, ART will introduce around 8% of communication overhead when there are 200 nodes, whereas the baseline approach introduces almost 10%.

Fig. 4(a) and (b) depicts the precision and recall values for the ART scheme and the baseline method with different percentages of malicious nodes. We find that both the precision and recall values decrease when there are a higher percentage of malicious nodes, which is pretty obvious. In addition, the ART scheme is able to produce a better performance than the

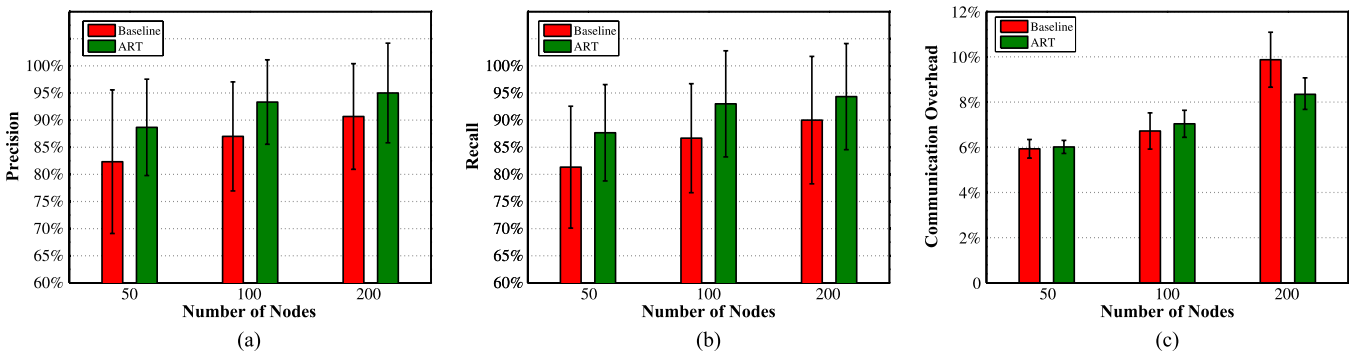



Fig. 3. Effect of node density on ART and baseline. (a) Precision of ART vs. baseline. (b) Recall of ART vs. baseline. (c) Comm. overhead of ART vs. baseline.

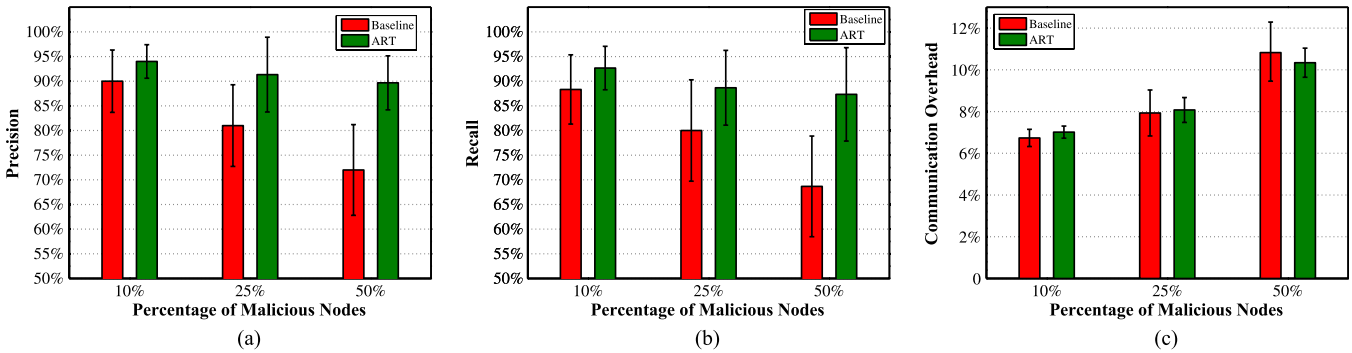



Fig. 4. Effect of adversary percentage on ART and baseline. (a) Precision of ART vs. baseline. (b) Recall of ART vs. baseline. (c) Comm. overhead of ART vs. baseline.

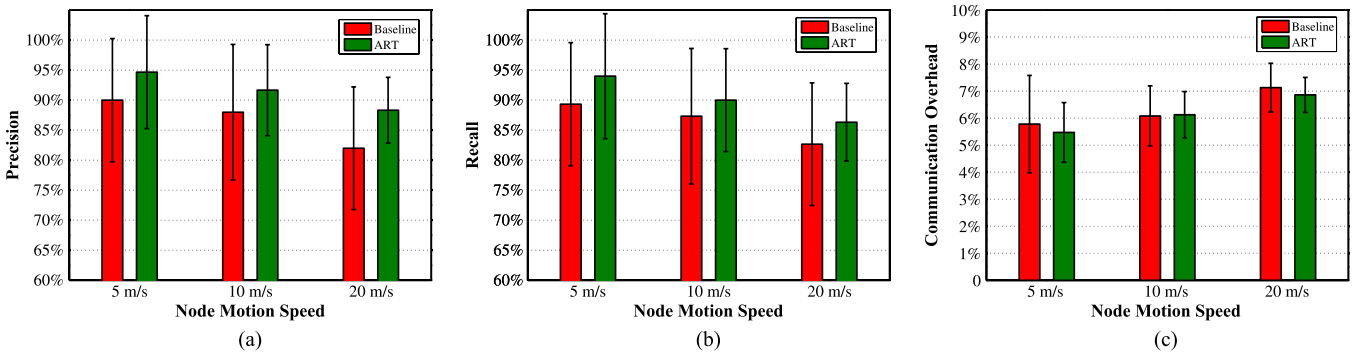



Fig. 5. Effect of node mobility on ART and baseline. (a) Precision of ART vs. baseline. (b) Recall of ART vs. baseline. (c) Comm. overhead of ART vs. baseline.

baseline method in terms of both precision and recall values. In terms of communication overhead, Fig. 4(c) shows that the ART scheme does not incur extra communication overhead compared to the baseline when the percentage of malicious nodes varies.

Fig. 5 illustrates the performance of the ART when the nodes move at different speeds. We find from Fig. 5 that the ART scheme always outperforms the baseline algorithm, and both of them will introduce a slightly higher communication overhead when the vehicles are moving faster. In addition, the precision and recall values are lower when the vehicles are moving faster. This is true because when the vehicles are moving faster, it is generally more difficult for the information regarding the untrustworthy vehicles to propagate. Thus, it is expected to take more rounds of communication to disseminate the information.

In addition to the first set of experiments which aim to evaluate the overall performance of the proposed ART scheme under difference network parameters, we are also particularly interested in knowing how well the ART scheme is resistant to different attack patterns, such as SA, BMA, and ZA as described in Section III-B. Therefore, we also conduct some other experiments for ART, launching different types of malicious attacks and observing the performance of the ART scheme with these attack patterns. Table II summarizes the specific attack patterns that have been used in the experiments. The experiment results are depicted in Figs. 6–8, respectively.

TABLE II
ATTACK PATTERNS IN THE EXPERIMENTS

| Attack Pattern | Behavior | Opinion |
|---|---|---|
| SA | misbehaving with prob. 0.5 | honestly sharing trust opinions with others |
| BMA | misbehaving with prob. 0.5 | sharing opposite trust opinions with prob. 0.5 |
| ZA | misbehaving with prob. 0.5 to half of nodes behaving normally to the other half of nodes | honestly sharing trust opinions with half of nodes sharing opposite trust opinions with the other half with prob. 0.5 |

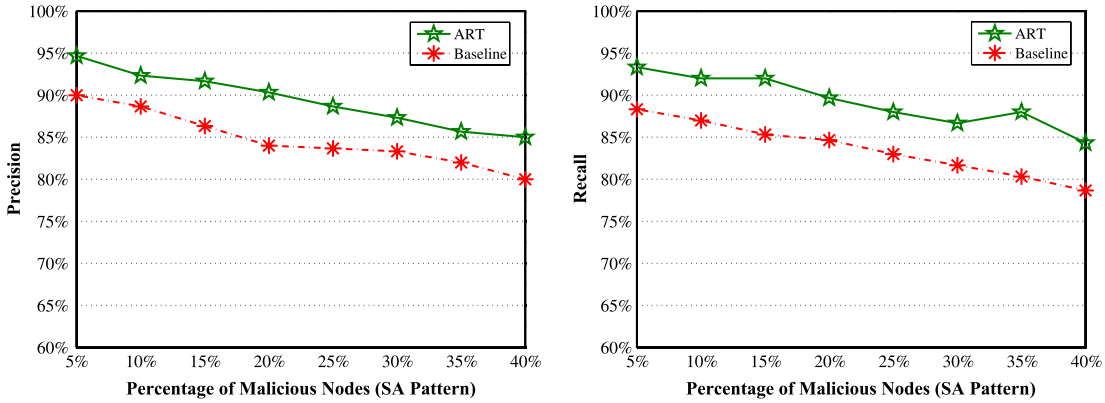



Fig. 6. ART vs. baseline under SA pattern. (a) Precision of ART vs. baseline. (b) Recall of ART vs. baseline.

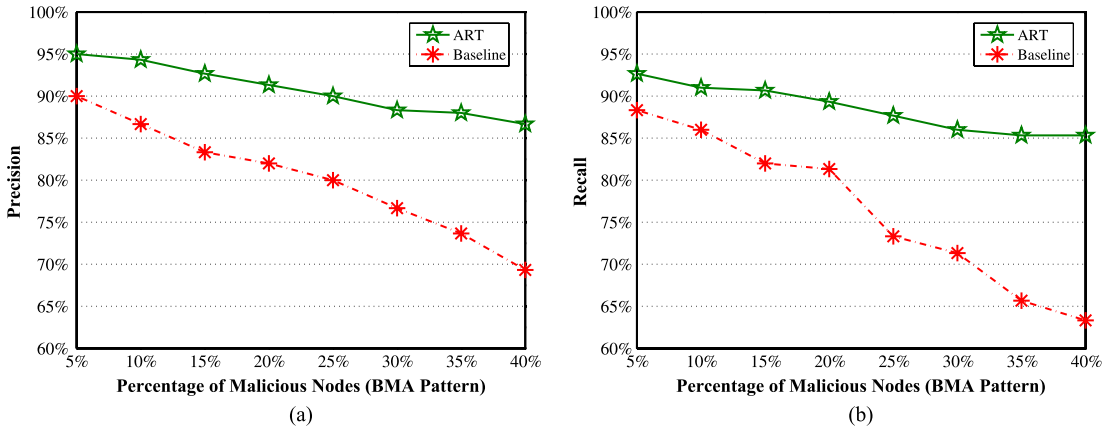



Fig. 7. ART vs. baseline under BMA pattern. (a) Precision of ART vs. baseline. (b) Recall of ART vs. baseline.

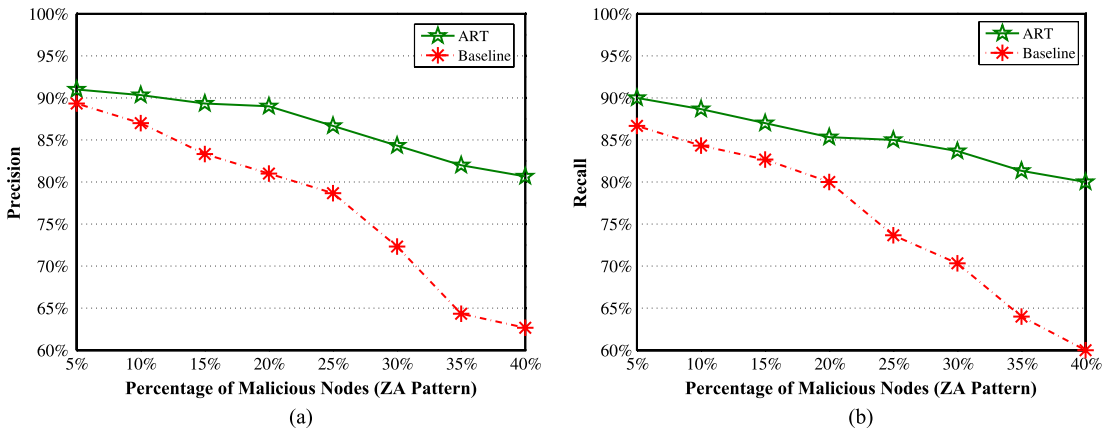



Fig. 8. ART vs. baseline under ZA pattern. (a) Precision of ART vs. baseline. (b) Recall of ART vs. baseline.

From Figs. 6–8, we can clearly find that the ART scheme outperforms the weighted voting (baseline) approach regardless of which attack pattern is utilized. Furthermore, we observe from Fig. 6 that the difference between the ART scheme and baseline is not that significant, which indicates that simple attack pattern is not very difficult to cope with for both approaches. This is true because malicious nodes are simply dropping or modifying packets without spreading any fake trust opinions and framing any benign nodes.

On the other hand, Fig. 7 shows that the weighted voting (baseline) approach suffers from the BMA pattern especially when there are a large amount of malicious nodes in the network, whereas the ART scheme can still achieve over 80% of precision and recall even when there are 40% of malicious nodes which are conducting bad mouth attacks. Note that bad mouth attack aims to intentionally share fake trust opinions (i.e., telling others a node is malicious while it is actually benign, and *vice versa*) so that the malicious nodes can remain undetected for a longer period of time and the benign nodes will be falsely accused of malicious behaviors. By using collaborative filtering based recommendation strategy as well as the Dempster–Shafer Theory of evidence, the proposed ART scheme is far more resistant to the weighted voting approach when the bad mouth attack is launched.

Finally, a sly attacker can also launch the zigzag attack, in which the attack behaviors are conducted in a more intermittent manner. Moreover, the attacker can demonstrate different attack patterns to different nodes. Thus, it is naturally more difficult to identify the malicious behaviors as well as the attacker who follows this attack pattern. Viewed from Fig. 8, it is obvious that the ART scheme can still resist the zigzag attack and achieve high precision and recall even when there are 40% of malicious nodes. On the other hand, the precision and recall values for the weighted voting approach get significantly degraded when the percentage of the attackers who follow ZA pattern increases.

In summary, we can clearly identify from Figs. 6–8 that when compared with the traditional weighted voting approach, the proposed ART scheme is better resistant to various attack patterns as well as to the high percentage of malicious nodes in the network.

## VI. Conclusion

In this paper, an attack-resistant trust management scheme named *ART* is proposed to evaluate the trustworthiness of both traffic data and vehicle nodes for VANETs. In the ART scheme, the trustworthiness of data and nodes are modeled and evaluated as two separate metrics, namely *data trust* and *node trust*, respectively. In particular, *data trust* is used to assess whether or not and to what extent the reported traffic data are trustworthy. On the other hand, *node trust* indicates how trustworthy the nodes in VANETs are. To validate the proposed trust management scheme, extensive experiments have been conducted, and experimental results show that the proposed ART scheme accurately evaluates the trustworthiness of data as well as nodes in VANETs, and it can also cope with various malicious attacks.

## References


[1] R. G. Engoulou, M. Bellache, S. Pierre, and A. Quintero, "VANET security surveys," *Comput. Commun.*, vol. 44, pp. 1–13, May 2014.

[2] M. Kakkasageri and S. Manvi, "Information management in vehicular ad hoc networks: A review," *J. Netw. Comput. Appl.*, vol. 39, pp. 334–350, Mar. 2014.

[3] B. T. Sharef, R. A. Alsaqour, and M. Ismail, "Vehicular communication ad hoc routing protocols: A survey," *J. Netw. Comput. Appl.*, vol. 40, pp. 363–396, Apr. 2014.

[4] S. Al-Sultan, M. M. Al-Doori, A. H. Al-Bayatti, and H. Zedan, "A comprehensive survey on vehicular ad hoc network," *J. Netw. Comput. Appl.*, vol. 37, pp. 380–392, Jan. 2014.

[5] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," *J. Comput. Security*, vol. 15, no. 1, pp. 39–68, Jan. 2007.

[6] Y. Lin and H. Song, "DynaCHINA: Real-time traffic estimation and prediction," *IEEE Pervasive Comput.*, vol. 5, no. 4, pp. 65–65, Oct.–Dec. 2006.

[7] J. Angwin and J. Valentino-Devries, Apple, Google Collect User Data, Apr. 2011. [Online]. Available: http://www.wsj.com/articles/SB10001424052748703983704576277101723453610

[8] Waze Mobile, Free Community-Based Mapping, Traffic & Navigation App. [Online]. Available: https://www.waze.com/

[9] J. R. Douceur, "The sybil attack," in *International Workshop on Peer-to-Peer Systems*, ser. Lecture Notes in Computer Science, P. Druschel, F. Kaashoek, and A. Rowstron, vol. 2429. Berlin, Germany: Springer-Verlag, 2002, pp. 251–260.

[10] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Ariadne: A secure on-demand routing protocol for ad hoc networks," in *Proc. 8th Annu. Int. Conf. MobiCom Netw.*, Atlanta, GA, USA, 2002, pp. 12–23.

[11] F. Nait-Abdesselam, B. Bensaou, and T. Taleb, "Detecting and avoiding wormhole attacks in wireless ad hoc networks," *IEEE Commun. Mag.*, vol. 46, no. 4, pp. 127–133, Apr. 2008.

[12] S. Buchegger and J.-Y. Le Boudee, "Self-policing mobile ad hoc networks by reputation systems," *IEEE Commun. Mag.*, vol. 43, no. 7, pp. 101–107, Jul. 2005.

[13] P.-W. Yau and C. J. Mitchell, "Security vulnerabilities in ad hoc networks," in *Proc. 7th Int. Symp. Commun. Theory Appl.*, 2003, pp. 99–104.

[14] 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, Apr. 2014.

[15] J. Molina-Gil, P. Caballero-Gil, and C. Caballero-Gil, "Aggregation and probabilistic verification for data authentication in VANETs," *Inf. Sci.*, vol. 262, pp. 172–189, Mar. 2014.

[16] N. Ekedebe, W. Yu, C. Lu, H. Song, and Y. Wan, "Securing transportation cyber–physical systems," in *Securing Cyber–Physical Systems*. Boca Raton, FL, USA: CRC Press, 2015, pp. 163–196.

[17] Y. Zhang and W. Lee, "Intrusion detection in wireless ad-hoc networks," in *Proc. ACM 6th Annu. Int. Conf. MobiCom Netw.*, Boston, MA, USA, 2000, pp. 275–283.

[18] H. Deng, Q.-A. Zeng, and D. Agrawal, "SVM-based intrusion detection system for wireless ad hoc networks," in *Proc. IEEE 58th VTC-Fall*, Oct. 2003, vol. 3, pp. 2147–2151.

[19] C.-Y. Tseng *et al.*, "A specification-based intrusion detection system for AODV," in *Proc. 1st ACM Workshop SASN*, Washington, DC, USA, 2003, pp. 125–134.

[20] Y.-A. Huang and W. Lee, "A cooperative intrusion detection system for ad hoc networks," in *Proc. 1st ACM Workshop SASN*, Washington, DC, USA, 2003, pp. 135–147.

[21] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in *Proc. ACM 6th Annu. Int. Conf. MobiCom Netw.*, Boston, MA, USA, 2000, pp. 255–265.

[22] L. Anderegg and S. Eidenbenz, "Ad hoc-VCG: A truthful and cost-efficient routing protocol for mobile ad hoc networks with selfish agents," in *Proc. 9th Annu. Int. Conf. MobiCom Netw.*, San Diego, CA, USA, 2003, pp. 245–259.

[23] Y. Xue and K. Nahrstedt, "Providing fault-tolerant ad hoc routing service in adversarial environments," *Wireless Pers. Commun.*, vol. 29, no. 3/4, pp. 367–388, Jun. 2004.

[24] M. Kefayati, H. R. Rabiee, S. G. Miremadi, and A. Khonsari, "Misbehavior resilient multi-path data transmission in mobile ad-hoc networks," in *Proc. 4th ACM Workshop SASN*, Alexandria, VA, USA, 2006, pp. 91–100.

[25] S. Buchegger and J.-Y. L. Boudec, "A robust reputation system for mobile ad-hoc networks," in *Proc. P2PEcon*, Berkeley, CA, USA, 2003, pp. 1–6.

[26] Q. He, D. Wu, and P. Khosla, "SORI: A secure and objective reputation-based incentive scheme for ad-hoc networks," in *Proc. IEEE WCNC*, Mar. 2004, vol. 2, pp. 825–830.

[27] S. Buchegger and J.-Y. L. Boudec, "The effect of rumor spreading in reputation systems for mobile ad-hoc networks," in *Proc. WiOpt, Model. Mobile, Ad Hoc Netw.*, 2003, pp. 131–140.
[28] S. Buchegger and J.-Y. Le Boudec, "Performance analysis of the confidant protocol," in *Proc. 3rd ACM Int. Symp. MobiHoc Netw. Comput.*, Lausanne, Switzerland, 2002, pp. 226–236.
[29] P. Michiardi and R. Molva, "CORE: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks," in *Proc. IFIP TC6/TC11 6th Joint Working Conf. Commun. Multimedia Security*, Portorož, Slovenia, 2002, pp. 107–121.
[30] A. Patwardhan, A. Joshi, T. Finin, and Y. Yesha, "A data intensive reputation management scheme for vehicular ad hoc networks," in *Proc. 3rd Annu. Int. Conf. Mobiquitous Syst. Workshops*, Jul. 2006, pp. 1–8.
[31] W. Li, A. Joshi, and T. Finin, "Coping with node misbehaviors in ad hoc networks: A multi-dimensional trust management approach," in *Proc. 11th Int. Conf. MDM*, May 2010, pp. 112–121.
[32] S. Taha and X. Shen, "A physical-layer location privacy-preserving scheme for mobile public hotspots in NEMO-based VANETs," *IEEE Trans. Intell. Transp. Syst.*, vol. 14, no. 4, pp. 1665–1680, Dec. 2013.
[33] Z. Li, C. Liu, and C. Chigan, "On secure VANET-based ad dissemination with pragmatic cost and effect control," *IEEE Trans. Intell. Transp. Syst.*, vol. 14, no. 1, pp. 124–135, Mar. 2013.
[34] T. Chim, S. Yiu, L. Hui, and V. Li, "OPQ: OT-based private querying in VANETs," *IEEE Trans. Intell. Transp. Syst.*, vol. 12, no. 4, pp. 1413–1422, Dec. 2011.
[35] R. Lu, X. Lin, X. Liang, and X. Shen, "A dynamic privacy-preserving key management scheme for location-based services in VANETs," *IEEE Trans. Intell. Transp. Syst.*, vol. 13, no. 1, pp. 127–139, Mar. 2012.
[36] G. Rebolledo-Mendez, A. Reyes, S. Paszkowicz, M. Domingo, and L. Skrypchuk, "Developing a body sensor network to detect emotions during driving," *IEEE Trans. Intell. Transp. Syst.*, vol. 15, no. 4, pp. 1850–1854, Aug. 2014.
[37] L.-Y. Yeh and Y.-C. Lin, "A proxy-based authentication and billing scheme with incentive-aware multihop forwarding for vehicular networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 15, no. 4, pp. 1607–1621, Aug. 2014.
[38] G. Shafer, *A Mathematical Theory of Evidence*. Princeton, NJ, USA: Princeton Univ. Press, 1976.
[39] C. Piao, J. Zhao, and J. Feng, "Research on entropy-based collaborative filtering algorithm," in *Proc. IEEE ICEBE*, Oct. 2007, pp. 213–220.
[40] J. S. Breese, D. Heckerman, and C. Kadie, "Empirical analysis of predictive algorithms for collaborative filtering," in *Proc. 14th Conf. UAI*, Madison, WI, USA, 1998, pp. 43–52.
[41] G. Adomavicius and A. Tuzhilin, "Toward the next generation of recommender systems: A survey of the state-of-the-art and possible extensions," *IEEE Trans. Knowl. Data Eng.*, vol. 17, no. 6, pp. 734–749, Jun. 2005.
[42] P. Resnick, N. Iacovou, M. Suchak, P. Bergstrom, and J. Riedl, "GroupLens: An open architecture for collaborative filtering of Netnews," in *Proc. ACM Conf.*, 1994, pp. 175–186.
[43] X. Zeng, R. Bagrodia, and M. Gerla, "GloMoSim: A library for parallel simulation of large-scale wireless networks," *ACM SIGSIM Simul. Dig.*, vol. 28, no. 1, pp. 154–161, Jul. 1998.
[44] M. Raya, P. Papadimitratos, V. D. Gligor, and J.-P. Hubaux, "On data-centric trust establishment in ephemeral ad hoc networks," in *Proc. IEEE INFOCOM*, 2008, pp. 1238–1246.
[45] I.-R. Chen, F. Bao, M. Chang, and J.-H. Cho, "Dynamic trust management for delay tolerant networks and its application to secure routing," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 5, pp. 1200–1210, May 2014.
[46] J. Davis and M. Goadrich, "The relationship between precision–recall and ROC curves," in *Proc. ACM 23rd Int. Conf. Mach. Learn.*, 2006, pp. 233–240.

**Wenjia Li** (M'11) received the Ph.D. degree in computer science from the University of Maryland Baltimore County, Baltimore, MD, USA, in 2011.

In August 2014, he joined the Department of Computer Science, New York Institute of Technology, New York, NY, USA, where he is currently an Assistant Professor. Prior to that, he was an Assistant Professor of computer science at Georgia Southern University, Statesboro, GA, USA, from August 2011 to July 2014. He has published more than 30 peer-reviewed papers. His research interests are in the areas of cyber security, mobile computing, and wireless networking, particularly security, trust, and policy issues for wireless networks, cyber–physical systems, Internet of Things, and intelligent transportation systems. His research has been supported by the University Transportation Research Center Region 2.

Dr. Li is a member of the ACM. He served as an Organizing Committee Member for various international conferences, such as ACM WiSec, IEEE MDM, IEEE IPCCC, IEEE Sarnoff, etc., and he also served as a reviewer for many prestigious journals, such as IEEE TWC, IEEE TPDS, IEEE T-IFS, IEEE TDSC, etc.

**Houbing Song** (M'12–SM'14) received the M.S. degree in civil engineering from the University of Texas, El Paso, TX, USA, in 2006 and the Ph.D. degree in electrical engineering from the University of Virginia, Charlottesville, VA, USA, in 2012.

In 2012, he joined the Department of Electrical and Computer Engineering, West Virginia University, Montgomery, WV, USA, where he is currently an Assistant Professor and the Founding Director of both the West Virginia Center of Excellence for Cyber–Physical Systems (WVCECPS), sponsored by the West Virginia Higher Education Policy Commission, and the Security and Optimization for Networked Globe Laboratory (SONG Lab). He was with Texas A&M Transportation Institute, Texas A&M University System, as an Engineering Research Associate in 2007. He has published more than 80 peer-reviewed papers. His research interests are in the areas of cyber–physical systems, Internet of Things, intelligent transportation systems, wireless communications and networking, and optical communications and networking. His research has been supported by the West Virginia Higher Education Policy Commission.

Dr. Song is a member of ACM. He has served as the General Chair or Technical Program Committee Chair for six IEEE international workshops and a Technical Program Committee Member for numerous international conferences, including ICC, GLOBECOM, INFOCOM, WCNC, among others. He has been an Associate Editor or a Guest Editor of more than ten international journals.