Peer-to-Peer Netw. Appl.
DOI 10.1007/s12083-012-0136-8

A social network approach to trust management in VANETs

Zhen Huang · Sushmita Ruj · Marcos A. Cavenaghi · Milos Stojmenovic · Amiya Nayak

Received: 8 December 2011 / Accepted: 4 April 2012

Abstract In the past few years, vehicular ad hoc networks(VANETs) was studied extensively by researchers. VANETs is a type of P2P network, though it has some distinct characters (fast moving, short lived connection etc.). In this paper, we present several limitations of current trust management schemes in VANETs and propose ways to counter them. We first review several trust management techniques in VANETs and argue that the ephemeral nature of VANETs render them useless in practical situations. We identify that the problem of information cascading and oversampling, which commonly arise in social networks, also adversely affects trust management schemes in VANETs. To the best of our knowledge, we are the first to introduce information cascading and oversampling to VANETs. We show that simple voting for decision making leads to oversampling and gives incorrect results in VANETs. To overcome this problem, we propose a novel voting scheme. In our scheme, each vehicle has different voting weight according to its distance from the event. The vehicle which is more closer to the event possesses higher weight. Simulations show that our proposed algorithm performs better than simple voting, increasing the correctness of voting.

Keywords Reputation system · Vehicular networks · Security · Information cascading · Information oversampling · P2P networks

1 Introduction

Vehicular ad hoc networks (VANETs) is a class of P2P ad hoc networks which consists of vehicles (peers), Road Side Units (RSUs) and Certification Authorities (CA). VANETs are build to ensure the safety of traffic. This is important, because accidents claim several lives. According to the National Highway Traffic Safety Administration (NHTSA) report, a total of 37,261 people got killed in traffic accidents in 2008 (http://www-fars.nhtsa.dot.gov/Main/index.aspx).

Communication can be of two types: Vehicle-to-Vehicle (V2V) or Vehicle-to-Infrastructure (V2I). In V2V communication, vehicles (nodes) send and receive messages to and from one to another. These messages can be alert signals about road congestion, accidents ahead or information about traffic on a given route. V2I communication takes place between nodes and road side infrastructure and involve finding nearest and cheapest gas stations, internet services, online toll payment, etc. VANETs are a class of ephemeral networks [1], in which the nodes have short lived connections with each other. The density of the network changes continuously as nodes move in and out of the range of each other. In all these situations, security

Z. Huang (✉) · S. Ruj · A. Nayak
SEECS, University of Ottawa, Ottawa, Canada
e-mail: robertzhen1988@hotmail.com

S. Ruj
e-mail: sruj@site.uottawa.ca

A. Nayak
e-mail: anayak@site.uottawa.ca

M. A. Cavenaghi
Unesp, Sao Paulo State University, DCo, Sao Paulo, Brazil
e-mail: marcos@fc.unesp.br

M. Stojmenovic
Singidunum University, Belgrade, Serbia
e-mail: mstojmenovic@singidunum.ac.rs

Published online: 01 May 2012

is an important concern. To preserve the security of the whole network, a node needs to authenticate itself while sending information. This is done using signature schemes [2, 3]. A node is given a public/private key pair by the CA. It signs the message using the private key, which can be verified by other nodes, using the sender's public key.

The other important concern is location privacy. Keeping track of nodes makes them susceptible to threats, in which the adversary might gain useful information by observing the movement of the nodes. A few papers [4–6] focus on peer location privacy, while [7] is focusing on how to detect the location intrusion in message. One way to ensure privacy is to use a set of *pseudonyms* for each node. The pseudonyms are like aliases. It should be ensured that these pseudonyms are unlinkable. A node changes its pseudonyms from time to time, such that it is not possible for an observer to know that two or more pseudonyms belong to the same node. The problems of assigning pseudonyms [8, 9], changing pseudonyms [10, 11], and authentication by using pseudonyms [12] have been studied extensively.

Due to the safety concerns, it is more important to know the correctness of the data, rather than the authenticity of the nodes. Nodes might misbehave due to selfish reasons and might not send corrupt information all the time. The vehicles are driven by humans and the human behavioral tendencies are reflected in the behavior of the nodes. Hence, it is more important to know which data can be trusted and which cannot be trusted. Trust management in VANETs is more complicated than that in MANETs. This is because of the following reasons:

1. Due to the ephemeral nature of VANETs, nodes are in contact for too short a time to build trust amongst themselves,
2. A misbehaving node might not be malicious but selfish. A node can send correct data and incorrect data, and cannot always be labeled as "good" or "bad",
3. Most reputation schemes in MANETs rely on voting. Sometimes there might not be enough nodes to reach a threshold number of votes, due to constantly changing topology.

This makes trust management schemes difficult to be implemented in VANETs. Zhang [13] presents a survey on trust management schemes in VANETs.

Simple voting decisions also lead to two major problems in ad hoc networks, which to the best of our knowledge has not been addressed in literature. These two problems arise in social networks and are known as *information cascading* [14, Chapter 16] and *oversampling* [15]. Suppose there is a decision to be made and people decide sequentially after observing the behavior of others. Then, one's decision is highly influenced by the previous decisions and might overrule its own observation.

Oversampling occurs in the following situation: For example, node A receives the opinion of nodes B and C. It might be possible that B's opinion is influenced by C. So we say that the opinion of C has been oversampled (http://web.mit.edu/newsoffice/2010/crowd-wisdom-1115.html). In such cases, there is a need to discount the opinion of B, so that C's decision is not oversampled. We observe that this situation arises commonly in VANETs. Suppose a node A receives the information of an event, "congestion" (say), from a node B and node C (where C's decision is obtained from B) and "no congestion" from node D and F. If the nodes were to decide what to do, and do a majority voting, then they receive two votes in both favor of and against congestion. However, the votes in favor of congestion has been over-weighed because C's decision is obtained from B. In such cases, the opinion of C should be discounted, by using a weighing factor α (<1). So instead of considering C's vote as 1, it is considered as α. Such a weighing mechanism will counter oversampling, as we show in this paper by analysis and simulation. This is the first paper which studies these two phenomenon in ad hoc networks. We also show experimentally that considering only the first hand information gives better results than voting the opinions of all neighboring nodes.

The paper is organized as follows. In Section 2.1, we present a survey of reputation schemes for MANETs and point out why each of them is unsuitable for VANETs. Section 2.2 presents reputation schemes used in VANETs and points out the weaknesses of those schemes. We discuss the problem of information cascading and information oversampling in Section 3. We propose an algorithm to overcome information cascading and oversampling, in Section 4. In Section 5, we experimentally show that our approach performs better than normal voting. We conclude in Section 6 with directions for future work. A preliminary version of this paper has appeared in [16].

2 Survey of reputation schemes

In VANETs, an important issue is that how to trust the specific vehicle or message. For instance, if a car sends the message that there is congestion at location X, should other vehicles believe that this information is correct and take corresponding action? The aim of reputation system is to construct trust value for each node in the network, the other nodes decide whom to trust based on these values. Resnick and Zeckhauser [17] list the following three goals for reputation systems:

(a) To provide information to distinguish between a trustworthy and an untrustworthy peer.
(b) To encourage peers to act in a trustworthy manner.
(c) To discourage untrustworthy peers from participating in the process.

There has been several works on reputation schemes in VANETs [13, 18–24]. These claim to build a trustworthy network, but suffer from several disadvantages. We will discuss each of these schemes in details in Section 2.2.

2.1 Reputation systems in MANETs

Reputation was first used in Internet and then spread to mobile ad hoc network. While trust management is applied to reputation system. The main features of trust are described below as given in [25–29]:

- A centralized certification authority is prone to single point failure, hence the decision method should be distributed. In other words, decentralized mechanism is required.
- The nodes in MANETs are not always cooperative. In a restricted environment, nodes may refuse to cooperate in order to save the energy or for some selfish reasons.
- Trust is not necessarily transitive. If A trusts B and B trusts C, it does not mean that A trusts C. Each node makes its own decision.
- Gathering reputation information from past relationship is computationally expensive, so excessive calculation should be minimized to reduce workload of the network.

Most trust management schemes make use of voting and game theoretic concepts. We show that these schemes have some drawbacks and cannot be applied as is to VANETs.

Marti et al. [30] propose a reputation system for ad hoc networks. In their system, a node monitors the transmission of a neighbor to make sure that the neighbor forwards traffic. If the neighbor does not forward traffic, it is considered as uncooperative, and its reputation is propagated throughout the network. In essence, one can consider such a reputation system as a repeated game whose objective is to stimulate cooperation. Such reputation systems, however, may have several issues. First, there is no formal specification and analysis of the type of incentive provided by such systems. Second, these systems have not considered the possibility that even selfish nodes can collude with each other in order to maximize their benefit. Third, some of the current systems depend on the broadcast nature of wireless networks in order to monitor other nodes. Such monitoring, however, may not always be possible due to asymmetric links when nodes use power control. Furthermore, directional antennas, which are gaining momentum in wireless networks in order to improve capacity, will also make monitoring hard. Besides the problems pointed out for MANETs, this reputation system cannot be applied to VANETs because a node is in contact with another node for a very short time. There is no time to monitor other node's transmissions.

Michiardi et al. [31] propose a mechanism, called CORE, to enforce node cooperation based on a collaborative monitoring technique. CORE is suggested as a generic mechanism that can be integrated with any network function like packet forwarding, route discovery, network management, and location management. The reputation metric is computed based on data monitored by the local entity and some information provided by other nodes involved in each operation. An interesting feature of the CORE mechanism is that denial of service attacks based on malicious broadcasting of negative ratings for legitimate nodes can be prevented. CORE is also based on the assumption that reputation is a good measure of node's contribution to common network operations. Nodes that have a good reputation, because they helpfully cooperate with other nodes, can use the resources of the network, while nodes with a bad reputation, because they refused to cooperate, are gradually excluded from the community. There are three types of reputation: a subjective reputation, an indirect reputation and a functional reputation. The term subjective reputation is used to talk about the reputation calculated directly from a node's observation. The reason why more relevance is given to past observations is that a sporadic misbehavior in recent observations should have a minimal influence on the evaluation of the final reputation value; as a result, it is possible to avoid false detections due to link breaks and to take into account the possibility of a localized misbehavior caused by disadvantaged nodes. The subjective reputation is evaluated only considering the direct interaction between a subject and its neighbors. The concept of indirect reputation is introduced to evaluate the effect of the information provided by other members of the community. Functional reputation has been used to evaluate trust in different situations, like packet forwarding or route selection. CORE system also cannot be applied to VANETs. The reason is that CORE is dependent on indirect reputation that is related to the information provided by other members of the network. Due to the ephemeral nature of VANETs, the contact between two nodes are short lived.

Fahnrich et al. [32] propose the Buddy System as a distributed reputation system that is based on social structure. The ensuing Buddy System improves the detection of vicious entities and, thus, increases cooperativeness. The considered system consists of autonomous entities that may cooperate in transactions. Each entity is autonomous and can therefore exhibit vicious behavior in any cooperation, i.e., it defects by breaking his commitments. Each entity runs an independent instance of the reputation system and reports any observed behavior. The instances of different entities may cooperate by exchanging recommendations. The individual trust levels are passed on in order to inform other entities about personal experiences made. The system is based on a mutual buddy-relationship that is established adaptively between a pair of entities (so-called buddies). A buddy-relationship necessitates especially high trust levels since the buddies mutually agree to be punished for the misbehavior of their partner buddy. There are two criteria for its establishment. Apart from mutually trusting each other, the entities have to perceive the trustworthiness of other agents likewise. This additional criterion is called similarity of world views. It is set in place in order to reduce the conflict potential between buddies. The authors show how the Buddy System overcomes the limitations of conventional distributed reputation systems. By the means of simulation, they have shown that the Buddy System improves the degree of cooperation and therefore the overall quality of ad hoc network. The Buddy System cannot be applied to VANETs because it is impossible to establish a buddy relationship between two nodes in a VANETs. Again, the contact between them are short lived. Therefore, any assumption on a relationship is not applicable.

In the paper by Dewan et al. [33], the reputation of nodes in an ad hoc network is used to identify and subsequently circumvent the malicious nodes. The reputation of a node is not contextual and is a function of the number of packets forwarded by a node. The nodes achieve high reputation by correctly routing packets for other nodes. If a node fails to route the packet even after promising to do so, it gets a low reputation and hence is removed from the network. In the proposed reputation scheme, the source node finds a set of paths to the destination by using a routing protocol for ad hoc networks. The source node sends the data packet to its neighbor with the highest reputation. The neighbor forwards the packet to the next hop neighbor with the highest reputation, and the process is repeated till the packet reaches its destination. The destination acknowledges the packet to the source that updates its reputation table by giving a recommendation of +1 to its neighbors. All the intermediate nodes in the route give a recommendation of +1 to their respective neighbors in the route and update their local reputation tables. If there is a malicious node in the route, the data packet does not reach its destination. As a result, the source does not receive any acknowledgment for the data packet in the stipulated time. The source gives a recommendation of −1 to the neighbor on the route. The intermediate nodes propagate this recommendation in the route upto the node that has dropped the packet. In other words, all the nodes between the malicious node and the sender, including the malicious node, get a recommendation of −1.

The salient features of the proposed reputation system are: 1) circumvention of malicious nodes, 2) injection of motivation to cooperate among nodes, 3) decentralized collection and storage of reputations, and 4) subsequent increase in the average throughput of the network. In addition, the nodes in the network are able to quickly use the reputation information to make routing decisions without having a significant impact on the routing performance. The authors conclude that the reputation scheme improves the throughput by 65% with 40% malicious nodes in a network where the nodes are static. The cost of this improvement is the increased number of route requests. The throughput can be further improved at the cost of extra messages, by making the nodes exchange their reputation databases using cryptographic protocols for ascertaining the credibility of the source of information and the correctness of the reputation information obtained. The reputation scheme presented by Dewan et al. cannot be applied to VANETs, because it is based on an assumption that all nodes are static. Besides this assumption, the reputation is also based on the number of packets a node forwards. It is not possible to accurately manage this information in VANETs due to its dynamic nature.

2.2 Reputation systems in VANETs

The requirement for reputation system in VANETs also differs from that in MANETs. All the ideas and techniques presented in Section 2.1 cannot be applied to VANETs. VANETs are different from MANETs in the following ways:

(a) VANETs is an ephemeral network in which cars are constantly roaming around and is highly dynamic. The velocity on a highway is up to 150 km per hour. At this high speed, the contact and reaction time is too short to build trust among themselves.

(b) VANETs is a large scale network where the number of nodes and the density is much higher than that in MANETs. Network traffic can be very high. Hence, there should be intelligent vehicle communication systems that are scalable and can prevent data congestion by deciding which peers to interact with [13].

(c) Almost all the existing reputation systems compute trust value based on the past interaction with target node. However, this assumption is not valid in VANETs due to the dynamic and open environment. In fact, if a vehicle is communicating with another vehicle, it is not guaranteed that it will interact with the same vehicle in the future. Therefore, the existing algorithms which are based on long-term relationship are not suitable for VANETs.

(d) Some of the reputation models [34] depend on a central entity to gather the information. However, the large number of nodes and high dynamic environment require a decentralized system in VANETs. Aggregation of reputation should be a local action instead of a global action.

(e) Another important issue is pseudonymous authentication which is ignored by many researchers. As discussed above, for privacy consideration, each vehicle is issued a large number of identities, and only CA knows the relation between real ID with pseudonymous identities. Therefore, it is infeasible to get meaningful reputation values because vehicles change identity over time. For instance, if vehicle A interacts with B then A has a reputation value for B, but at next moment if B changes its pseudonyms to C, the reputation value stored in A is no longer useful.

Only a few trust models have been proposed for honest information sharing in VANETs. Based on the characteristics discussed above, there are two basic models: *entity-oriented trust model* and *information-oriented trust model*. Entity-oriented trust model focuses on the trust of vehicles that means constructing trust values for vehicles and determine whether or not to believe the vehicles, whereas information-oriented trust model decides how to trust the message transmitted. Existing information-oriented models consider each vehicle being equal, as a result, majority voting is widely used to judge the correctness of the message.

Entity-oriented model As we discussed above, reputation of vehicles is not easily built in this ephemeral environment. Two typical entity-oriented trust models are proposed by Gerlach [35] and Minhas et al. [36]. Gerlach in [35] propose a sociological trust model based on the principle of trust and confidence tagging. Their trust establishment service tags content of the database with confidence value which may be based on certification or self-tests of the system. Then, they describe how to choose a confidence value. Meanwhile, the authors also propose an architecture for communication and a model for privacy.

Minhas et al. [36] develope a multi-facet trust modeling framework which incorporates role-based trust, experience-based trust, and majority-based trust to receive the most effective reports. Meanwhile, they describe an algorithm that shows how to integrate various trusts. This model allows the vehicle to actively inquire an event by sending requests to other vehicles. The above two schemes are based on the trust value of vehicles.

Information-oriented model The entity-oriented model does not work for ephemeral networks like VANETs. The information-oriented model constructs trust not based on vehicles but on message itself. In these models, long-term relationships between vehicles are not required which is the basis in entity-oriented model. Hence, *information-oriented trust* is more efficient in this life-critical network because it decrease the delay of relationship processing and computing.

2.3 Problems with existing reputation schemes for VANETs

One of the first papers about reputation in VANETs is VARS, by Florian Dotzer et al. [18]. In that paper, the authors propose a modular reputation system architecture that strictly separates direct and indirect reputation handling from opinion generation. VARS is not based on the behavior of nodes but on the opinion about distributed content, i.e., forwarding nodes form an opinion on the content of a message; this opinion is attached to the message before forwarding it to other nodes. Therefore, receivers can evaluate the opinion of other nodes and use it as a basis for their own decision about the trustworthiness of a message. On arrival of an event message every forwarding node generates an opinion on the trustworthiness of this message. An opinion is calculated either from experience if the event is detected, from indirect trust if the sender is known, or from partial opinions attached to the message or a combination thereof. This generated opinion is appended as another partial opinion to the message, before it is forwarded. A problem pointed out by the authors is that attacks like simple modification or deletion of messages can be wielded by every forwarding node as no authentication is provided. Another possible problem with VARS is that, if the number of forwarding nodes is high (in the case of a dense network), the communication bandwidth would be seriously compromised due to the overhead due to the extra information (many opinions) on each package forwarded.

Another paper about reputation in VANETs is *Vehicle Behavior Analysis to Enhance Security in Vanets* [23]. In that paper, the authors introduce a distributed Vehicle Behavior Analysis and Evaluation Scheme (VEBAS). The scheme comprises of a framework for behavior analysis on which an evaluation of neighboring vehicles regarding trustworthiness is performed. This system is able to distinguish between three classes: trustworthy, untrustworthy, and neutral vehicles. Therefore, it detects misbehavior, especially intentional misbehavior, and honors evident honest behavior and also preserves a class of vehicles that cannot be analyzed due to insufficient (sensor) information.

Another paper about reputation in VANETs is [19] by Nai-Wei Lo et al.. An event-based reputation system (ERS) is introduced in the paper, to filter out inaccurate messages caused by the dynamics of traffic event and vehicles with different detection capabilities on embedded sensors, and false messages spread by malicious attackers in VANETs. The purpose is to determine whether a traffic event really exists and how long it lasts through distributed vehicle observations. The status of a traffic event is stored and managed in each vehicle which has encountered it or is aware of it from received messages. ERS is enlightened by a cooperation enforcement schemes, where nodes collaboratively observe neighbors and broadcast warnings if misbehaved nodes are discovered. Traffic information comes either from received messages via wireless interface or from on-board sensors. An event table in ERS stores all received and derived traffic event information including event identity, type of traffic event, occurrence timestamp, event location, message transmission range, event reputation value, and event confidence list. One obvious problem with ERS is the difficulty in managing the confidence list for each traffic event created in the network. Another potential problem is when a vehicle broadcasts an emergency message signaling the existence of an accident on the road, ERS may fail to deliver the message to other drivers just in time to avoid another accident because of the lack of similar messages to corroborate the traffic event. This can jeopardize the security of other drivers.

2.4 Trust in VANETs

A trust module using game theoretic techniques was presented by Raya et al. [22]. There are two types of games: one played between the group of good nodes and the group of adversarial nodes, and another played between the nodes of the same type. Each node is assigned benefit if it behaves well and a cost if it behaves badly. Nodes observing misbehaviors can either vote or abstain from voting. There are some issues with this approach:

1. Who decides the cost and benefit?
2. Raya et al. [22] assume these costs incurred by a node to be fixed. But, in reality in a continuously changing environment, these costs will also change and so will the threshold of trust (to decide who wins the game).
3. Different types of vehicles must have different costs and benefits. For example, if a police car behaves badly, then it will incur more costs than an ordinary car.

A Central Authority cannot decide this because it might be far away (say a government security agency). An interesting question will be to model the costs and benefits with the changing network topology.

Umar et al. [20] examine the challenge of designing intelligent agents to enable the sharing of information between vehicles in mobile ad hoc vehicular networks. Their focus was on developing a framework that models the trustworthiness of the agents of other vehicles in order to receive the most effective reports. The authors developed a multi-facet trust modeling framework that incorporates role-based trust, experience-based trust, and majority-based trust.The framework is able to restrict the number of reports that are received. The authors included an algorithm to integrate these various dimensions of trust, along with experimentation to validate the benefits of their approach. The authors emphasized the importance of different facets that were included. The authors also clarified how their approach was able to meet various critical challenges for trust modeling in VANETs. As a final result they presented a methodology to enable vehicle to vehicle communication via intelligent agents. In order to capture the complexity that arises between interacting agents in VANETs, the authors propose several different trust metrics with various key characteristics. The authors also propose that, in order to derive a rather complete and comprehensive view of trust for agents in VANET environments, it is necessary to integrate security solutions with trust management. The core of their model is divided in two parts. The first one is composed of role-based, experience-based, and priority-based trusts. These trusts maintain trustworthiness of agents in order for trusted agents (called advisors) to be chosen for their feedback. The first two trusts (role-based and experience-based) are combined into the priority-based trust, that can be used to choose proper advisors. The role-based trust exploits certain predefined roles that are enabled through the identification of agents (vehicles). Agents can put more trust in certain agents as compared to others (law enforcing authorities, for instance). The experience-based trust represents a component of trust that is based on direct interactions among agents. The second part of their model is composed of the majority opinion. This part aggregates feedback from selected advisors. Based on this model, when an agent in a VANETs receives reports from other agents about an event, eg., traffic or collision ahead, it may need to verify if the information received is reliable. To do so, the agent asks other trusted agents about the received information. For this purpose, each agent in the system keeps track of a list of other agents. The agent updates the trust values of the senders after the truth of their reported events is revealed.

The role-based approach is based on the following four different roles listed in decreasing importance: authority (agents representing authorities such as traffic patrols, law enforcement, police, etc.), expert (agents specialized in road condition related issues such as media (TV, radio, etc.), traffic reporters, etc., seniority (agents familiar with the traffic or road conditions of the area in consideration, e.g. local people who commute to work on certain roads or have many years of driving experience with a good driving record), ordinary (all other agents). The problem with this approach is to assume that the nodes can maintain a list of trusted and untrusted agents and that it is possible to request “advices” about a message. The ephemeral nature of VANETs leads to a very short lived relationship between nodes, for which is not possible to build an effective list of trusted nodes to ask for advices. Furthermore, due to the speed each node is moving in the network, when an advice arrives it may be too late for the node to consider it. These issues have not been considered by the authors.

In another paper by Umar et al. [21], the authors use the same multi-facet trust model introduced by their previous work. In this paper, they argue that there is a need to model trust in various dimensions and that combining these elements effectively can assist agents in making transportation decisions. They introduced two elements to their proposed model: i) distinguishing direct and indirect reports that are shared, and ii) employing a penalty for misleading reports, to promote honesty. They demonstrate through a series of experiments of simulated traffic how these two elements together serve to increase the value of the trust model. In order to distinguish direct and indirect experience, when information is provided by an agent to another agent, it is required that each agent declare whether its information has been derived from firsthand experience or not. It is initially assumed that this declaration is truthful, and determine which action to take through a weighting of the advice that has been provided. If an agent is not a direct witness but claims to be one, then it will run the risk of having its trust value reduced more severely, if its advice is verified to be unreliable. The main idea is that an agent that asks for information from other agents will value advice from the direct witnesses more than that from the indirect ones. An agent B is considered dishonest or deceitful by an agent A if the personal experience trust value that A has on B falls below some value that A can accept. Each agent that seeks advice from other agents maintains a set of dishonest agents to whom it will not respond when asked, as a penalty to these dishonest agents. The authors demonstrate by experiments that the proposed penalty system effectively promotes honesty. Besides the problems pointed out for the previous paper, another problem with this approach is that a node can lie to a requesting agent about a firsthand information. Sometimes the node may say it is a firsthand information when it is not, and the node may say it is not, when it is a firsthand information (the dishonest node tries to trick the requesting node to gain advantage). Furthermore, the penalty applied to a misbehaving node is not enough to enforce its good behavior, because the time two agents (vehicles) are in contact with other is not long enough to establish a trust relationship between them.

In the paper [24], the authors present a trust-based framework for message propagation and evaluation in vehicular ad-hoc networks where peers share information regarding road condition or safety and others provide opinions about whether the information can be trusted. More specifically, the trust-based message propagation model collects and propagates peer’s opinions in an efficient, secure, and scalable way by dynamically controlling information dissemination. The trust-based message evaluation model allows peers to evaluate the information in a distributed and collaborative fashion by taking into account others’ opinions. Experimental results demonstrate that the framework significantly improves network scalability by reducing the utilization of wireless bandwidth caused by a large number of malicious messages. The system is also demonstrated to be effective in mitigating the malicious messages and protecting peers from being affected. The idea of the framework is to evaluate and disseminate a message based on its quality. The framework was designed in a way that messages can be evaluated in a distributed and collaborative fashion. At the same time, the dissemination depth of a particular message is largely dependent on its quality, so that messages of good quality propagate to the furthest distance while malicious data, such as spam, is controlled to a local minimum. The message quality is modeled using a trust-based approach, the quality of a message is mapped to a trustworthiness value, which can be computed from a collection of distributed feedback from other peers in the network. Specifically, during the message propagation, the peer who receives the message can instantly provide feedback, namely, a trust opinion generated from an equipped *analysis module*.

A set of trust opinions are appended to the message during message propagation. For those who receive the message, their *action module* may decide to trust or distrust the message by computing its trustworthiness from an aggregated list of trust opinions. Apart from the trust modeling on data quality, the behavior of vehicle entities is modeled using a peer-to-peer trust approach. Three types of messages are generated in the system: sender message, trust opinion, and aggregate message. A sender message comes from a peer which wants to send an information. Associated with the message is the confidence. Higher confidence indicates the sender itself is more confident of the reported event. Trust opinion is a message provided by a peer that serves as the evaluation of the sender message. Evaluation is conducted by comparing the reported event with the peer's current knowledge, which may come from a number of equipped car sensors, the local database, or even human interactions. Aggregated message is a combination of a sender message and a list of trust opinions from distinct peers.

One design principle is that the trust opinion should always be generated before any disclosure of the existing trust opinions in the aggregated message; the generation of the trust opinion is purely based on the peer's local knowledge such as direct observations. So, malicious peers who give trust opinions by strategically guessing the message trustworthiness from others' trust opinions can be removed from the network. If a trust opinion can be provided, it is broadcasted and appended to the sender message. In the model, message propagation consists of two components: cluster cooperation and the relay control model. Based on a cluster-based routing mechanism, the cluster cooperation serves as the foundation for message propagation and trust opinion aggregation. The relay control model works as a filter that controls the relay of messages. The trust opinion aggregation scheme ensures that message evaluation and propagation can be done with little interference on each other. It provides high flexibility in the sense that during message propagation, trust opinions can be aggregated in a secure, scalable, and efficient way.

The model also employs both role-based trust and experience-based trust. A minority of vehicles, such as police cars, which are assigned a specific role and a specific role-based trust value. For other vehicles, they are associated with experience-based trust. Each peer maintains experience-based trust for other peers. The offline central authority assigns roles and updates role-based trust, collects distributed experience-based trust from peers, and rewards or punishes peers accordingly. This work presents the same issues pointed out in [20] and [21]: it is based on opinions propagated in the network. The limitations of bandwidth, in case of a dense network, and the lack of a mechanism to detect lies propagated by malicious nodes can jeopardize the effectiveness of this approach.

3 Information cascading and oversampling in VANETs

The decisions taken by nodes in the network influence the decisions taken by other nodes. In certain situations, the opinions about events reported by nodes can be so overwhelming that the opinion of one node can be suppressed. It occurs mainly when decisions are made sequentially [14]. Consider the situation shown in Fig. 1.

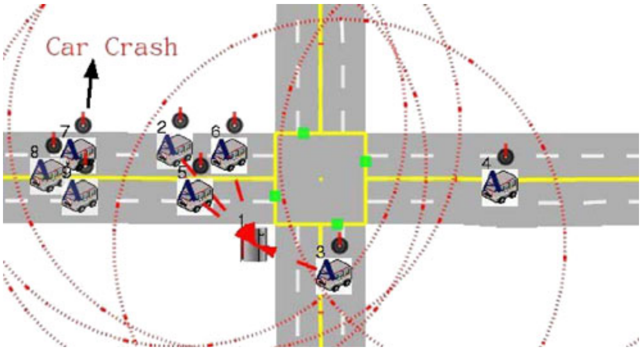

Fig. 1 A network situation

There are five nodes in the vicinity of an intersection (nodes 2, 3, 4, 5, and 6), 1 is an RSU. Nodes 2, 5, and 6 consist of the first-observation set. Node 3 is in the communication range of nodes 2, 5 and 6. Node 4 is in the range of node 3. Let us assume some event (like a "Car Crash") occurs on the left of first-observation set (2, 5, and 6) (as shown in the Fig. 1), then nodes will send out alert messages. After receiving these alert messages, node 3 will make a decision and re-broadcast these messages to node 4. Node 4 receives four messages from four different nodes (messages from nodes 2, 5, and 6 are first-hand and retransmitted by node 3 to node 4, message from node 3, which it calculates from the first-hand decisions).

Now, suppose that the majority of nodes 2, 5, and 6 send out false information (it means two false informations and one correct information). All the vehicles behind nodes 2, 5, and 6 will receive the false information. There is no way to prevent this.

Now assume that nodes 2 and 5 are good, while nodes 6 and 3 are malicious/selfish. So, the majority of first-observation set is correct and node 3 makes an incorrect decision deliberately. Node 4 will receive two correct and two false (incorrect) messages. This situation is called information cascading, where the decisions of other nodes influences one node to take a decision contrary to its observation. Even if node 4 observes that node 2 and 5 have acted as if there is a congestion, its decision might be overridden by that of 6 and 3. So a wrong decision will cascade through the entire network. There should be a way to decrease the importance of the message sent by node 3.

The above situation can also leads to oversampling. When node 4 makes a decision, it uses the opinions of nodes 2, 3, 5 and 6. However, the opinion of node 3 is based on the opinions of nodes 2, 5 and 6. So, the observations of nodes 2, 5 and 6 are being oversampled. This is an instance of information oversampling. One way to overcome this, is to give weight to the decisions made by nodes. For example, nodes which observe an event are considered with weight 1. However less weight is given to nodes, which are at two or more hops from the direct observers.

4 Counting information oversampling

Consider a network containing N nodes. Emergency events can be either congested road, hazardous road condition, accidents, etc. Nodes transmit alert signals on observing such events. Some nodes can generate false alert messages either for malicious or selfish reasons. A node which generates an alert message is known as a first-hand observer.

A node can receive contradictory messages about events, for example "accident" and "no accident". In such situations, it has to decide which of these informations are correct and transmits that information. Nodes can receive several messages from other nodes and make a decision about which one to accept. A node can receive messages from direct observers or through multi-hop paths.

4.1 Network model

We first give the notations of our network. If a vehicle observes an event (for example, an accident) in front of it, it transmits the information to the vehicles behind it. Let n_i be a vehicle. Vehicle n_j is said to be in the neighborhood of n_i, if n_j is in the communication range of n_i. The neighborhood of n_i is denoted by $nbd(i)$. Hence $n_j \in nbd(i)$ (Table 1).

A message M_i sent by a node n_i contains a number c, which denotes the number of hops from the forst hand observers to n_i. For example, the first hand observers have $c = 0$, second hand observers have $c = 1$, and so on. This number is denoted by $c(M_i)$. M_i also contains a decision d_i, which can be either $+1$ or -1. Let F be a set of vehicles which observe an event. They report either an accident C (correct) or no accident I (incorrect). The decision of any vehicle n_i is denoted by d_i. A vehicle n_i receives messages from its neighbors and has to decide whether there is an accident or not. It considers all the neighbors $n_j \in nbd(i)$ that are in front of n_i. A majority voting algorithm works as follows. Let $v_i =$ number of nodes which report $C-$ number of vehicles which report I. If $v_i \geq 0$, then $d_i = 1$ which indicates that the vehicle n_i says "there is an accident", and if $v_i < 0$, then $d_i = -1$ to indicate that the vehicle says "there is no accident". A benign vehicle transmits d_i and a malign vehicle transmits $-d_i$.

Table 1 Table of notations

Notation	Meaning
n_i	ith vehicle
$nbd(i)$	Neighborhood set of vehicle n_i
M_i	Message sent by vehicle n_i
$c(M_i)$	The number of hop between n_i with first-hand observers
d_i	Decision of vehicle n_i
F	The set of first-hand obervers
α	Weight factor

4.2 Our algorithm

To deal with information oversampling we do not consider all the opinions received with equal weight. We give more weight to vehicles which are closer to the event (that lead to the alert), than to vehicles that are far away. The opinion of a vehicle, which observes an event directly is given a weight of one, whereas a vehicle which receives second hand information is given a weight α. The opinion of the vehicle at two hops from the direct observer is given a wight α^2 and, so on. The pseudo code of our approach is in Algorithm 1. If n_i is the neighbor of n_j, n_i maybe receive the message from n_j for a few times since there exist several routes, in our scheme, we only consider the message which is directly from n_j.

Algorithm 1 This algorithm decides the opinion of node n_i, based upon the messages it received from its neighbors $nbd(i)$

Input: Node n_i which has to make a decision and messages M_j, where $n_j \in nbd(n_i)$

Output: Decision taken by each node n_i "accident" or "no accident"

```
$v_i = 0$
for $n_j \in nbd(i)$ and in front of $n_i$ do
    $w_j = \alpha^{c(M_j)}$
    $v_i = v_i + w_j d_j$
end for
if $v_i \geq 0$ then
    if $n_i$ is a good node then
        $d_i = 1$
        Opinion of $n_i$ is "there is accident"
    else
        $d_i = -1$
        Opinion of $n_i$ is "there is no accident"
    end if
else
    if $n_i$ is a good node then
        $d_i = -1$
        Opinion of $n_i$ is "there is no accident"
    else
        $d_i = 1$
        Opinion of $n_i$ is "there is accident"
    end if
end if
$c(M_i) = 1 + \min_{n_j \in nbd(i) \text{and in front}}\{c(M_j)\}$
```

If a vehicle receives n messages, the set of vehicles R_1 are first hand observers, the set of vehicles R_2 are one-hop neighborhood of R_1, the set R_n are $(n-1)$-th hop neighborhood of R_1, then the decision of vehicle is taken as $\sum_{i \in R_1} d_i + \alpha \sum_{i \in R_2} d_i + \cdots + \alpha^{n-1} \sum_{i \in R_n} d_i$.

Let's look back to the example in Section 3. Vehicle 2, 5 and 6 consist of first-hand observers, hence the weight of these three is 1. While vehicle 3 is the neighbor of 2,5 and 6, so the weight of vehicle 3 is α. Set $\alpha = 0.5$, when vehicle 4 makes the decision, the value is $1 + 1 - 1 - 0.5$ since vehicle 2 and 5 are benign while 6 and 3 are malign. Now after we applied this simple scheme, vehicle 4 will give the correct decision which means the information cascading is overcame in this situation.

5 Experimental results

This section shows how simple voting can result in incorrect decision making. The algorithm performs better by reducing the effect of oversampling. The best approach is to rely only on the information of the first-hand observers and transmit only that information across to other nodes. There is no need to transmit the decision of the intermediate nodes to the other nodes. This is because it will result in oversampling and hence incorrect results, and the intermediate nodes might be malicious/selfish and change received decisions.

Different decision making situations are simulated using NCTUns (National Chiao Tung University Network Simulator, http://nsl10.csie.nctu.edu.tw/). The simulator was proposed by S.Y.Wang in 2002 and written in C++. Table 2 shows the parameters we choose for each vehicle in the simulation. The following simulation environment is considered:

(a) The simulations occur around a road intersection.
(b) In every experiment, 35 vehicles are randomly deployed in the vicinity of the road intersection.
(c) Each experiment is run for 10 times, and the average is calculated.
(d) The transimission range is set as 100 m. Due to the path loss, the effective range in the experiment is approximate 80 m. That means every two vehicles during 80 m radius can receive the messages from each other.
(e) No obstacles(like buildings) are considered in the simulation.

Table 2 Experiment parameters

Frequency	2400 MHz
Path loss model	Two ray ground
Antenna height (m)	1.5
Transmission power (dbm)	15
Transmission range (m)	100
Type of antenna (degree)	360
TxGain of antenna	1
RxGain of antenna	1
Fading channel	Ricean
Width of road (m)	20

5.1 Simulation results

We show how our algorithm performs for different value of α in Fig. 2. Our algorithm reach the best performance when $\alpha = 0$ which means the intermediate vehicle's opinions to a specific event are not considered. In other words, each vehicle makes decision only based on the messages from first-hand obervers. While $\alpha = 1$ means the weight of each decision is equal, and the voting correctness is the lowest.

We then demostrate that our algorithm can exactly reduce the impact of information oversampling. We compare three different voting schemes to show the improvement of our scheme.

Mechanism 1: Each vehicle makes a decision based on the messages from the first-hand observers. This means theoretically every vehicle should obtain the same opinion for a specific event since they all receive the same messages.

Mechanism 2: The messages vehicles use to vote are from neighbors. Neighbors are considered to be the vehicle who reports an event in front.

Mechanism 3: This is a combination of Mechanism 1 and Mechanism 2. Vehicles make their own decisions based on their neighbor's messages and the first-hand obervers' messages.

Figure 3 shows the different performances of above three schemes. Mechanism 1 reaches the best performance in all these three schemes, which means if we do not consider the messages(opinions) of intermediate vehicle, the voting correctness increase. One can note that Mechanism 1 is the situation that when $\alpha = 0$ in our proposed algorithm. While in Mechanism 3, each vehicle not only consider the messages from first-hand observers, but also from the intermediate vehicles. Therefore the information oversampling is existing as we discussed before, consequently the voting performance is lower. Results and conclusions obtained with the simulations are the following:

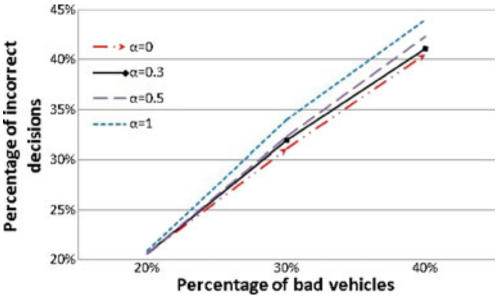

Fig. 2 Experimental results with different values of alpha

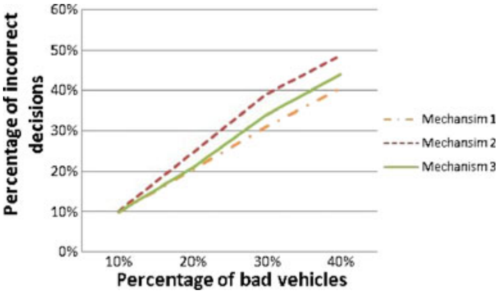

Fig. 3 Experimental results comparing different decision-making mechanisms

1. If we give lower weight to the intermediate vehicle's opinion, according to Fig. 2, with the decreasing of weight factor α, the voting performance imporves.
2. When weight factor $\alpha = 0$, there is no information oversampling in our scheme since each vehicle behind only consider the messages from first-hand observers.
3. Our algorithm presented in Section 4.2 is considered as a way to handle information oversampling. And the above simulations illustrate it clearly.

6 Conclusion

In this paper, the limitations of reputation schemes in VANETs have been discussed. We survey trust management schemes in VANETs and point out their drawbacks and limitations. We show that trust management schemes in MANETs cannot be used for VANETs. We identified that the problem of information cascading and oversampling also adversely affect trust management schemes in VANETs. We showed that simple voting for decision making leads to oversampling and gives incorrect results in VANETs. To overcome this problem, we proposed a novel voting scheme that performs better than simple voting. Through simulations, we have shown that our scheme increased the correctness of voting. Though the solution is described in the situation for VANETs, this can be applied to MANETs to deal with information oversampling.

The following questions need more explanations: when the vehicles make the decision? Do they make a decision immediately after receiving the messages? Or do they wait for a small interval to collect the opinions of other vehicles? In real life situations, there are delays in transmissions. If we make decisions immediately, we might lose important messages to make the voting. However, if we wait for some time before voting, there is also a problem: during this interval, vehicles might receive some incorrect messages. This will adversely affect the decision. This is an open problem.

Acknowledgements This work is partially supported by NSERC Grant CRDPJ386874-09 and "Digital signal processing, and the synthesis of an information security system", TR32054, Serbian Ministry of Science and Education.

References

1. Raya M (2009) Data-centric trust in ephemeral networks. PhD thesis. EPFL, Lausanne
2. Wasef A, Shen X (2009) Maac: message authentication acceleration protocol for vehicular ad hoc networks. In: IEEE GLOBECOM, pp 1–6
3. Zhu H, Lin X, Lu R, Ho P-H, Shen X (2008) Aema: an aggregated emergency message authentication scheme for enhancing the security of vehicular ad hoc networks. In: IEEE ICC, pp 1436–1440
4. Lu R, Lin X, Shen X (2010) SPRING: a social-based privacy-preserving packet forwarding protocol for vehicular delay tolerant networks. In: Proc. IEEE INFOCOM'10, San Diego, California, USA, 14–19 March 2010
5. Lin X, Lu R, Liang X, Shen X (2011) STAP: a social-tier-assisted packet forwarding protocol for achieving receiver-location privacy preservation in VANETs. In: Proc. IEEE INFOCOM'11, Shanghai, China, 10–15 April 2011
6. Lu R, Lin X, Liang X, Shen X (2010) Sacrificing the plum tree for the peach tree: a socialspot tactic for protecting receiver-location privacy in VANET. In: Proc. IEEE Globecom'10, Miami, Florida, USA, 6–10 Dec 2010
7. Ruj S, Cavenaghi MA, Huang Z, Nayak A, Stojmenovic I (2011) On data centric misbehavior detection in VANETs. In: IEEE 74th Vehicular Technology Conference, VTC-Fall, San Francisco, USA
8. Papadimitratos P, Buttyan L, Holczer T, Schoch E, Freudiger J, Raya M, Ma Z, Kargl F, Kung A, Hubaux JP (2008) Secure vehicular communication systems: design and architecture. IEEE Wirel Commun Mag 46(11):100–109
9. Papadimitratos P, Buttyan L, Hubaux J-P, Kargl F, Kung A, Raya M (2007) Architecture for secure and private vehicular communications. In: IEEE ITST, pp 1–6
10. Buttyán L, Holczer T, Vajda I (2007) On the effectiveness of changing pseudonyms to provide location privacy in vanets. In: ESAS. Lecture notes in computer science, vol 4572, pp 129–141
11. Freudiger J, Manshaei MH, Le Boudec J-Y, Hubaux J-P (2010) On the age of pseudonyms in mobile ad hoc networks. In: IEEE INFOCOM, pp 1577–1585
12. Calandriello G, Papadimitratos P, Hubaux J-P, Lioy A (2007) Efficient and robust pseudonymous authentication in vanet. In: Holfelder W, Santi P, Hu Y-C, Hubaux J-P (eds) Vehicular ad hoc networks, pp 19–28
13. Zhang J (2011) A survey on trust management for vanets. In: 25th IEEE international conference on advanced information networking and applications, pp 105–112
14. Easley D, Kleinberg J (2010). Networks, crowds, and markets: reasoning about a highly connected world. Cambridge University Press
15. Acemoglu D, Dahleh MA, Lobel I, Ozdaglar A (2010) Bayesian learning in social networks. Available at http://web.mit.edu/newsoffice/2010/crowd-wisdom-1115.html
16. Huang Z, Ruj S, Cavenaghi MA, Nayak A (2011) Limitations of trust management schemes in VANET and countermeasures. In: IEEE PIMRC
17. Resnick P, Zeckhauser R (2002) Trust among strangers in internet transactions: empirical analysis of eBay's reputation system. In: Baye MR (ed) The economics of the internet and E-commerce. Advances in applied microeconomics. Elsevier Science, pp 127–157
18. Dotzer F, Fischer L, Magiera P (2005) Vars: a vehicle ad-hoc network reputation system. In: IEEE international symposium on a world of wireless mobile and multimedia networks, pp 454–456
19. Lo N-W, Tsai H-C (2009) A reputation system for traffic safety event on vehicular ad hoc networks. EURASIP - Journal on Wireless Communications and Networking. doi: 10.1155/2009/125348
20. Minhas UF, Zhang J, Tran T, Cohen R (2010) Towards expanded trust management for agents in vehicular ad-hoc networks. IJCITP 5(1):3–15
21. Minhas UF, Zhang J, Tran T, Cohen R, Cheriton DR (2010) Intelligent agents in mobile vehicular ad-hoc networks: leveraging trust modeling based on direct experience with incentives for honesty. In: IEEE/WIC/ACM international conference on web intelligence and intelligent agent technology, pp 243–247
22. Raya M, Shokri R, Hubaux J-P (2010) On the tradeoff between trust and privacy in wireless ad hoc networks. In: ACM WISEC, pp 75–80
23. Schmidt RK, Leinmuller T, Schoch E, Held A, Schafer G (2008) Vehicle behavior analysis to enhance security in vanets. In: Workshop on vehicle to vehicle communications
24. Zhang J, Chen C, Cohen R (2010) A scalable and effective trust-based framework for vehicular ad-hoc networks. JoWUA 1(4):3–15
25. Adams WJ, Davis NJ (2005) Toward a decentralized trust-based access control system for dynamic collaboration. In: IEEE workshop on information assurance, pp 317–324
26. Eschenauer L, Gligor VD, Baras J (2002) On trust establishment in mobile ad-hoc networks. In: Proceedings of the security protocols workshop, pp 47–66
27. Sun YL, Han Z, Ray Liu KJ (2006) Information theoretic framework of trust modeling and evaluation for ad hoc networks. IEEE J Sel Areas Commun 24(2):305–317
28. Lu R, Li X, Liang X, Lin X, Shen X (2011) GRS: The green, reliability, and security of emerging machine to machine communications. IEEE Commun Mag (Feature topic on recent progress in machine to machine communications) 49(4):28–35

29. Li X, Li Z, Stojmenovic M, Narasimhan V, Nayak A (2012) Autoregressive trust management in wireless Ad Hoc networks. In: Ad Hoc sensor wireless networks, (to appear)
30. Marti S, Giuli TJ, Lai K, Baker M (2000) Mitigating routing misbehavior in mobile ad hoc networks. In: MOBICOM, pp 255–265
31. Michiardi P, Molva R (2002) Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks. In: Mobile ad hoc networks. communication and multimedia security
32. Fahnrich S, Obreiter P (2004) The buddy system—a distributed reputation system based on social structure. Technical report, Universitat Karlsruhe, Faculty of Informatics
33. Dewan P, Dasgupta P, Bhattacharya A (2004) On using reputations in ad hoc networks to counter malicious nodes. In: IEEE international conference on parallel and distributed systems, pp 665–672
34. Zhang J, Cohen R (2006) Trusting advice from other buyers in e-marketplaces: the problem of unfair ratings. In: 8th international conference on electronic commerce: the new e-commerce—innovations for conquering current barriers, obstacles and limitations to conducting successful business on the internet, pp 225–234
35. Gerlach M (2007) Trust for vehicular applications. In: International symposium on autonomous decentralized systems, pp 295–304
36. Minhas U, Zhang J, Tran T, Cohen R (2010) Intelligent agents in mobile vehicular ad-hoc networks: leveraging trust modeling based on direct experience with incentives for honesty, pp 243–247

Zhen Huang is currently a Ph.D student in Electric and Computer Engineering at University of Ottawa, Canada. He received his Master's degree in Electric and Computer Engineering from University of Ottawa in 2011, and B.E. degree in Communications Engineering from Southwest University of Science and Technology, China. His research interests are security in Vehicular ad hoc networks and smart grid. Mailing address is SEECS, University of Ottawa, 800 King Edward, Ottawa, ON, K1N 6N5, Canada. Email: zhuan045@uottawa.ca

Sushmita Ruj received her B.E. degree in Computer Science from Bengal Engineering and Science University, Shibpur, India in 2004, and Masters and Ph.D in Computer Science from Indian Statistical Institute, India in 2006 and 2010, respectively. Between 2009 and 2010, she was a Erasmus Mundus Post Doctoral Fellow at Lund University, Sweden. She is currently a Post Doctoral Fellow at University of Ottawa, Canada. Her research interests are in security in mobile ad hoc networks, vehicular networks, cloud security, combinatorics and cryptography. She is the Editorial Board of Ad Hoc and Sensor Wireless Networks. Her mailing address is SEECS, University of Ottawa, 800 King Edward, Ottawa, Ontario, K1N6N5 Canada. Email: sushmita.ruj@gmail.com

Marcos A. Cavenaghi has been working at Unesp - State University of Sao Paulo in Brazil since 1994. His research interests include Security in Vehicular ad hoc Networks and Wireless ad hoc Networks, Distributed Systems, and Grid Computing. Cavenaghi received a PhD in Computational Physics from USP - University of Sao Paulo, Brazil in 1997, a MsC in Sciences from USP - University of Sao Paulo, Brazil in 1992, and a BsC degree in Physics from Unesp - State University of Sao Paulo, Brazil in 1990. His mailing address is Department of Computing, Av. Luiz E.C. Coube 14-01, 17033-360 - Bauru – SP, Brazil. Email: macavenaghi@gmail.com

Milos Stojmenovic is an assistant professor at the department of Informatics and Computation at Singidunum University, in Belgrade, Serbia. He received his PhD in Computer Science degree at the School of Information Technology and Engineering, University of Ottawa, in 2008. He has published roughly thirty articles in the fields of computer vision, image processing, and wireless networks. More details can be found at www.site.uottawa.ca/~mstoj075. Mailing address: Singidunum University, Danijelova 32, 11000, Belgrade, Serbia. Email: mstojmenovic@singidunum.ac.rs

Amiya Nayak received his B.Math. degree in Computer Science and Combinatorics & Optimization from University of Waterloo in 1981, and Ph.D. in Systems and Computer Engineering from Carleton University in 1991. He has over 17 years of industrial experience in software engineering, avionics and navigation systems, simulation and system level performance analysis. He is in the Editorial Board of several journals, including IEEE Transactions on Parallel & Distributed Systems, International Journal of Parallel, Emergent and Distributed Systems, International Journal of Computers and Applications, and EURASIP Journal of Wireless Communications and Networking. Currently, he is a Full Professor at the School of Electrical Engineering and Computer Science at the University of Ottawa. His research interests are in the area of fault tolerance, distributed systems/algorithms, and mobile ad hoc networks with over 150 publications in refereed journals and conference proceedings. Mailing address School of Information Technology & Engineering, University of Ottawa, 800 King Edward Avenue, Ottawa, ON K1N 6N5, Canada. Email: anayak@site.uottawa.ca