Publish or Drop Traffic Event Alerts? Quality-aware Decision Making in Participatory Sensing-based Vehicular CPS

RAJESH P. BARNWAL*, CSIR-CMERI Durgapur and Indian Institute of Technology Kharagpur
NIRNAY GHOSH*, Indian Institute of Engineering Science and Technology Shibpur
SOUMYA K. GHOSH, Indian Institute of Technology Kharagpur
SAJAL K. DAS, Missouri University of Science and Technology, USA

Vehicular cyber-physical systems (VCPS), among several other applications, may help address an ever-increasing challenge of traffic congestion in large cities. Nevertheless, VCPS can be hindered by information falsification problem, resulting due to the wrong perception of a traffic event or deliberate faking by the participating vehicles. Such information fabrication causes the re-routing of vehicles and artificial congestion, leading to economic, safety, environmental, and health hazards. Thus, it is imperative to infer truthful traffic information in real-time to restore the operational reliability of the VCPS. In this work, we propose a novel reputation scoring and decision support framework, called *Spoofed and False Report Eradicator (SAFE)*, which offers a cost-effective and efficient solution to handle information falsification problem in the VCPS domain. The framework includes humans in the sensing loop by exploiting the paradigm of *participatory sensing*, a concept of a *mobile security agent (MSA)* to nullify the effects of deliberate false contribution, and a variant of the *distance bounding* mechanism to thwart location-spoofing attacks. A regression-based model integrates these effects to generate the expected truthfulness of a participant's contribution. To determine if any contribution is true or false, a generalized linear model is used to transform the expected truthfulness into a *Quality of Contribution (QoC)* score. The QoC of different reports is aggregated to compute user reputation. Such reputation enables classification of different participation behaviors. Finally, an *Expected Utility Theory (EUT)*-based decision model is proposed which utilizes the reputation score to determine if event-specific information should be published or dropped. To evaluate the *SAFE* framework through experimental study, we used both simulated and real data to compare its reputation-based user segregation performance with state-of-the-art frameworks. Experimental results exhibit that *SAFE* captures the fine differences in participants' behavior through the quality and quantity of participation, and the accuracy of their informed location. It also significantly improves operational reliability through publishing the information of only legitimate events.

CCS Concepts: • **Cyber-Physical Systems → Transportation Systems**; *Vehicular Network*; Participatory Sensing; Decision Theory;

Additional Key Words and Phrases: Vehicular cyber-physical system, Participatory sensing, Information falsification, Reputation, Automated decision making

*Co-primary authors

Authors' addresses: R. P. Barnwal, Information Technology Group, CSIR-Central Mechanical Engineering Research Institute, Durgapur, India (r_barnwal@cmeri.res.in); N. Ghosh, Department of Computer Science and Technology, Indian Institute of Science Engineering and Technology, Shibpur, India (nirnay@cs.iiests.ac.in); S. K. Ghosh, Department of Computer Science and Engineering, Indian Institute of Technology, Kharagpur, India (skg@cse.iitkgp.ac.in); S. K. Das, Department of Computer Science, Missouri University of Science and Technology, Rolla, USA (sdas@mst.edu);

XXXX-XXXX/2019/1-ART1 $15.00
https://doi.org/10.1145/3321480

ACM Reference format:
Rajesh P. Barnwal*, Nirnay Ghosh*, Soumya K. Ghosh, and Sajal K. Das. 2019. Publish or Drop Traffic Event Alerts? Quality-aware Decision Making in Participatory Sensing-based Vehicular CPS. *ACM Transactions on Cyber-Physical Systems* 1, 1, Article 1 (January 2019), 28 pages.
https://doi.org/10.1145/3321480

1 INTRODUCTION

According to a survey of the United Nations, more than 54% of the world's population lives in urban areas, a proportion that is expected to increase to 66% by 2050[1]. Transportation systems have always been an indispensable part of urban life for many decades. With the current surge in urban population, the number of both private and public vehicles are growing at an alarming rate. This is evident from the annual increase in the number of vehicles in developing countries like India, which is approximately 11%, as opposed to 4% growth in the road infrastructure[2]. Irrespective of the geographical location, the biggest problem faced by the current transportation management system is managing traffic congestion, which has cascading effects on the economy, public safety, environment, and health.

Traffic congestion causes approximately $87.2 billion annual drains on the US economy, with 4.2 billion work-hours and 2.8 billion gallons of fuel wasted waiting in traffic, which is equivalent to one work week and three weeks worth of gas per year [Ekedebe et al. 2015]. Congestion increases the error in driving, which accounts for 93% of approximately 6 million annual automobile crashes [Malta et al. 2009] [Ekedebe et al. 2015] causing loss of human lives and damage of properties. As per the report published by the US Federal Highway Administration, traffic accidents account for approximately 50-60% of traffic congestions in cities [Reiss 1991] [Zhang et al. 2011]. Thus, besides traffic jam, an accident can also cause congestion which entails the need for accurate and up-to-date information for its prevention. Moreover, tailpipe emission is the single largest man-made source of carbon dioxide, nitrous oxides, and methane that can increase the air pollution index by many-fold [Zhang et al. 2011] and it can also increase the risk of health hazards, as identified by several medical reports [Peters et al. 2004]. Thus, there is an increasing need for addressing the traffic congestion problem in order to improve safety, the efficiency of the transportation sector, and protection of the environment as well as human health.

Expansion of roads and developing new infrastructures can offer an immediate solution to address this problem. However, such approaches are costly and challenging because, with the increase in urban population, land resources are fast diminishing. During the 2008 Beijing Olympics, the city administration imposed the restriction on private cars based on odd/even license plate numbers to keep 50% traffic off the road. This policy is still followed in Beijing and a few other cities around the world and can reduce congestion and the associated air pollution problem to some extent. However, enforcing such a policy may not be convenient across all geographical regions [Zhang et al. 2011].

The concept of a *cyber-physical system (CPS)* may help address the above-mentioned challenges to a great extent. A CPS is a next-generation integrated system with sensors (including human users), actuators, and computation/control core. It is designed to sense and interact with the physical world (including human users) and support real-time, guaranteed performance in safety-critical applications [Rajkumar et al. 2010]. The application of CPS in the transportation or vehicular sector, henceforth called *vehicular CPS (VCPS)*, is expected to transform the way people interact with highway transportation systems. VCPS will connect vehicles, infrastructures, and drivers, and provide a centralized platform for dissemination of up-to-date and accurate traffic information

[1]http://www.un.org/en/development/desa/news/population/world-urbanization-prospects-2014.html
[2]http://www.indiaspend.com/investigations/indias-traffic-nightmare-roads-grow-4-vehicles-grow-11-2

which can provide real-time route guidance, thus avoiding congestion and potentially reducing accidents caused due to human errors.

1.1 Next Generation Vehicular CPS

In general, *vehicular ad hoc networks (VANETs)* or *Internet of Vehicles (IoVs)* forms the networking infrastructure of VCPS [Rawat and Bajracharya 2017] [Ekedebe et al. 2015]. In VANET the nodes (vehicles) communicate with each other (without disclosing individual identities) using vehicle-to-vehicle (V2V) and/or vehicle-to-infrastructure (V2I) communications through dedicated short-range communications (DSRC) technology [Jiang and Delgrossi 2008]. This often restricts the VCPS service to only high-end vehicles (a small fraction of traffic worldwide) and also requires the establishment of dedicated road-side infrastructures. This necessitates a novel sensing and communication framework for VCPS.

Alongside, recent years have also seen a massive proliferation of smartphone technology. Indeed, their widespread adoption has thrived mobile sensing and mobile Internet, which was previously envisioned as the *Participatory Sensing (PS)* [Burke et al. 2006]. According to Ericsson's Mobility Report (2016)[3], the number of smartphone users has been projected to be 6.3 billion by the end of 2021, suggesting almost one for every person on the planet. Thus, it is imperative that smartphones will soon become the most powerful sensing device and may replace the traditional sensory data collection infrastructure.

In the PS paradigm, smartphone users can register to a PS application and voluntarily contribute (in the form of a report, image, audio. etc.) certain observations, typically in lieu of rewards computed by different incentive schemes [Restuccia et al. 2016] [Luo et al. 2017]. The PS system filters and analyzes such contributions to generate a piece of summarized information and disseminates it to enable better decision making. As the PS paradigm fuses human intelligence (sensing and information gathering) with machine intelligence (analysis and filtering), its utility in social space has increased by many folds. The real benefit of PS paradigm is that none of its functionalities (i.e., sensing, information gathering, analysis, and publishing of information) need the establishment of a dedicated infrastructure [Restuccia and Das 2014], thereby reducing overheads associated with sensor deployment, management, and periodic maintenance. Moreover, for reaping the benefits of VCPS services, smartphone-based participatory sensing is definitely a cost-effective choice as compared to other options such as owning a high-end car.

Fig. 1 shows the architecture of our envisioned PS-based VCPS. As evident, the paradigm of participatory sensing and its associated app is expected to enrich the human-assisted data collection and message exchanging aspect of VCPS environment. The PS-supported VCPS will reduce the sensing costs for both the service provider and consumers. In this system, vehicle drivers will sense the traffic condition (viz., traffic jam, accident, weather hazard, road condition etc.) and generate reports using a smartphone application. These reports will be submitted to the PS server in the cloud via the cellular network, which in turn, will publish a summarized alert as broadcast notification. Based on the received alert, the vehicles will actuate their movements that ultimately change the traffic dynamics.

However, the realization of VCPS using the PS paradigm is poised to introduce new security challenges. Owing to the "open" nature of the PS paradigm, the application may get exposed to false contributions [Huang et al. 2010] [Wang et al. 2016], resulting in the dissemination of erroneous information and thus aggravating the congestion problem. In general, PS applications incentivize users so that they remain motivated to persistently contribute useful sensory data. For example.

[3]https://www.ericsson.com/res/docs/ 2016/ericsson-mobility-report-2016.pdf

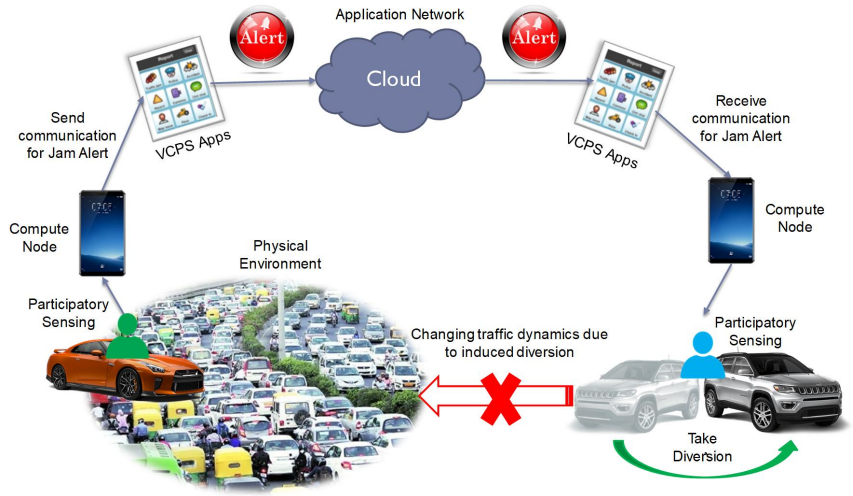


Fig. 1. Envisioned VCPS Architecture

real-life traffic monitoring application like *Waze*[4] practices "gamification" by rewarding the *quantity of participation*, rather than the *quality of contribution* [Barnwal et al. 2016] [Bhattacharjee et al. 2017a]. This implicitly motivates dishonest users to generate intermittent false reports to gain undue incentives. Moreover, there can be spoofers who pretend to be present in the vicinity of actual events by camouflaging their GPS locations and then generate reports for earning incentives. Finally, there may be malicious users who collude among themselves to generate false reports in bulk (spam) and overwhelm the PS system. Occasionally, false contributions may also be generated owing to the wrong perception of the event. Regardless of the motive, information falsification invariably incurs loss of revenue owing to distribution of undue incentives, and defiles the overall reliability of the VCPS services.

We argue that besides the *quantity*, assessing the *quality of contribution (QoC)* is equally necessary [Restuccia et al. 2017]. This QoC is essentially an indicator of truthfulness of user participation and is similar to its *trust score*. Moreover, participant reputation generated from his truthful contribution helps to classify him as honest or dishonest (e.g., liar, spoofer, malicious). To make the VCPS resilient to false information, QoC also helps to decide if future reports from that user will be considered for publishing or dropping [Bhattacharjee et al. 2019].

1.2 Contributions of this Work

This paper proposes a framework, called *Spoofed and False report Eradicator* (*SAFE*), which attempts to address the problem of information falsification in vehicular CPS. First, we propose a QoC measure for each user contribution based on two mechanisms: (i) *mobile security agents (MSAs)* [Restuccia and Das 2014] to validate the user contributions, and (ii) a variant of *distance bounding* method [He et al. 2011] to verify user's locations. Deployment of MSAs weakens the effect of *deliberate false contributions* by using a customized version of Jøsang's opinion and trust model [Jøsang 1999]. On the other hand, the distance bounding method thwarts location spoofing attacks. Henceforth, we model the expected truthfulness of the contribution as a regression score using *Gompertz* and *inverse sigmoid* functions as the weights (coefficients) for MSAs and distance bounding effects, respectively. Subsequently, we transform the expected truthfulness to a QoC (trustworthiness) measure using the logit link function that captures the odds of a contribution being true or false.

[4]www.waze.com

Second, we aggregate the QoC measures of all the contributions made by a user to compute a raw user reputation score. A normalized reputation score is generated in the interval [-1, +1] by means of a scaling function. It is used for classifying users as honest, liars and spoofers.

Third, we propose an *expected utility theory (EUT)*-based two-level decision-making model that makes use of the reputation scores and other contextual information to publish only true events.

Finally, we use both simulated and real data for extensive performance evaluation of the *SAFE* framework. We show that our approach outperforms two state-of-the-art PS reputation scoring mechanisms: (i) Jøsang's opinion and trust model-based *FIDES* system [Restuccia and Das 2014], and (ii) *Gompertz* function-based model [Huang et al. 2010] [Huang et al. 2014], in terms of distinctly identifying different user behaviors based on their reputations. Experimental results depict that *SAFE* provides a reputation score which renders fair distinction among different participating behaviors. Furthermore, our EUT-based decision-making model guarantees accuracy by publishing only true events.

The rest of this paper is organized as follows. Section 2 discusses the existing works on handling information falsification problem in VCPS as well as reputation-based PS systems. Section 3 presents the system and threat models and discusses the design principle of the PS sub-system, contained in the VCPS. Section 4 proposes the *SAFE* framework for generating user reputation scores while Section 5 presents an application of *SAFE* by proposing an EUT-based decision-making model. Section 6 discusses the results and Section 7 offers conclusions.

2 RELATED WORK

This section reviews different *centralized* mechanisms to prevent information falsification attacks in vehicular CPS. Further, in the context of our participatory sensing (PS)-based approach, we also identify the limitations with the existing related works.

2.1 Handling Information Falsification in Vehicular CPS

As mentioned, information falsification is a major security challenge in VCPS, where the underlying network model is a VANET [Krishna et al. 2015] [Barnwal and Ghosh 2016]. In such attacks, compromised nodes and adversaries create a large number of pseudo-identities and disseminate false information [Park et al. 2009] [Qu et al. 2015]. The objective behind this deceptive behavior is to disturb normalcy for specific illegal purposes and generate a fake consensus among other vehicle drivers. Indeed, *Waze* was the subject of such a Sybil attack in Israel, where the adversary generated a large number of fake traffic jam reports and orchestrated artificial roadblocks and subsequent re-routing [Sinai et al. 2014].

Tackling information falsification issue in VANETs is predominantly done by the following mechanisms [Hubaux et al. 2004]: (i) source authentication, and (ii) message integrity. For a centralized approach, these requirements are implemented by proposing a *Trusted third party (TTP)*, which is supported by multiple road side units or RSUs [Raya and Hubaux 2005]. For authenticating the legitimacy of vehicles, the TTP maintains a *certificate revocation list (CRL)* which contains the identities of the misbehaving vehicles. One possible approach to identify them is to compute the trust scores based on their past behavior [Raya et al. 2007]. The enlisted vehicles are revoked from accessing the VANET resources.

The TTP updates the CRL periodically and shares it with the co-located RSUs, in turn, check the latest CRL and authenticate the vehicles before broadcasting the messages generated by them [Huang et al. 2011] [Shim 2012]. This will implicitly ensure that the fabricated messages do not get disseminated in the VANET. However, the major issue with the CRL-based authentication is its scalability, particularly storing, searching, and distributing the list in real-time as its size grows. Moreover, significant infrastructure cost will be incurred to deploy RSUs for hosting the TTPs. For

ensuring message integrity, a digital signature enabled *VANET Public Key Infrastructure (VPKI)* has been proposed, the details of which are available in [Ekedebe et al. 2015] [Qu et al. 2015].

2.2 Handling Information Falsification in Participatory Sensing

State-of-the-art literature shows that prevention of information falsification in the PS paradigm is done by three primary approaches: (i) recruitment of trustworthy participants, (ii) truth inference by reliability assessment of sources, and (iii) establishing a trust relationship with the participants.

Establishing trust relationships in the PS paradigm is an essential requirement as the sensing platform has to depend on the contributions from its participants in absence of the real-time ground truth. Thus, our proposed work explicitly falls under the purview of the third category. A few relevant works in this area are as follows.

2.2.1 Gompertz Function-based Reputation. Gompertz function models a time series, where the growth is slowest at the start and end of a time period. Such a function has been used in [Huang et al. 2010] [Huang et al. 2014] [Yu et al. 2014] to compute the participants' reputation in the PS paradigm. For example, in [Huang et al. 2010] [Huang et al. 2014], reputations of devices reporting environmental noise data have been computed. The model takes as input past cooperation levels and maps them into a cumulative reputation score. The level of cooperation is determined by a "watchdog" module which runs an outlier detection algorithm to measure the distance between the submitted data and the consensus.

A major limitation of Gompertz-based reputation models is that they do not consider the uncertainty factor in the trust assessment. Handling uncertainty is an important aspect as far as traditional trust definition is concerned [Jøsang 1999]. Furthermore, it does not unify the quality and quantity of contributions and is not also fair to different participating behaviors.

2.2.2 Fuzzy Inference-based Reputation. In [Amintoosi and Kanhere 2013] [Amintoosi and Kanhere 2014] [Amintoosi et al. 2015], the authors leverage fuzzy logic to compute trust scores based on the collected trustworthiness evidence. They assumed that every participant is a part of an existing on-line social network platform and his friendship relations are depicted by a social graph. The system works in a publish/subscribe manner where a *requester* publishes a sensing task with a fixed deadline. A set of contributors, known as *participants*, who are friends with the requester, report their observations related to the sensing task.

Trustworthiness of a contributing user depends upon the combination of the following five personal and social factors: *expertise, timeliness, location, friendship duration,* and *interaction time gap*. A *Trust of Participant (ToP)* metric is derived from the weighted sum of these five factors. Another metric, called *Quality of Contribution (QoC)*, which reflects the quality of sensing report in terms of accuracy, precision, and timeliness, is determined by an outlier detection algorithm. Finally, *Trust of contribution (ToC)* is computed by designing a fuzzy inference system where the antecedents are different fuzzy sets formed by partitioning the crisp values of *ToP* and *QoC*.

One prominent limitation with fuzzy inference-based approaches is that they need regular monitoring of the locations and other personal information of the participants, and thus not privacy preserving. Such location tracking may not be acceptable to most of the participants, leading to in-feasibility in practical usage. Another issue is the requirement for a fairly high degree of subjectivity while assigning weights to the social factors and forming the fuzzy sets. The final trust score is highly sensitive to the choice of these weights and the partitioning scheme of the domain of *ToP* and *QoC*.

2.2.3 Feedback Distribution-based Reputation. Several works in the literature [Restuccia and Das 2014] [Ganeriwal et al. 2008] [Xiang et al. 2017] have used feedback distribution-based approach to

compute trust scores of the participants in the realm of participatory sensing. These works have explicitly used Jøsang's belief models [Jøsang 1999] [Jøsang and Ismail 2002] which considered the state space of trustworthiness evidence to be feedback-based rating. Depending on the binary or ternary nature of the feedback domain, trust modeling is done by *Beta* or *Dirichlet* distribution. Even some real PS applications, viz., FourSquare, Waze, and Yelp, use rating feedback mechanism, whereby consumers of the service provide positive, negative or neutral ratings against a published information. The benefit of using a feedback rating paradigm is that it is easy, fast, less expensive and exudes the essence of the PS paradigm.

However, there exist several limitations with reputation scoring done based on Jøsang's belief models [Jøsang 1999] [Jøsang and Ismail 2002]. Besides being less aggressive in penalizing users that contribute corrupted data, these models neither take into account the confidence of the rating community on a particular event nor have any provision to control the effect of deliberate "undecided" ratings, leading to an undue increase in the trust score [Bhattacharjee et al. 2017b]. Rating-based systems expect a significant proportion of feedbacks within a short time span to dynamically compute accurate trust scores, which may not be necessarily true for all real-time applications. Moreover, providing ratings is mostly voluntary and does not fetch any incentive, which demotivates users from submitting feedbacks. Table 1 summarizes the limitations of the state-of-the-art reputation scoring methodologies in participatory sensing paradigm.

Table 1. Handling Information Falsification by Reputation Scoring: Summary

Underlying Approach	**Evidence Collection**	**Remarks**
Gompertz function [Huang et al. 2010] [Huang et al. 2014] [Yu et al. 2014]	Outlier detection	Gompertz function does not handle uncertainty in trust computation and is also not fair to different participating behaviors.
Fuzzy logic [Amintoosi and Kanhere 2013] [Amintoosi and Kanhere 2014] [Amintoosi et al. 2015]	Spatio-temporal location, endorsement, expertise	Potential privacy breach due to trajectory tracking and a higher degree of subjectivity in deciding membership functions and fuzzy sets.
Feedback distribution [Restuccia and Das 2014] [Ganeriwal et al. 2008] [Xiang et al. 2017]	Ratings submitted by participants	Sufficient feedback may not be always available. Non-consideration of both *quality* and *quantity* of contributions can lead to colluding attacks.

Thus, it is clear that the existing literature does not address one or more of the following issues: (i) uncertainty in trust computation, (ii) avoid tracking of participants' trajectory to preserve privacy, and (iii) leverage both "quality" and "quantity" of participation to thwart colluding attacks.

Nevertheless, to address the problem of location spoofing and false-event report generation by considering all of the above-mentioned issues, there is a need for a comprehensive QoC-aware decision-making framework for participatory sensing-based VCPS. Our proposed framework is expected to mitigate the effect of spoofers and liars. Further, to supplement the limitations of Gompertz-based reputation models while utilizing its strength, the framework must devise a mechanism for fusion of Gompertz-based reputation models with Jøsang's belief model for computing the reputation score. Finally, it is imperative for the framework to constitute a robust decision-making model to filter out false and spoofed reports in real-time by utilizing the prior event-occurrence knowledge and reputation of the participants, resulting from the fusion model.

3 SYSTEM AND THREAT MODELS

In this section, we present the system model, threat model, and the design principle of the proposed *SAFE* framework.

3.1 System Model

As depicted in Fig. 2, the system model captures a particular urban area, divided into multiple sensing regions. Let the sensing regions contain U users and E events. Each user possesses smartphone(s) and is registered to a PS application supported by the vehicular CPS. The major components of this

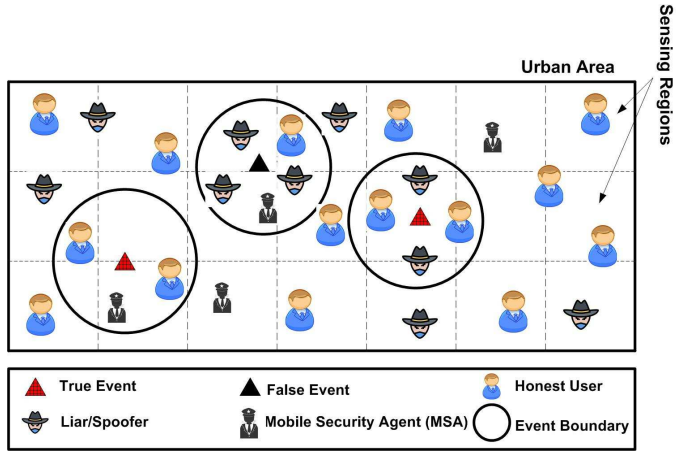


Fig. 2. System Model

model are as follows:

Report: A report r_j is a notification generated by a user in response to his perception of a traffic incident (viz., accident, jam, road closure, weather hazard, etc.) at a particular time epoch (defined below). Modern-day smartphone apps get complete access to built-in sensors (with user consent) once they are installed. Likewise, we assume that at the time of submitting reports, the PS application reads the data generated by low-level sensors like GPS, accelerometer, gyroscope, and so on. For ease of representation, we will use the notation j to denote a report. The terms 'report', and 'contribution' have been used to refer 'means of participation'.

Event: An event $e_l \in E$ is an alert to publish information related to a traffic incident after the PS application receives a pre-defined number of "similar" reports and verifies their truthfulness. This information sent to the rest of the VCPS system for analysis, decision making, and actuation in the physical space (refer Fig.3). If reports from two participants are similar in terms of location, time epoch, and incident type, they are considered to be generated for the 'same' event instance. For notational convenience, we will use l to represent an event.

Generally, each event l should belong to a set of potential event types $\mathbb{Z}$, indexed by $z \in \{1, \cdots, |\mathbb{Z}|\}$. As illustrated in Fig. 2, an event can be either reported truthfully (True Event) or falsely (False Event) by the participant and present within a fixed boundary. Reports from the registered participants within that boundary will be only considered for that event. This boundary may be generated after the PS system extracts an expected event location (as the center of the circle) from the set of geo-tagged reports. Some common approaches to construct the event boundary are the various geospatial clustering methods ranging from GPS stamps to MGRS (Military Grid Reference System) conversion [Huang et al. 2010].

Time epoch: A time epoch t_k is the fixed temporal window during which the sensing reports from different users are accepted, their reputation scores are updated, and the decision about publishing the event is taken. It is noted that the reputation scores of only those users who have generated reports in the current time epoch will be updated. For simplicity of notation, we will denote an epoch as k.

The system model consists of two types of users:

Participant: A participant $u_i \in U$ is a participating user who is commuting (in a vehicle) along the vicinity of an event and has the proclivity to generate report(s). Any participant who has generated at least one report is liable to have a reputation score which reflects the overall quality of contribution as well as the degree (quantity) of participation. We refer a user simply as i for notational convenience.

Mobile security agent (MSA): A mobile security agent (MSA) is a trusted user who moves across different sensing regions and reports *reliable* information about his surroundings to the PS application. He cannot be sabotaged to either move out of a region intentionally or submit false information to generate a wrong consensus about the occurrence of an event. Depending on the requirement, the VCPS can deploy multiple MSAs. However, it is not necessary to have MSAs present in all the sensing regions at a given time epoch which can restrict the PS platform from receiving truthful information. In practical scenarios, the reliability of the MSAs may be guaranteed by some sort of reward provided upfront by the VCPS administrator. For example, MSAs could be taxicab or bus drivers who drive across different sensing regions all over the day.

3.2 Threat Model

In general, neutral users do not have any selfish intent to generate multiple reports during the same time epoch as it will be considered as a single contribution to the PS system. However, malicious users can take advantage of the absence of MSAs at a particular region during a time epoch and pose the threat of generation of rogue reports. Although it is completely non-deterministic if any region will be devoid of MSAs at a particular time epoch, still such users can exhibit the following types of participation:

False participation: This participation occurs if a dishonest participant (termed as a liar) generates intermittent false reports to increase his degree of participation with the goal of gaining undue incentives. Such participation may or may not be verified at a particular time epoch depending on the presence or absence of MSAs in the event vicinity. The liar may or may not spoof his location while generating false reports.

Side-channel participation: Such participation can occur when a rogue user intends to earn undue incentives through proxy participation. The user (termed as spoofer) exercising this participation will undergo social engineering to know about a true event, and then generate reports in spite of not being physically present in that sensing region. This can be done by spoofing the GPS of his smartphone using various location faking apps and masquerade himself to be present at the actual event site.

3.3 Design Principle

Vehicular CPS conceived in this work includes humans (drivers) in the feedback loop. They act as sensors and contribute data in the form of reports on the status of the traffic at different sensing regions by using smartphone-based PS application. Such sensing task may be either *explicit* (i.e., done directly by humans) or *implicit* via the sensors (e.g., sensors equipped to smartphones, wearables, vehicles, etc.) the humans own [Guo et al. 2015]. The sensed information contributed by the humans is analyzed and aggregated by the VCPS to trigger and publish an event. This facilitates

better decision making in the physical space. Fig. 3 presents a schematic representation of the vehicular CPS.

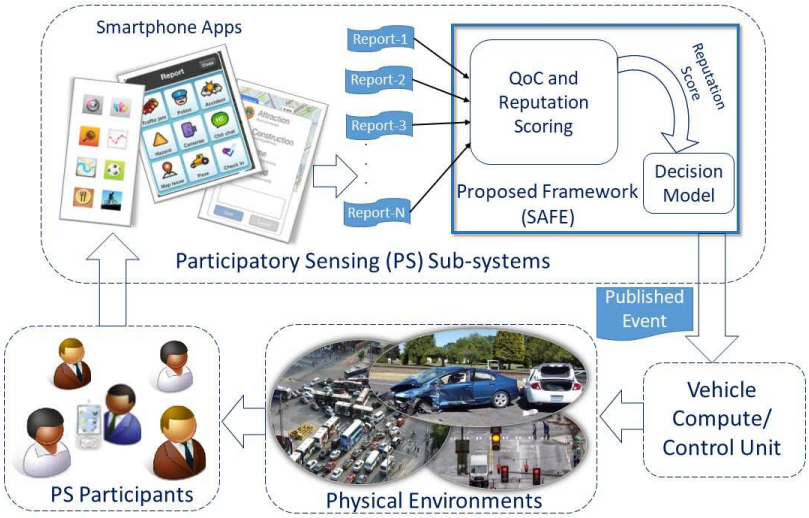


Fig. 3. Design Principle of the Proposed *SAFE* Framework

As evident from Fig. 3, four major components of the VCPS forming a loop are: (i) PS participants, (ii) the PS sub-system, (iii) the vehicle compute/control core, and (iv) physical environment. The PS sub-system is an important component in the VCPS loop. It collects rich sensory information generated by human users via smartphone applications and relieves the VCPS from the deployment of any road-side infrastructure. However, to ensure the operational reliability of the VCPS loop, there is a need to ensure that the information generated by the PS sub-system is accurate and up-to-date. As the latter provides an interface to receive data from the crowd, evaluating the *quality of contribution (QoC)* needs to be done here to ensure dissemination of correct information onto the other parts of the VCPS loop. To address the above challenge, we propose the *SAFE* framework, which is a module within the PS sub-system. Fig.3 shows two major modules in the *SAFE* framework:

- *QoC and Reputation Scoring*: It computes the QoC for each contribution (report) generated by a participant. Next, it aggregates the QoC scores of all the reports which the participant has generated to compute his own reputation score.
- *Automated Decision-Making Model*: It publishes the final event by computing the expected utility on each event type using the number of reports received and the reputation scores of the contributors.

4 *SAFE*: SPOOFED AND FALSE REPORT ERADICATOR FRAMEWORK

In this section, we present the modules of our proposed framework *SAFE*, which aims to provide QoC and reputation scoring.

4.1 Modeling Opinion on User Generated Report

As discussed in Section 3.1, the VCPS deploys a few mobile security agents (MSAs) who move across different sensing regions at various time epochs. These MSAs provide truthful feedback based on

which the *SAFE* framework decides whether a user report is to be believed or not. However, regions where none of the MSAs is present during a time epoch, it is *uncertain* about the participants' contributions. Depending on the feedback of the MSAs, the framework develops an *opinion* for each user report generated during a particular time epoch [Restuccia and Das 2014]. Formally, an opinion is defined as follows [Jøsang 1999]:

Definition 1. *(Opinion). An opinion $\theta_{i,j}^k$ is a vector $\theta = [b, d, u]$, such that $b + d + u = 1$, $\{b, d, u\} \in [0, 1]$, where b, d, and u are respectively the probabilities of belief, disbelief, and uncertainty on report j generated by user i during time epoch k.*

Initially, if any user i has just registered with the PS application but is yet to contribute any information, the opinion vector will assign equal probabilities to belief, disbelief, and uncertainty. In other words, $b = d = u = \frac{1}{3}$ and the opinion vector will be given as: $\theta_{i,0}^0 = [\frac{1}{3}, \frac{1}{3}, \frac{1}{3}]$. We introduce two *distrust rates* $0 < \mu_1, \mu_2 < 1$ which will increase or decrease the influences of the probability masses on the overall opinion. We adopt the strategy used in [Restuccia and Das 2014] to vary the impacts on belief, disbelief, and uncertainty, depending on the nature of participation, i.e., if it is true, false, or unknown.

If any MSA endorses a user contribution as true or false, then belief or disbelief will be changed by the factor μ_1 depending on the MSA's feedback about that report generated at a given time epoch. However, if MSAs are not available in the event boundary, and the user contribution cannot be verified, the uncertainty measure on the overall opinion will boost up by the factor μ_2, while the impacts on the other two masses will be diminished. As the feedbacks from MSA is considered to be more truthful, we have $\mu_1 < \mu_2$.

Thus, if report j generated at time epoch k is declared to be true based on the MSA's observation, the opinion vector will be updated as follows:

$$\theta_{i,j}^k = [(b_i^{k-1})^{\mu_1}, (d_i^{k-1})^{2-\mu_1}, (u_i^{k-1})^{2-\mu_1}] \tag{1}$$

where b_i^{k-1}, d_i^{k-1}, and u_i^{k-1} are the belief, disbelief, and uncertainty measures on user i, computed till the $(k-1)^{th}$ time epoch.

Similarly, if a report has been found to be false according to the MSA's feedback, the opinion vector becomes:

$$\theta_{i,j}^k = [(b_i^{k-1})^{2-\mu_1}, (d_i^{k-1})^{\mu_1}, (u_i^{k-1})^{2-\mu_1}] \tag{2}$$

Finally, if the truthfulness of a report cannot be verified due to the absence of MSAs at a particular event boundary, the opinion vector is given as:

$$\theta_{i,j}^k = [(b_i^{k-1})^{2-\mu_2}, (d_i^{k-1})^{2-\mu_2}, (u_i^{k-1})^{\mu_2}] \tag{3}$$

If a user does not generate any report during a particular time epoch, it will carry forward the existing opinion vector to the future epochs.

After each update, the measures are normalized such that they sum up to 1. Finally, the expectation on report j can be derived by considering the probability expectation value of its opinion as follows [Jøsang 1999]:

$$\varepsilon\{\theta_{i,j}^k\} = \frac{b + u}{b + d + 2u} \tag{4}$$

4.2 Truthfulness of a User Contribution

The opinion vector derived on the basis of MSA feedbacks is one of the important components to determine the truthfulness of a user contribution. However, as the MSA cannot validate the reports in all regions and at all time-epochs, we also need to determine if the user is exercising any side-channel participation. The veracity of the user location can be determined by the distance

bounding method. It computes the spatial distance between the event location (given by the GPS values in the report) and the participant's spatial coordinates retrieved from the access points [He et al. 2011]. These access points are the interfaces through which the PS sub-system communicates with cellular tower data driver[5]. We model the problem similar to a weighted regression approach where the *expectation from the opinion about a report* and the *spatial distance* are the predictor variables, and truthfulness is a dependent variable. Thus, if w_o and w_s are the coefficients (or weights) of expectation from the opinion and spatial distance, respectively, the truthfulness for any report j, generated by user i at time epoch k will be given as:

$$\tau_{i,j}^k = w_o.\varepsilon\{\theta_{i,j}^k\} + w_s.\sqrt{||g_{i,j}^k - c_{i,j}^k||^2} \tag{5}$$

where, $||g_{i,j}^k - c_{i,j}^k||^2$ is squared L2-norm to compute the distance between the GPS-based location $g_{i,j}^k$ and the cellular tower-based location $c_{i,j}^k$, while user i generated report j at epoch k. The L2-norm function is given by the Euclidean[6] distance between two points $p = (x_1, y_1)$ and $q = (x_2, y_2)$ as:

$$||p - q||^2 = (x_2 - x_1)^2 + (y_2 - y_1)^2 \tag{6}$$

For the convenience of representation, we use $\delta_{i,j}^k = \sqrt{||g_{i,j}^k - c_{i,j}^k||^2}$ and express Eqn.(5) as:

$$\tau_{i,j}^k = w_o.\varepsilon\{\theta_{i,j}^k\} + w_s.\delta_{i,j}^k \tag{7}$$

The spatial distance between two locations can take up any value from the real domain, thus making the expected truthfulness unbounded. In order to ensure that the value of truthfulness lies within the interval [0, 1], the distance factor in Eqn.(7) needs to be normalized. We consider δ_{max} to be the maximum tolerable distance between the location of the event and that of the nearest cellular tower using which the participant has sent the report. Thus, the modified expression for expected truthfulness is as follows:

$$\tau_{i,j}^k = w_o.\varepsilon\{\theta_{i,j}^k\} + w_s.\frac{\delta_{i,j}^k}{\delta_{max}} \tag{8}$$

It is evident from Eqn. (8) that if a user is reporting from a location which is nearer to the cellular tower, then $\delta_{i,j}^k$ will be low. Further, on normalization by δ_{max}, the expected truthfulness will be further reduced and this is a contradiction to our notion of *side-channel participation*. Therefore, to prevent higher truthfulness on location-spoofed reports, we further modify the expression as follows:

$$\tau_{i,j}^k = \begin{cases} w_o.\varepsilon\{\theta_{i,j}^k\} + \beta(j).w_s.(1 - \frac{\delta_{i,j}^k}{\delta_{max}+\epsilon}), & \text{if } \delta_{i,j}^k \leq \delta_{max} \\ w_o.\varepsilon\{\theta_{i,j}^k\}, & \text{Otherwise} \end{cases} \tag{9}$$

We introduce $\epsilon \ll \delta_{max}$ to handle the boundary case where $\delta_{i,j}^k = \delta_{max}$. The binary function $\beta(j)$ returns 1 if the report j is either verified to be true (by the MSA) or considered undecided due to the absence of MSAs. However, for false contributions, the function will return 0 and nullify the impact of the location veracity. The second condition of Eqn. (9) shows that the effect of the location veracity is also invalidated if the distance between the event site (as obtained from the GPS value) and the nearest cellular tower location is greater than the maximum tolerable distance.

[5]https://security.stackexchange.com/questions/65181/how-do-location-based-apps-avoid-getting-cheated-by-emulated-gps

[6]Assuming the UTM coordinates, otherwise Haversine formula can be used.

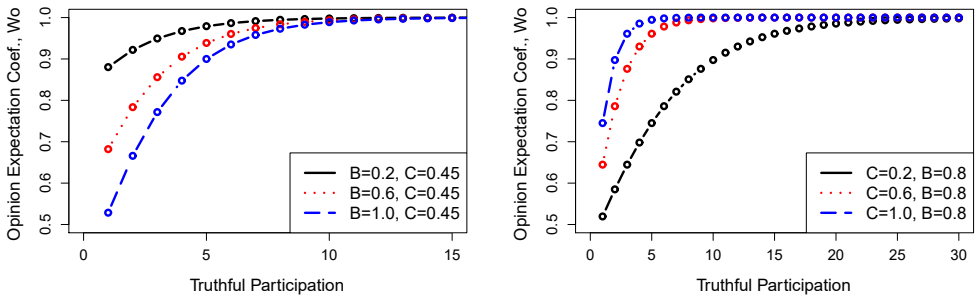
4.2.1 Estimation of Opinion Expectation Coefficient. Besides the expectation from an opinion about report j, truthfulness should also consider the quality of prior participation for its acceptance. This is essential as the PS sub-system must reward users with a higher degree of quality participation. In practice, a user does not have a high reputation at the initial stage. It takes considerable time and a fairly large number of positive interactions to build a good reputation. This resembles some social aspects where the trust depends on factors, such as friendship duration, the number, and frequency of interactions, and so on.

Similarly, if a user frequently interacts with the PS sub-system by submitting truthful information, a trust relationship gets rapidly developed. Such relationship plays a pivotal role in scenarios where the PS system cannot verify the correctness of reports due to unavailability of MSAs at certain sensing regions. Users with a higher degree of truthful participation are expected to submit true information than the ones with sporadic contributions. Hence, the coefficient of opinion expectation should take this notion into consideration.

As mentioned in Section 2.2.1, the *Gompertz* function dynamically reflects the changes in the user's behavior along with different participation. Mimicking the reputation building process in real life, the initial value grows slowly during the gestation period, followed by the period of growth and then reaching to the points of steady state. Such behavior is reflective of trust build-up in multi-user systems like PS applications. The weight w_o will give higher weight to the opinion if the contributor has a higher number of previous truthful participation. This motivates us to model w_o in terms of the Gompertz function:

$$w_o = A \cdot e^{-Be^{-C(\phi_i - \varphi_i)}} \tag{10}$$

where, A is the upper asymptote which decides the maximum value the output can attend, B is positive constant which controls the displacement of the reputation score, C adjusts the growth rate. The input functions ϕ_i and φ_i denote respectively, the frequencies of previous truthful and untruthful interactions of user i. The factor $(\phi_i - \varphi_i)$ penalizes deceptive behavior and reduces the trust developed upon the participant i through prior contributions. Untruthful interactions are determined from the MSA endorsements and location spoofing evidences.



(a) Displacement Parameter, B (b) Growth Parameter, C

Fig. 4. Parameters for w_o

Parameter recommendations for w_o (A, B, C): The upper asymptote A determines the maximum value which the coefficient w_o can attain. Since the expected truthfulness of a contribution lies within the interval $[0, 1]$, the maximum value is $w_o = 1$. Thus, we fixed the value as $A = 1$.

Fig. 4(a) illustrates the effect of B on the initial values of w_o before the latter enters into the exponential phase. This parameter is used to remove uncertainties due to varying participation

behaviors. For example, a user who has contributed with all true reports during first few participations yields a higher trust which implicitly reduces uncertainty. Thus, B can be set to a lower value to make w_o start from a high value. Conversely, if any participant has generated false reports or a mixture of true/false reports, the PS system will be skeptical regarding the quality of his future contributions and can assign a larger B to prevent w_o from attaining higher values at a smaller number of truthful participation.

Fig. 4(b) shows the effect of C that regulates the rate of growth of w_o with respect to the number of truthful participation. As evident, the lower the value of C, the higher is the number of true contributions expected from a user. For example, if any user has a history of generating false reports, then C should be small such that w_o attains highest value only after adequate truthful reports are received. However, if the VCPS system is non-restrictive, it can diminish the value of C. Conversely, for genuine participants, the PS sub-system can afford to maintain a higher C.

4.2.2 Estimation of Spatial Distance Coefficient. As evident from Eqn. (7), the normalized spatial distance factor has an inverse effect on the overall truthfulness of the contribution. The larger the spatial distance between the two points, the higher will the conviction of a potential side-channel participation. Consequently, the confidence on the contribution will be reduced. Thus, the coefficient needs to be modeled in such a way that it gives higher weight to smaller spatial distances and vice-versa. For the smallest distance, we must have maximum confidence which should persist until the distance remains relatively low. However, as the distance gradually increases, the confidence should also amortize and diminish once the former attains a very high value. The following equation models the spatial distance coefficient in the light of the above arguments:

$$w_s = \begin{cases} 1 - e^{-\frac{\lambda}{\frac{\delta^k_{i,j}}{\delta_{max}+\epsilon}}}, & \text{if } 0 < \frac{\delta^k_{i,j}}{\delta_{max}+\epsilon} < 1 \\ 1, & \text{if } \frac{\delta^k_{i,j}}{\delta_{max}+\epsilon} = 0 \\ 0, & \text{if } \frac{\delta^k_{i,j}}{\delta_{max}+\epsilon} > 1 \end{cases} \tag{11}$$

where, $0 < \lambda < 1$ is the decay rate which needs to be tuned to accommodate different participating behaviors.

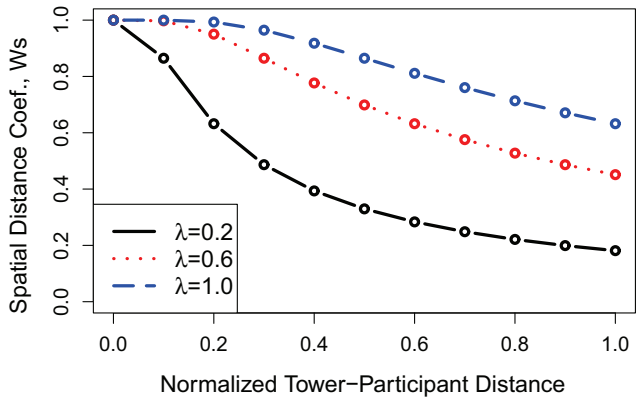


Fig. 5. Decay Parameter for w_s: λ

Parameter recommendations for w_s (λ): Fig. 5 shows the effect of λ that controls the decay of w_s with respect to the normalized distance between the cellular base station and the participant. In general, if the participant's report contains an event location that is close to a base station, the PS sub-system tends to give the benefit of the doubt and believes that there may not be any location spoofing attempt, resulting in a higher w_s. In contrast, if the distance increases, the perception of risk magnifies as the possibility of location spoofing attack looms large. Hence, a higher λ may be set for a participant from whom the system frequently finds the mismatch in reported event location and the site of the closest base station. For predominantly honest contributors, λ can be low to restrict rapid decay of trust.

4.3 Quality of a Contribution

Eqn. (9) defines $\tau_{i,j}^k$ as the expected truthfulness on a report j, contributed by user i at time epoch k. Now, the system needs to perform a regression to determine the odds of the contribution j being true or false, which we model as the *quality of contribution (QoC)*. Although the MSAs are deployed to get reliable feedbacks, there still exists uncertainty due to the absence of MSA from a sensing region under contention, and side-channel participation of the user. We have used the *generalized linear models (GLM)* for mapping the truthfulness value to QoC. If $Q_{i,j}^k$ is the QoC of the report j generated by participant i in time epoch k, then we use the *logit* function to establish a link between it and $\tau_{i,j}^k$ [Bhattacharjee et al. 2017a]:

$$Q_{i,j}^k = \ln\left(\frac{\tau_{i,j}^k}{1-\tau_{i,j}^k}\right) \tag{12}$$

Note that $Q_{i,j}^k$ has value in the interval $[-\infty, +\infty]$. The logit function gives monotonically decreasing weights to all $\tau_{i,j}^k < 0.5$, and monotonically increasing ones to the rest.

4.4 User Reputation

The QoCs of the reports generated by a participant (or user) are aggregated to generate a raw reputation score. For the most general case, if the participant i has generated n reports at a particular time epoch k, we aggregate the QoCs of reports (each given by $Q_{i,j}^k$) to derive an updated reputation score till the current time, say T^{th} time epoch. Thus:

$$R_i^T = \sum_{k=1}^{T}\sum_{j=1}^{n} Q_{i,j}^k \cdot P(i,j,k) \tag{13}$$

where,

$$P(i,j,k) = \begin{cases} 1, & \text{If user } i \text{ generated report } j \text{ at epoch } k \\ 0, & \text{Otherwise} \end{cases} \tag{14}$$

4.5 Normalized Reputation

The aggregated reputation score R_i^T obtained from Eqn. (13) can have any value in the interval $[-\infty, +\infty]$. In order to give a bound to it, we use a scaling function which converts the raw R_i^T score into a normalized score $\rho_i^T \in [-1, +1]$, given as:

$$\rho_i^T = \begin{cases} 1 - e^{-\alpha|R_i^T|}, & \text{if } R_i^T > 0 \\ -(1 - e^{-\alpha|R_i^T|}), & \text{if } R_i^T < 0 \\ 0, & \text{if } R_i^T = 0 \end{cases} \tag{15}$$

Here $0 < \alpha \ll 1$ is the parameter to control the rate of growth of the reputation score within [-1, +1].

5 APPLICATION OF THE REPUTATION SCORE: DECISION MODEL

The *SAFE* framework so far was committed to forming a base of reasonably genuine users by computing their QoC with the help of MSA feedbacks and location veracity. The truthfulness of the published information was dependent on the endorsements made by the MSAs. However, once the framework builds a pool of users with a good reputation scores, the information publishing step itself could be automated, without MSA interventions. In this section, we show how the *SAFE* framework can be applied to infer true events and support dependable decisions for publication of 'event'. As discussed in Section 3, the PS sub-system in the VCPS may receive reports that indicate an event type belonging to $\mathbb{Z}$ from a prospective event boundary, say r. Ideally, we should only be relying on the reports from those users, who have $\rho_i > 0$ (the genuine participants) and currently present within the boundary r. However, there are following possibilities which make the decision process non-trivial in the absence of the ground-truth.

First, different types of event reports can be received within the given event boundary r, which may be relevant or irrelevant in reality. Human perception difference might be the reason for reporting of irrelevant event report by a genuine user. Moreover, due to lack of previous interactions, handling new users (without any reputation score) may be a difficult proposition. Additionally, the rare event's true report may not be considered as genuine reporting based on prior, if malicious users can successfully manipulate and report more likely event falsely.

Mistakes in decision making and publishing fake events or dropping true events may result in the wasteful expenditure on incentives to the malicious users. Wrong decision also decreases the reliability of the overlall participatory *VCPS* application. This entails that even if the reports suggesting two or more event types may be received from the boundary r at the same time epoch, it has to be decided at runtime which among them is most likely to be accurate. To address these challenges, we propose a simplified two-level decision model as presented below, which is inspired by our previous work [Bhattacharjee et al. 2019]. Here, we proposed a *Prospect theory*-based decision model which is complex and needs to handle multiple parameters. In contrast, this work presents a simpler model based on *Expected utility* theory.

5.1 Two-Level Model

In simplified two-level decision-making model, there are two steps. First level, namely $D1$, filters the one most probable event among the several reported event and decides *which* event to publish. Whereas, second level, namely $D2$, decides *whether* there is a sufficient evidences in support of the filtered out event from the decision level $D1$. A schematic representation of the two-level decision-making model is depicted in Fig. 6.

The first level decision is necessitated if the PS sub-system of the participatory *VCPS* receives reports of multiple types of events for the same spatio-temporal window. This could be either due to a legitimate wrong perception or a mixture of rogue and honest observations. Note that, even if prior reputation scores are used to ignore reports from very low reputation users, there is still a possibility of zero-day attacks in which devices of some of the participants may be compromised in the current time epoch. Therefore, it is imperative to decide the most likely event type among the set of reported events. The requirement of decision making in the near real-time boundary poses non-trivial challenge.

The second level decision is postulated by the fact that even if we got the most probable event type, there may be insufficient evidences in support of its occurrence. For example, in a situation where reports notifying different event types have been received in similar proportions, it implies that

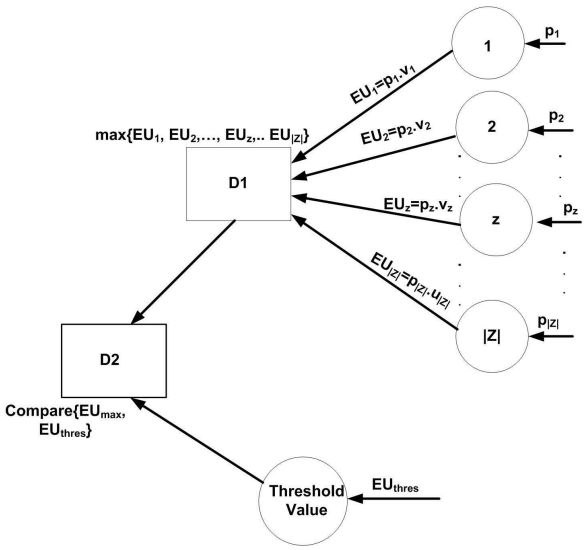


Fig. 6. Two-level Decision Model

the participants are themselves uncertain about the actual event, which tilts the odds towards not publishing anything. Depending on the *VCPS's* risk policy, *avoiding a false event may sometimes come at the expense of not publishing true events*. Nevertheless, in vehicular domain, the non-publication of a true event has much less impact in comparison to publication of a false event. This is owing to the fact that the latter causes unnecessary inconvenience for commuters at multiple locations and thus results in decrease in the reliability of the system. Thus, the objective of a two-level decision process will be to avoid publishing false events, while maximizing successful publishing of true events.

We have adopted an *Expected Utility Theory (EUT)*-based approach to compute a value for each reported event types (which are outcomes in this context). This value is based on the available pieces of evidence (viz., the number of supporting reports, aggregated reputation score of the reporters) received in the current time epoch, and essentially measures the confidence of the PS sub-system on the occurrence of a particular event type. The values of each event type are further weighed by their prior likelihood of occurrences to generate corresponding expected utilities. In the next section, we present the mathematical formulations to the utility and the value functions.

5.1.1 Expected Utility on Event Types. Expected Utility Theory (EUT) [Mongin 1997] gives a measure of the utility to be achieved by playing an n-outcome risky prospect $g = \{p_1, x_1; \ldots; p_n, x_n\}$, where p_i is the likelihood of receiving outcome x_i, and x_i's are in descending order of attractiveness. The expected utility function is given as:

$$EU_g = \sum_{i=1}^{n} p_i.v(x_i) \tag{16}$$

where, $v(x_i)$ is monotonic value function and p_i is the outcome probability.

However, in the context of deciding whether or not to publish the traffic events, two subtle differences exist compared to the above mentioned expected utility function: (i) unlike the outcomes (x_i) in EUT, the outcomes (e.g., jam, accident, etc.) in our case are unordered, and (ii) the outcomes are independent and mutually exclusive of one another. There may exist location-specific correlations between different event types, but their generalization is beyond our scope. Thus, the n-outcome

risky prospect is reduced to *one-outcome* prospect, viz., whether a jam has occurred or not, whether an accident has occurred or not, and so on.

As mentioned in Section 3.1, $\mathbb{Z}$ is the set of all traffic event types for which the reports can be generated. Then for any event type $z \in \mathbb{Z}$, if its evidences generate a value v_z, then the one-outcome expected utility function is given as:

$$EU_z = p_z.v_z \tag{17}$$

where, p_z denotes the prior likelihood of occurrence of event type z in a given sensing region and at a particular time epoch. Such prior likelihood value can be considered as the ground truth which changes over time. It provides additional support for the belief that a particular incident has occurred or not.

5.1.2 Value Function. The PS sub-system, due to its prior interactions with the users in any event boundary r, generates reputation score for each of them based on the quantity and quality of their contributions. For any event type, the available evidences are the *number of supporting reports* and the *aggregated reputation scores of the participants*. Thus, for a particular event type $z \in \mathbb{Z}$, the corresponding number of reports N_z and the aggregated reputation score $\mathcal{R}_z$ form the current pieces of evidence, and $\frac{N_z}{\sum_{\forall z \in \mathbb{Z}} N_z}$ and $\frac{\mathcal{R}_z}{\sum_{\forall z \in \mathbb{Z}} \mathcal{R}_z}$ are the measures of the event type's relative support and trustworthiness, respectively [Bhattacharjee et al. 2019].

We use a weighted regression approach to model the overall value (v_z) gained from the evidences in support of the event type z. It is expressed as a weighted sum of support and trustworthiness and is given as:

$$v_z = \gamma . \frac{N_z}{\sum_{\forall z \in \mathbb{Z}} N_z} + (1 - \gamma) . \frac{\mathcal{R}_z}{\sum_{\forall z \in \mathbb{Z}} \mathcal{R}_z} \tag{18}$$

where, $0 \leq \gamma \leq 1$ is the preference factor which the PS administrator assigns to two evidence types. Such preferences are controlled by the context-sensitive inputs such as the location, temporal biases, and other such information. For instance, if an event report received from a historically crowded spatiotemporal window, the PS system may assign more weight to the support (reports). However, for the sparse spatiotemporal window, when and where participation is expected to be low, more emphasis will be given to the trustworthiness (reputation). Finally, we compute the expected utility EU_z of event type z by using Eqn.(17).

5.1.3 Decision Level D1. In the decision-level $D1$, we search for a reported event which has the maximum utility value. The event with such maximum value is declared as the winner from this level and qualifies for decision-level $D2$. However, in the case of contradiction between two or more different event types, when they have the same utility value, all the events are discarded as the uncertainty in decision making process is not resolved. Formally, the first level decision process is defined as:

$$D1 = \begin{cases} \text{Select } z, & \text{iff } EU_{max} = EU_z \\ \text{No } z \text{ is selected}, & \text{Otherwise} \end{cases} \tag{19}$$

5.1.4 Decision Level D2. The decision-level $D2$ gets invoked only based on the positive output from $D1$. If an event type is getting qualified at decision-level $D1$, the same is passed to $D2$ to check its utility value in comparison to a pre-defined threshold. The final decision for publishing the event or dropping the same gets guided by the Eqn.(20).

$$D2 = \begin{cases} \text{Publish } z, & \text{if } EU_{max} \geq EU_{thres} \\ \text{Drop } z, & \text{Otherwise} \end{cases} \tag{20}$$

Choosing an appropriate EU_{thres} is subjective and also application-specific, but it should never be fixed at any absolute value. Low values can result in publishing either rogue events (generated by dishonest users), or events whose veracity cannot be determined due to the lack of sufficient evidences. Similarly, higher EU_{thres} will drop most of the events whose evidences are not significant.

It is to be understood that EU_{thres} is also a utility similar to that for different event types, and it will vary with different decision-making tasks rendered at other time epochs. The variation is due to the evidences, based on which the utility is estimated, and will most often be different at different time epochs.

One possible evidence-aware heuristic is to set up EU_{thres} as a significant fraction/percentage of the sum of the utilities for all event types estimated at the current time epoch. This ensures that the winner event type will only be published if its utility forms the majority share of the sum of current utilities. Thus, if the PS administrator sets y as the threshold percentage, then EU_{thres} will be given as:

$$EU_{thres} = \frac{y}{100} \times \sum_{z \in \mathbb{Z}} EU_z \tag{21}$$

6 PERFORMANCE EVALUATION

The primary objective of the proposed *SAFE* framework is to ensure that the users in the VCPS are segregated based on the quality of their participation. Such segregation will enable prevention of information falsification attacks. The efficacy of this framework has been extensively studied through the development of a customized simulator (details explained in Section 6.1) using the *R-tools*[7]. Both synthetic as well as real data have been used to evaluate the performance of the proposed framework. The data considered for experimentation consist of a large number of mobility traces of the participating vehicles, MSAs, randomly generated events, and the locations of fixed cellular towers.

6.1 Simulation Settings

We have implemented the random waypoint mobility model to replicate the movement of the participating vehicles. The experiment has been divided into two parts. In the first part, we study the performance of *SAFE* framework in classifying genuine and dishonest participants based on dynamic reputation. The performance has been evaluated using both synthetic and real datasets. The second part studied the performance of the decision-making model using *SAFE*-generated reputation scores to support publishing or dropping of the events under contention.

Table 2 presents the basic simulation and system parameters used for experimental purpose. For synthetic dataset, we generated randomly distributed cellular base-stations (having a sensing radius of $30km$) across the simulation area and stored their coordinates in a file for finding out the normalized distance between the participants and their nearest base-station. Under the normal situation, a participant's report has been taken into account only if its location is within the sensing range of the base station. We followed the distribution function proposed in [Barnwal et al. 2018] for random event generation across different regions of the simulation area. After an event gets generated at a particular location, we construct a circular boundary around that point with a fixed radius of $2km$.

Each experiment has been performed with 100-500 participants, and to minimize random effects, results are obtained by taking the average. The optimal values for distrust rates μ_1 and μ_2, at which minimal fluctuation of reputation occurs are empirically determined. It has been found that μ_1 and μ_2 give reasonably smooth reputation profiles at 0.2 and 0.8, respectively. The simulations have

[7] https://www.rstudio.com/

Table 2. Basic Simulation Parameters

Parameter	Value
Simulation Area (km^2)	150 x 150
Number of Participants	100-500
MSAs (in %)	5-25
Node's Min Speed (km/time epoch)	20
Node's Max Speed (km/time epoch)	100
Pause Time between Trips (in time epoch)	10
Communication range of Base-station (km)	50
Simulation Time (in time epochs)	100
Distrust rate (μ_1, μ_2)	0.2, 0.8
Maximum asymptote for w_o, A	1
Displacement factor for w_o, B	0.8
Growth rate for w_o (C)	0.45
Decay rate for w_s (λ)	0.2
Growth rate for ρ (α)	0.01

been conducted assuming time epoch as a unit for discrete experimentation. If two or more reports are generated during a particular time epoch and within the same event boundary, then they are considered for the same event instance. The size of the time epoch in real implementation may vary based on the historical data.

To simulate the spoofing activity, we induced the event report submissions by those participants who are not within the communication range of any of the base-stations presents within the event boundary. During the experiments, we fixed the percentage of the total participants who can be the spoofers. Further, to simulate false contributors, some of the participants within the communication range of the base-stations near the site of the event have been selected randomly with a predefined probability and replaced their event reports with the false one.

6.2 Reputation-aware User Profiling

One of the primary objectives of the *SAFE* framework is to profile a user based on the reputation computed from his participating behavior. To study different user profiles created by the framework, we maintain the reputations of users generated overall time epochs. Fig. 7 shows that with time, *SAFE* is able to identify six different user profiles based on their nature of participation. We consider the score 0 to be a neutral reputation, i.e., the reputation of newly registered participants. The profiles of the participating users are identified as follows:

1) Earlier Spoofing then Genuine Reporting (ESTG): In this behavior profile, the participant spoofed his location in the initial few contributions, then started generating true reports. This is reflected in the reputation score, which dropped to low values owing to spoofing and then gradually increased with a higher number of true participation.

2) Sometimes True Sometimes False (STSF): This type of participant launches *on-off* attacks by intermittently generating true and false reports with certain probabilities. The average reputation score of these participants never attained positive value which implies that *SAFE* is robust against *on-off* attacks.

3) Always Spoofing with True/False Reporting (ASTF): Such participant always spoofs his locations and occasionally succeed in generating reports for true events. The average reputation score of this class of users is low although their contributions are true. However, since they exercised proxy participation, our framework penalized them.

4) Always True but Lower Participation (ALTP): These users are honest but their contribution to the

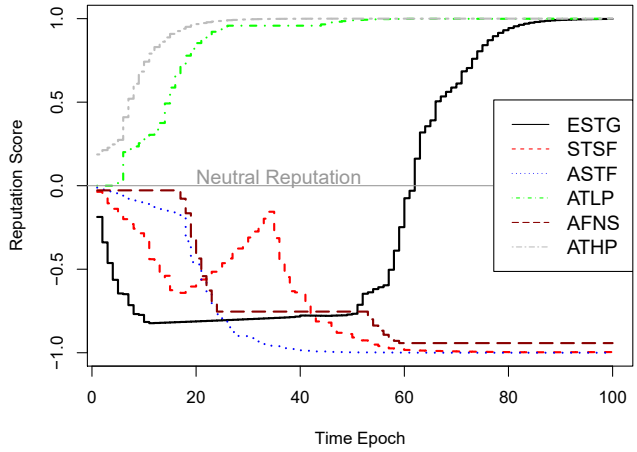


Fig. 7. User Profiles based on their Reputation

PS sub-system is sporadic. Such users end up with good reputation score, but not as high as the ones who have a higher degree of participation.

5) Always False but Not Spoofing (AFNS): Such participants always lie and generate fake reports. But they do not spoof to camouflage their locations. The average reputation score of this profile gradually decreases over time.

6) Always True with Higher Participation (ATHP): The participants belonging to this profile are genuine and also contribute persistently. The average reputation scores of these users are on the higher side compared to the ALTP profile.

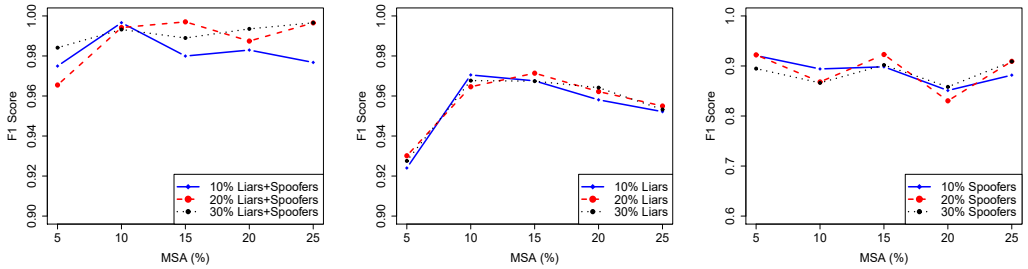
6.3 Effect of MSAs on User Classification

This section studies the effect of increasing the number of mobile security agents (MSAs) on user classification in presence of varying fractions (10%, 20%, and 30%) of different forms of rogue participations. The objective here is to study the optimal percentage of MSAs that are sufficient to achieve higher classification accuracy with less false positives and false negatives at the end of the simulation time. Since we measure and compare the performance of the *SAFE* framework in terms of the classification accuracy, we use the widely accepted *F1-score* [Fawcett 2006] as the metric. The *F1-score* is a balanced measure of *precision* and *recall*, where a score of 1 and 0 imply best and worst classification performances, respectively. It can be expressed in terms of *precision* and *recall* by their harmonic means as:

$$F1\ score = 2 * \frac{precision * recall}{precision + recall} \tag{22}$$

where, $precision = \frac{TruePositive}{TruePositive+FalsePositive}$ and $recall = \frac{TruePositive}{TruePositive+FalseNegative}$.

For experiments, we randomly choose 10%, 20% and 30% of participants as rogue at a time, and make them contribute false and spoofed reports with probability 1. The objective here is to find out the effect of MSA percentage on the segregation of true report contributors among the total reporters comprising of honest, liars and spoofers. The general notion is that if the number of MSAs increases in the sensing regions, the detection rate of false contribution will also improve considerably. However, we observed that this may not always be true as depicted in Fig. 8.



(a) Liar + Spoofer (b) Liar (c) Spoofer

Fig. 8. Classification Performance w.r.t Varying Proportions of MSAs

Fig. 8 shows the *F1-score* for gradually increasing fractions of MSAs. From the plots, we observe an interesting fact that on some occasions, with the increase in the percentage of MSA, the *F1-score* gets affected in an adverse manner. This appears counter-intuitive. A possible reason behind this behavior is that the mobility of MSAs is independent of that of the participants. An increase in the MSA's percentage means there is comparatively fewer participants in each area of interest, whose reputation needs to be adjudged. This phenomenon may be referred to as the *saturation effect*. Since the time of simulation is fixed during our experiments, the participation frequencies of all users (honest, liars and spoofers) are also limited. As a result, the number of rogue participations is also on the lower side, and thus it remains undetected over the simulation window. However, it has been observed that if we run the simulation for longer durations, the *F1-score* improves with the increasing percentage of MSAs. Hence, there is a trade-off between the malicious-participant detection time and its accuracy.

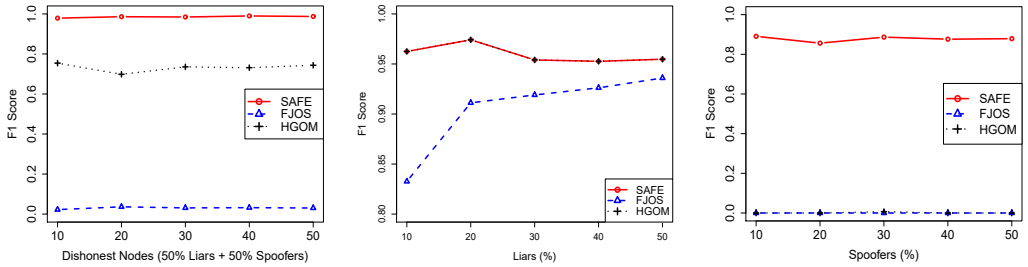
Figs. 8(a) and 8(b) demonstrate that for different fractions of liars, the *F1-score* is optimal when the number of MSAs constitutes 10% of all participants in the present simulation setup. For other MSA percentages, the performance was not stable. However, the optimal percentage of MSAs may vary depending on the size of the simulation area to provide a sufficient shield for each sensing region. Thus, to study the effect of other parameters, we have taken the optimal percentage of MSAs as 10% of total population for the rest of the experiments.

The above experiment has been further conducted with different proportions of spoofer participants, with the probability of spoofing being 1. We randomly selected those participants as spoofers, who are presently not within the communication range of base-station at the event location. Fig. 8(c) shows that the MSA percentage does not significantly affect the classification performance if only the spoofers constitute the rogue participants. Except for some random effects, the result is more or less constant for varying proportions of MSAs. This is intuitive because, in the *SAFE* framework, MSAs do not validate if any report is generated by spoofing the location of an event.

6.4 Effect of Rogue Participation on User Classification

In this section, we evaluate the performance of *SAFE* and compare its user classification performance with two state-of-the-art reputation models proposed for participatory sensing paradigm: (i) Jøsang's opinion and trust model-based *FIDES* system [Restuccia and Das 2014], referred to as *FJOS*, and (ii) *Gompertz* function-based model [Huang et al. 2010] [Huang et al. 2014], which we refer to as *HGOM*.

Fig. 9(a) shows the classification accuracy of three methods when dishonest participants are present as both liars and spoofers. Clearly, *SAFE* yields maximum accuracy even if the rogue users sum up to 50% of the total contributors. The Gompertz function-based *HGOM* achieved an *F1-score* of 0.75 but mostly failed to capture the spoofing behavior. On the contrary, the performance of



(a) Liar + Spoofer (b) Liar (c) Spoofer

Fig. 9. Classification of Participants in presence of Rogue Contributions

FJOS is poor due to its failure in classifying the spoofing behavior. Additionally, *FJOS* cannot penalize those contributions which are not endorsed by the MSAs, or if the liar is generating false reports intermittently.

In Fig. 9(b), we depict the performances of the methods in the presence of only liars. Interestingly, the accuracies achieved by both *SAFE* and *HGOM* are comparable for varying proportion of lying participants. The performance of *FJOS* has considerably improved due to its capability of identifying liars with the help of MSAs. However, it suffers from the lack of consideration of previous participation behaviors while assessing reports currently not validated by the MSAs.

In a situation where spoofers are the primary rogue contributors, *SAFE* comprehensively outperforms the other two methods (refer to Fig. 9(c)). The reason is that neither *HGOM* nor *FJOS* has the provision to detect location faking attacks and they consider all such contributions to be genuine. Conversely, our *SAFE* framework succeeds in achieving *F1-score* of 0.9. This reflects the balance between high precision and recall in accurately classifying spoofed and genuine participation.

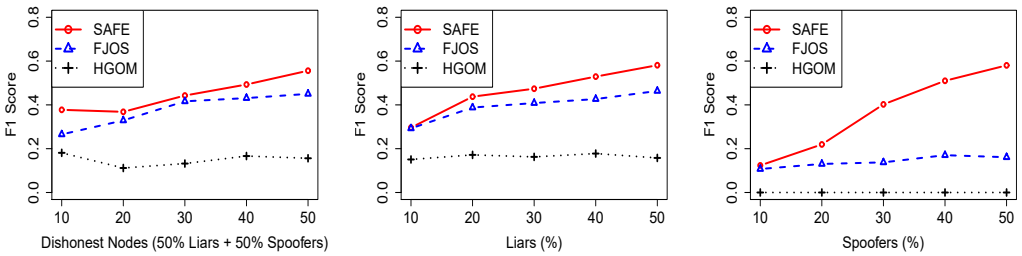
6.5 Evaluation of SAFE with Real Data

We have used the real dataset publicly available in the *CRAWDAD* archive [8] for extensive evaluation of the *SAFE* framework. The dataset consists of a smartphone app-generated GPS traces of 289 taxicabs across different regions of Rome, collected during the period *01-Feb-2014* to *04-Feb-2014*. The data has been collected for the purpose of research on participatory sensing [Alswailim et al. 2016]. To realize the data generated by participatory sensing, the taxicabs are equipped with peripheral temperature sensors, and while moving the taxi collects timestamped temperature of its current location.

For our experiment, we divided the city area of $22.5km \times 22.5km$ into nine sensing regions (each of $7.5km \times 7.5km$) and simulated a cellular base-station at the center of each region. The sensing time of the temperature report has been discretized into four temporal bins per day, each bin being six hours duration. We generate a temperature value for every active taxicab in a certain temporal bin by applying Gaussian distribution. The mean temperature at a particular region and during a given temporal bin has been considered as the ground truth. The taxicabs have been configured to generate temperature values with the random Gaussian error of 10% on either side of the mean. If the value is generated within this range, we considered that the contribution is true, otherwise false. For convenience, we discretized the real value with 0 and 1, depending on if the contribution is false or true, respectively. Some of the randomly selected taxi cabs have been designated as the MSAs, who always contribute true temperature readings of the regions through which they travel. Rest of the taxicabs have been divided into honest (50%), liar (25%), and spoofers (25%) which respectively generate true, false, and spoofed values depending upon their predefined rates.

[8] https://crawdad.org/queensu/crowd_temperature/20151120/

Below we present the performance of the three methods in terms of the *F1-score*. It is worth noting that the accuracy obtained with the help of real dataset is on the lower side, compared to the synthetic data. This can be attributed to the fact that the mobility model considered in the implementation of our framework is the random waypoint, while in the real dataset it is modeled by the trajectories of the participating vehicles.



(a) Liar + Spoofer (b) Liar (c) Spoofer

Fig. 10. Classification of Participants in the Presence of Rogue Contributions (Using Real Data)

Fig. 10(a) shows the classification accuracy of the three methods when both liars and spoofers are present. Although the *F1-score* is on the lower side, it is evident that *SAFE* yields the highest accuracy, with gradual improvement in performance as the percentage of rogue users increases. Interestingly, with the real data *FJOS* performed better than *HGOM*, but both ended up with low *F1-score* as they cannot penalize spoofed reports.

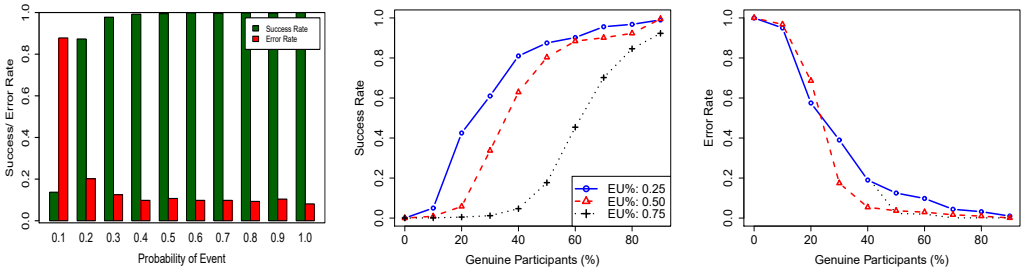
Fig. 10(b) presents the performance of the methods in the presence of only liars. It is worth noting that unlike Fig. 9(b), *FJOS* again outperforms *HGOM* by a significant margin as it can identify liars based on the MSA feedbacks. Nevertheless, *SAFE* outperforms *FJOS* under different proportions of lying participants due to better penalization scheme for contributions not endorsed by the MSAs.

SAFE comprehensively outperforms *FJOS* and *HGOM* (refer to Fig. 10(c)) if the rogue participants are only spoofers. The reason is that neither *HGOM* nor *FJOS* has the provision to detect the location faking attacks and they consider all such contributions to be genuine.

6.6 Decision Making Accuracy

In the decision model, our objective is to show how the PS sub-system makes trustworthy decisions, and thus ensures better operational accuracy through the publishing of only true events. We measure the performance of the EUT-based decision model by means of the following metric: (i) *Success rate:* It is the proportion of the total *true events* which gets successfully published after passing through the two levels of decision-making module, and (ii) *Error rate:* It is the proportion of the total *true events* which get dropped due to either of the decision level mechanism. The aim of the proposed two-level decision-making model is to inhibit the publication of false events and successfully publish the potential true events (rare or frequent) for the benefit of the participants. Unless otherwise mentioned, the values of the parameters considered for evaluating the decision model are: $\gamma = 0.5$, and $EU_{thres} = 50\%$ of the sum of the utilities.

Publishing True Events: Fig. 11(a) shows the success and error rates in publishing true events with increasing prior likelihoods of occurrence (p_z). For very rare events (i.e., $p_z < 0.2$), the proposed decision model fails to publish the majority of them, yielding a significantly high error rate. This is because, low likelihood reduces the overall expected utilities of the rare events, thus disqualifying them in the second level of the decision making. In contrast, as the prior likelihood of events becomes greater than 0.2, the success rate increases many-folds and attains the near-maximum

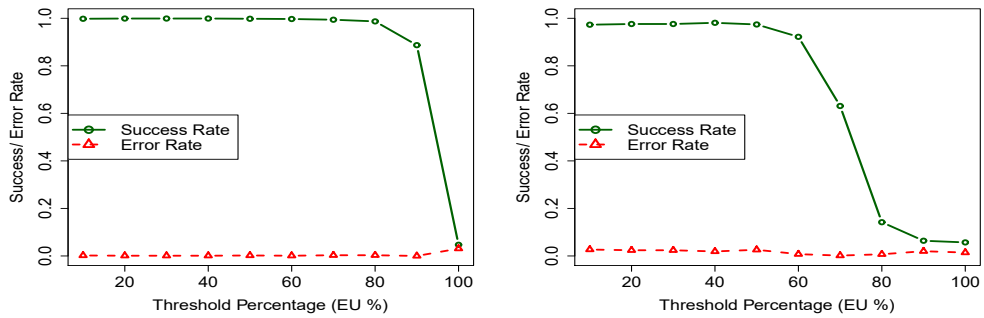


(a) Success/Error Rates vs p_z (b) Succ. Rate vs % Genuine Participation (c) Error Rate vs % Genuine Participation

Fig. 11. Performance of EUT-based Decision Model

value for all events with a likelihood of occurrence greater than 0.4. As the likelihood of occurrence increases, even with a moderate confidence value, the expected utility also increases and surpasses the threshold. This ensures that relatively frequent true events will not remain unpublished.

Success/Error Rates vs % of Genuine Participation: As mentioned earlier, the *SAFE* framework segregates genuine participants from dishonest ones by means of reputation scores. However, in practice, these genuine participants may get subverted at the current time epoch (zero-day attack) or wrongly perceive a true event. Thus, we vary the percentages of genuine participation to study the performances of the decision model (refer to Figs. 11(b) and 11(c)). It is evident that for low EU thresholds (0.25 and 0.50), the success rate increases rapidly even if the fraction of genuine participation is on the lower side. This is intuitive, as low threshold entails a non-restrictive PS sub-system that allows the events to easily qualify decision level *D2* even with the smaller confidence value. However, with a smaller fraction of genuine participation, the higher success rate is not always guaranteed as potential sabotaging can be achieved. Conversely, the conservative system expects significant support from the participants to make publish/drop decisions and uses higher EU_{thres}. It is noted that the error rates for all thresholds are very high at low participation. This is due to not allowing the true events (which has yielded relatively lesser confidence values) to get published. However, the error rates gradually decrease as the higher number of genuine participants starts contributing. Thus, the choice of EU_{thres} is subjective to the VCPS and it depends upon whether it is risk-seeking (liberal) or risk-averse (conservative).



(a) Frequent Event (b) Rare Event

Fig. 12. Effect of EUT Threshold (Genuine Participation = 85%)

Effect of EUT Threshold on Frequent and Rare Events: The EU threshold percentage is one of the important factors that influence successful publishing of true events. Thus, to study the effect

of EUT threshold, we conducted experiments for both frequent (i.e., $p_z \geq 0.6$) and rare events (i.e., $p_z \leq 0.4$) under a situation where 85% of the participants are genuine, which we believe is a reasonable assumption for any realistic system. Fig. 12(a) demonstrates that for frequently occurring events, the decision module of the *SAFE* framework achieves 100% success rate even if we fix the EU threshold as high as 80% of the sum of all event confidences. However, for rare events, a maximum of 60% of the sum of confidence values needs to be set to achieve the highest success rate. Thus, for all events, the minimum threshold to be maintained is 60% which is still on the higher side. This is because, as we have shown in Fig. 11(b) that to achieve significant success rate backed up with substantial evidences (from genuine participants), the EU_{thres} needs to be set at a higher value. Thus, it is a configuration parameter which the VCPS has to adjust depending upon its risk attitude (risk-seeking or risk-averse) and the percentage of genuine participation available. Interestingly, for both rare and frequent events, the error rates are negligible, implying that irrespective of the thresholds the proposed decision model does not miss out publishing true events (rare or frequent).

7 CONCLUSION

In this work, we handled the problem of information falsification in a participatory sensing-based vehicular cyber-physical system (VCPS) and proposed a regression-based reputation framework, called *SAFE*. The framework utilizes the participatory sensing paradigm and mobile security agents (MSAs) to detect rogue contributions; it also uses a modified distance bounding method to address the location spoofing attacks. The *SAFE* framework assesses the quality of contribution (QoC) of a given participant by building an MSA-supported opinion and measuring the spatial similarity between the reported event location and the site of the actual cellular base station. The reputation score of the participating user is calculated as the aggregation of the *QoCs* based on contributed reports. The normalized reputation score is then utilised for profile-based segregation of honest, liar and location spoofer. The proposed approach ensures fairness within different segregated groups by taking both, participation (i.e., quantity) and quality into account. We further proposed a decision model based on expected utility theory. The decision model takes the users' reputation score as an input and make decision for publishing or drop-out the events to enhance the operational reliability of the system. Extensive experiments with synthetic and real dataset demonstrates that the *SAFE* framework is efficient in terms of user behavior classification and decision accuracy as compared to the state-of-the-art participatory sensing-based reputation models.

ACKNOWLEDGEMENT

The authors would like to thank the guest editors and the anonymous reviewers for valuable suggestions that helped us to improve the quality of the manuscript to a considerable extent. The authors acknowledge the support of CSIR-CMERI Durgapur, IIT Kharagpur, IIEST Shibpur, and Missouri S&T to carry out this research. The work of S. K. Das is partially supported by NSF grants under award numbers: CNS-1545050, CNS-1545037, CCF-1725755, and CNS-1818942.

REFERENCES

Mohannad A Alswailim, Hossam S Hassanein, and Mohammad Zulkernine. 2016. A reputation system to evaluate participants for participatory sensing. In *Global Communications Conference (GLOBECOM), 2016 IEEE*. IEEE, 1–6.

Haleh Amintoosi and Salil S Kanhere. 2013. A trust-based recruitment framework for multi-hop social participatory sensing. In *Distributed Computing in Sensor Systems (DCOSS), 2013 IEEE International Conference on*. IEEE, 266–273.

Haleh Amintoosi and Salil S Kanhere. 2014. A reputation framework for social participatory sensing systems. *Mobile Networks and Applications* 19, 1 (2014), 88–100.

Haleh Amintoosi, Salil S Kanhere, and Mohammad Allahbakhsh. 2015. Trust-based privacy-aware participant selection in social participatory sensing. *Journal of Information Security and Applications* 20 (2015), 11–25.

Rajesh P Barnwal, Nirnay Ghosh, Soumya K Ghosh, and Sajal K Das. 2016. Enhancing Reliability of Vehicular Participatory Sensing Network: A Bayesian Approach. In *Smart Computing (SMARTCOMP), 2016 IEEE International Conference on*. IEEE, 1–8.

Rajesh P. Barnwal, Nirnay Ghosh, Soumya K. Ghosh, and Sajal K. Das. 2018. PS-Sim: A Framework for Scalable Simulation of Participatory Sensing Data. In *IEEE International Conference on Smart Computing (SMARTCOMP)*. 195–202.

Rajesh P Barnwal and Soumya K Ghosh. 2016. KITE: an efficient scheme for trust estimation and detection of errant nodes in vehicular cyber-physical systems. *Security and Communication Networks* 9, 16 (2016), 3271–3281.

Shameek Bhattacharjee, Nirnay Ghosh, Vijay K Shah, and Sajal K Das. 2017a. QnQ: A Reputation Model for Securing Mobile Crowdsourcing Systems from Incentive Losses weighted QoI scoring mechanism in social sensing using community confidence. In *IEEE International Conference on Communications and Network Security (CNS)*. IEEE, 1–9.

Shameek Bhattacharjee, Nirnay Ghosh, Vijay K Shah, and Sajal K Das. 2017b. W2Q: A dual weighted QoI scoring mechanism in social sensing using community confidence. In *Pervasive Computing and Communications Workshops (PerCom Workshops), 2017 IEEE International Conference on*. IEEE, 375–380.

Shameek Bhattacharjee, Nirnay Ghosh, Vijay K Shah, and Sajal K Das. 2019. QnQ: Quality and Quantity based Unified Approach for Secure and Trustworthy Mobile Crowdsensing. *IEEE Transactions on Mobile Computing* (2019), 1–1. https://doi.org/10.1109/TMC.2018.2889458

Jeffrey A Burke, Deborah Estrin, Mark Hansen, Andrew Parker, Nithya Ramanathan, Sasank Reddy, and Mani B Srivastava. 2006. Participatory sensing. *Center for Embedded Network Sensing* (2006).

Nnanna Ekedebe, Wei Yu, Chao Lu, Houbing Song, and Yan Wan. 2015. Securing transportation cyber–physical systems, CRC Press, Boca Raton. (2015), 163–195.

Tom Fawcett. 2006. An introduction to ROC analysis. *Pattern recognition letters* 27, 8 (2006), 861–874.

Saurabh Ganeriwal, Laura K Balzano, and Mani B Srivastava. 2008. Reputation-based framework for high integrity sensor networks. *ACM Transactions on Sensor Networks (TOSN)* 4, 3 (2008), 15.

Bin Guo, Zhu Wang, Zhiwen Yu, Yu Wang, Neil Y Yen, Runhe Huang, and Xingshe Zhou. 2015. Mobile crowd sensing and computing: The review of an emerging human-powered sensing paradigm. *ACM Computing Surveys (CSUR)* 48, 1 (2015), 7.

Wenbo He, Xue Liu, and Mai Ren. 2011. Location cheating: A security challenge to location-based social network services. In *Distributed computing systems (ICDCS), 2011 31st international conference on*. IEEE, 740–749.

Dijiang Huang, Satyajayant Misra, Mayank Verma, and Guoliang Xue. 2011. PACP: An efficient pseudonymous authentication-based conditional privacy protocol for VANETs. *IEEE Transactions on Intelligent Transportation Systems* 12, 3 (2011), 736–746.

Kuan Lun Huang, Salil S Kanhere, and Wen Hu. 2010. Are you contributing trustworthy data?: the case for a reputation system in participatory sensing. In *Proceedings of the 13th ACM international conference on Modeling, analysis, and simulation of wireless and mobile systems*. ACM, 14–22.

Kuan Lun Huang, Salil S Kanhere, and Wen Hu. 2014. On the need for a reputation system in mobile phone based sensing. *Ad Hoc Networks* 12 (2014), 130–149.

Jean-Pierre Hubaux, Srdjan Capkun, and Jun Luo. 2004. The security and privacy of smart vehicles. *IEEE Security & Privacy* 2, 3 (2004), 49–55.

Daniel Jiang and Luca Delgrossi. 2008. IEEE 802.11 p: Towards an international standard for wireless access in vehicular environments. In *Vehicular Technology Conference, 2008. VTC Spring 2008. IEEE*. IEEE, 2036–2040.

Audun Jøsang. 1999. An Algebra for Assessing Trust in Certification Chains.. In *NDSS*, Vol. 99. 80.

Audun Jøsang and Roslan Ismail. 2002. The beta reputation system. In *Proceedings of the 15th bled electronic commerce conference*, Vol. 5. 2502–2511.

T Raghu Vamsi Krishna, Rajesh P Barnwal, and Soumya K Ghosh. 2015. CAT: Consensus-assisted trust estimation of MDS-equipped collaborators in vehicular ad-hoc network. *Vehicular Communications* 2, 3 (2015), 150–157.

Tie Luo, Salil S. Kanhere, Jianwei Huang, Sajal K. Das, and Fan Wu. 2017. Sustainable Incentives for Mobile Crowdsensing: Auctions, Lotteries, Trust and Reputation Systems. *IEEE Communications Magazine* 55, 3 (March 2017), 68–74.

Lucas Malta, Chiyomi Miyajima, and Kazuya Takeda. 2009. A study of driver behavior under potential threats in vehicle traffic. *IEEE Transactions on Intelligent Transportation Systems* 10, 2 (2009), 201–210.

Philippe Mongin. 1997. Expected utility theory. *Handbook of economic methodology* 342350 (1997).

Soyoung Park, Baber Aslam, Damla Turgut, and Cliff C Zou. 2009. Defense against sybil attack in vehicular ad hoc network based on roadside unit support. In *Military Communications Conference, 2009. MILCOM 2009. IEEE*. IEEE, 1–7.

Annette Peters, Stephanie Von Klot, Margit Heier, Ines Trentinaglia, Allmut Hörmann, H Erich Wichmann, and Hannelore Löwel. 2004. Exposure to traffic and the onset of myocardial infarction. *New England Journal of Medicine* 351, 17 (2004), 1721–1730.

Fengzhong Qu, Zhihui Wu, Fei-Yue Wang, and Woong Cho. 2015. A security and privacy review of VANETs. *IEEE Transactions on Intelligent Transportation Systems* 16, 6 (2015), 2985–2996.

Ragunathan (Raj) Rajkumar, Insup Lee, Lui Sha, and John Stankovic. 2010. Cyber-physical Systems: The Next Computing Revolution. In *Proceedings of the 47th Design Automation Conference (DAC'10)*. ACM, 731–736.

Danda B Rawat and Chandra Bajracharya. 2017. *Vehicular Cyber Physical Systems*. Number 978-3-319-44493-2. Springer, Switzerland.

Maxim Raya and Jean-Pierre Hubaux. 2005. Security aspects of inter-vehicle communications. In *5th Swiss Transport Research Conference (STRC)*.

Maxim Raya, Panagiotis Papadimitratos, Imad Aad, Daniel Jungels, and Jean-Pierre Hubaux. 2007. Eviction of misbehaving and faulty nodes in vehicular networks. *IEEE Journal on Selected Areas in Communications* 25, 8 (2007).

Robert A Reiss. 1991. *Freeway Incident Management Handbook*. U.S. Department of Transportation, Federal Highway Administration.

Francesco Restuccia and Sajal K Das. 2014. Fides: A trust-based framework for secure user incentivization in participatory sensing. In *World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2014 IEEE 15th International Symposium on a*. IEEE, 1–10.

Franceso Restuccia, Sajal K. Das, and Jamie Payton. 2016. Incentive Mechanisms for Participatory Sensing: Survey and Research Challenges. *ACM Transaction on Sensor Networks* 12, 2 (2016), 13:1–13:40.

Franceso Restuccia, Nirnay Ghosh, Shameek Bhattacharjee, Sajal K. Das, and Tommaso Melodia. 2017. Quality of Information in Mobile Crowdsensing: Survey and Research Challenges. *ACM Transaction on Sensor Networks* 13, 4 (2017), 34:1–34:43.

Kyung-Ah Shim. 2012. CPAS: An Efficient Conditional Privacy-Preserving Authentication Scheme for Vehicular Sensor Networks. *IEEE Transactions on Vehicular Technology* 61, 4 (2012), 1874–1883.

Meital Ben Sinai, Nimrod Partush, Shir Yadid, and Eran Yahav. 2014. Exploiting social navigation. *arXiv preprint arXiv:1410.0151* (2014).

Gang Wang, Bolun Wang, Tianyi Wang, Ana Nika, Haitao Zheng, and Ben Y Zhao. 2016. Defending against sybil devices in crowdsourced mapping services. In *Proceedings of the 14th Annual International Conference on Mobile Systems, Applications, and Services*. ACM, 179–191.

Qikun Xiang, Jie Zhang, Ido Nevat, and Pengfei Zhang. 2017. A Trust-based Mixture of Gaussian Processes Model for Robust Participatory Sensing. In *Proceedings of the 16th Conference on Autonomous Agents and MultiAgent Systems*. International Foundation for Autonomous Agents and Multiagent Systems, 1760–1762.

Ruiyun Yu, Rui Liu, Xingwei Wang, and Jiannong Cao. 2014. Improving data quality with an accumulated reputation model in participatory sensing systems. *Sensors* 14, 3 (2014), 5573–5594.

Junping Zhang, Fei-Yue Wang, Kunfeng Wang, Wei-Hua Lin, Xin Xu, and Cheng Chen. 2011. Data-driven intelligent transportation systems: A survey. *IEEE Transactions on Intelligent Transportation Systems* 12, 4 (2011), 1624–1639.