

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
3 March 2011 (03.03.2011)

PCT

(10) International Publication Number
WO 2011/026092 A1

- (51) International Patent Classification:
G06F 17/00 (2006.01)
- (21) International Application Number:
PCT/US2010/047293
- (22) International Filing Date:
31 August 2010 (31.08.2010)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
61/238,681 31 August 2009 (31.08.2009) US
- (71) Applicant (for all designated States except US): **TELCORDIA TECHNOLOGIES, INC.** [US/US]; One Telcordia Drive 5G116, Piscataway, NJ 08854-4157 (US).
- (72) Inventors; and
- (75) Inventors/Applicants (for US only): **VAN DEN BERG, Eric** [NL/US]; 207 10th Street, Apartment 2, Hoboken, NJ 07030 (US). **ZHANG, Tao** [US/US]; 247 Harmon Avenue, Fort Lee, NJ 07024 (US).
- (74) Agents: **FEIG, Philip, J.** et al.; Telcordia Technologies, Inc., One Telcordia Drive 5G116, Piscataway, NJ 08854-4157 (US).

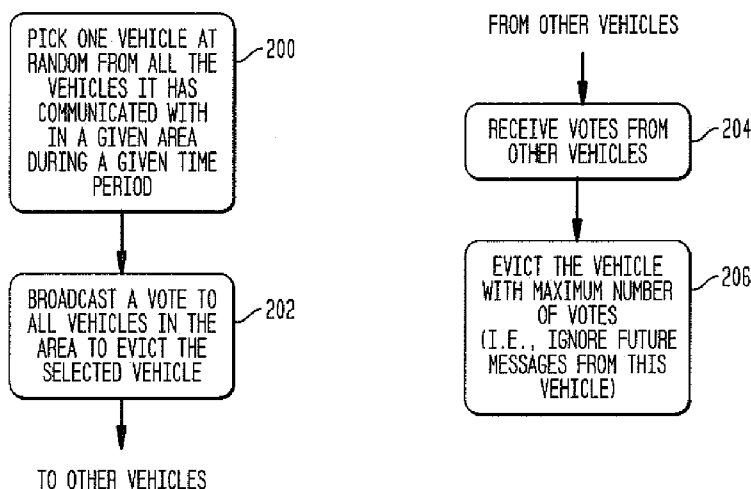
(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— with international search report (Art. 21(3))

(54) Title: SYSTEM AND METHOD FOR DETECTING AND EVICTING MALICIOUS VEHICLES IN A VEHICLE COMMUNICATIONS NETWORK

FIG. 2



(57) Abstract: In a vehicle communication network, some vehicles may be used by attackers to send false information to other vehicles which may jeopardize the safety of other vehicles. Vehicles should be able to detect malicious communications activities and to mitigate the impact of malicious vehicles by evicting (eliminating) suspected malicious vehicles from the system. Evicting a vehicle is to ignore the messages sent from the vehicle for a specified time period. Voting and sacrifice principles are combined using a mathematical model based on the "Mafia Game". The Mafia Game model focuses on the relative size of the group of attackers within a neighborhood necessary to dominate the entire network in the neighborhood (i.e., to eventually evict all the innocent vehicles).

WO 2011/026092 A1

**SYSTEM AND METHOD FOR DETECTING AND EVICTING
MALICIOUS VEHICLES IN A VEHICLE COMMUNICATIONS
NETWORK**

5 **CROSS-REFERENCE TO RELATED APPLICATIONS**

This application claims the benefit of U.S. Provisional Application No. 61/238,681, filed on August 31, 2009, which is incorporated by reference herein in its entirety.

10 **FIELD OF THE INVENTION**

The present invention relates to malicious behavior detection and malicious vehicle detection in a vehicle communications network.

15 **BACKGROUND OF THE INVENTION**

Agents interested in malicious behaviors include all entities that may engage in such behaviors and/or profit from it. These agents are grouped into three categories according to the amount of resources they may have to cause harm to the vehicular
20 network:

The first category of attackers are solitary attackers who mainly operate on their own. They have limited monetary resources and use the Internet as their main source of information. Examples of attackers in this category include: Unscrupulous or opportunistic individuals; Computer hackers; Automotive, electronic, or computer hobbyists; and Very
25 loosely organized groups.

The second category of attackers are typically one or more groups of individuals who are moderately coordinated, communicate on a regular basis, have moderate resources, can obtain information not publicly known or available. Examples of attackers
30 in this category include: Corrupt Insiders and Unscrupulous Businesses.

The third category of attackers are highly organized, have access to expansive resources, can infiltrate organizations and obtain closely held secrets, may consider life

and individuals expendable to achieve their goals, and may be supported by governing bodies of foreign nations. Examples of attackers in this category include: Organized Crime and Foreign nations.

5 Some of the potential motivations that may drive agents to exhibit malicious behaviors within a vehicular network, in an order of increasing impact, are: Sadistic pleasure in harming other vehicles or the entire vehicular network; Preferential treatment from the vehicular network for the purposes of evading law enforcement, assisting in criminal operations, or diverting attention from a primary attack; Prestige in a successful
10 hack or a new virus launch; Manipulate traffic authority decisions; Acquiring personal advantages in driving conditions or economic gain; e.g., committing insurance fraud or car theft; Promote national, political, and special interests; and Civil, political and economic disruption, including warfare.

15 Security attacks and malicious behaviors based on communications activities in a vehicle-to vehicle (V2V) communications environment can be categorized as follows:

1) Attackers could modify the communication content coming from their vehicles' software or hardware, including: inaccurate traffic conditions, including false
20 warnings related to forward collisions, blind spot situations, lane changes, unsafe passing; and inaccurate driving conditions or patterns, such as false statements about speeds, braking, directions, positions, and intersection movement.

2) Attackers could modify the communication functionalities of their vehicles' software or hardware to carry out attacks, such as one of the attacks above and the
25 following: modifying transmission timing intervals of messages; delaying the delivery of messages; sending more messages than the vehicle is designed to; not sending messages for a long enough time interval; and disabling the functioning of a vehicle's software, say, because of privacy concerns. Attackers could attempt to impersonate vehicles or other
30 network entities (e.g., servers) to cause harm to the vehicular network operations. Attackers could act as intruders and attempt to use data stored on vehicles or other network entities (e.g., servers) to cause harm to the vehicular network operations.

In order to ensure safe and secure operation of a vehicle communications system, malicious use of the certificates to cause harm to the vehicles networks and applications need to be detected so that these certificates can be revoked. Malicious vehicles used to cause significant harm to the vehicle networks and applications need to be detected and
5 “evicted” from the vehicle communications network. If vehicles have frequent infrastructure network connectivity, they can rely on trusted servers in the infrastructure network to detect and respond to security threats. These infrastructure servers could collect information from a large number of vehicles and have sufficient processing capabilities to analyze the data to detect malicious activities. However, when vehicles have sporadic or
10 zero infrastructure connectivity along the roads, attackers could perform attacks without being monitored by any highly trusted entities such as infrastructure servers. Vehicles can no longer rely on any infrastructure-based servers to help detect malicious activities. As a result, attacks will have much higher chances to be successful, and attackers would have a much higher chance of being undetected. Vehicles would have to rely on themselves and
15 interactions with other potentially untrusted vehicles to detect malicious activities and mitigate their impacts.

In V2V communications, particularly with no infrastructure network support, it is essential for the vehicles to be able to rely on themselves and distributed techniques to
20 detect malicious communications activities and to mitigate the impact of malicious vehicles by evicting (or eliminating) suspected malicious vehicle from the system (i.e., to ignore the messages sent from the suspected malicious vehicle). Such a capability allows the vehicles to communicate securely without being excessively impacted by malicious activities without relying on infrastructure network connectivity.

25 Several approaches exist in the prior art in which vehicles decide locally whether or not to evict a suspected malicious vehicle from the system. Two methods have recently been considered for V2V vehicular communications networks are: voting mechanisms, and ‘Sacrifice’ by individual vehicles, in which a suspected device is evicted together with
30 its ‘accuser’. (This is also sometimes termed “suicide for the common good”).

In a voting mechanism, such as LEAVE described by T. Moore et al. “Fast exclusion of errant devices from vehicular networks”, Proceedings IEEE SECON, San

Francisco, CA, June 16-20, 2008, vehicles vote by exchanging signed claims of impropriety of another vehicle. Each vehicle then adds these warning messages to its 'accusation list'. Once the warning votes against a vehicle exceed a threshold, the accused vehicle is placed on a 'blacklist', similar to a local or temporary certificate revocation list (CRL). For nodes which are placed on the blacklist, additional 'disregard this vehicle' messages will be broadcast to other vehicles. Typically, the majority vote principle is used to decide when to deem another vehicle untrustworthy and to send a warning message about this untrusted vehicle.

10 A majority vote detection mechanism relies on an 'honest majority': every node must have more good neighbors than bad. Therefore, local communication graph structure can have a significant effect on the dynamics of the voter model, see, e.g., V. Sood, T. Antal, S. Redner, "Voter models on heterogeneous networks", Phys. Rev. E, April 2008. Bad nodes can eliminate good nodes if they form a local majority. Good nodes can
15 eliminate bad nodes if they have a local majority. Specifically, they can send sufficiently many 'warning' and/or 'disregard' messages in LEAVE, for example.

 For V2V communications, consider the following threat model: attackers can disseminate false messages and abuse the elimination mechanism. Furthermore, multiple
20 attackers can collude.

 In a 'sacrifice' based model, any vehicle can evict any other vehicle by simultaneously agreeing to limit its own participation in future V2V communications hence giving his decision more credibility. Therefore, in this scheme it is easier to evict a
25 node than in a vote-based mechanism where a majority votes from multiple vehicles are used to decide whether to evict a vehicle. However, abuse of this mechanism is made more costly by forcing simultaneous removal of the accuser: 'Disregard' messages by an accuser cause simultaneous disregard of both the suspected node and its accuser.

30 The prior art fails to address how to determine how many malicious vehicles can the vehicle network tolerate before the innocent vehicles loss their ability to detect and evict malicious vehicles. The present invention has a provable bound on the number of malicious vehicles the system can tolerate before the system loses its ability to detect and

evict malicious vehicles. This is important for determining how long the malicious detection and eviction method can continue to run before it has to rely on other means, such as communications with infrastructure-based intrusion detection systems, to eliminate the malicious vehicles.

5

SUMMARY OF THE INVENTION

The present invention provides an approach that combines the vote and the sacrifice principles using a mathematical model called the "Mafia Game". The Mafia Game model focuses on the relative size of the group of attackers within a neighborhood necessary to dominate the entire network in the neighborhood (i.e., to eventually evict all the innocent vehicles). This combined approach does not lead to a false decision probability which the vote and the sacrifice mechanisms have to address. Furthermore, a low level of mobile or fixed infrastructure network connectivity could significantly increase the performance of the proposed approach.

In a vehicle communication network, some vehicles may be used by attackers to send false information to other vehicles which may jeopardize the safety of other vehicles. For example, a malicious vehicle may broadcast erroneous emergency break light messages to cause neighboring vehicles to think the malicious vehicle is breaking hard so the other vehicles will also have to reduce their speeds suddenly, which may cause accidents.

Vehicles should be able to detect malicious communications activities and to mitigate the impact of malicious vehicles by evicting (eliminating) suspected malicious vehicles from the system. Evicting a vehicle is to ignore the messages sent from the vehicle for a specified time period.

Such malicious behavior detection and mitigation methods can allow vehicles to communicate securely without being excessively impacted by malicious activities without relying on infrastructure network connectivity.

The present invention combines the voting and the sacrifice principles using a mathematical model based on the "Mafia Game". The Mafia Game model focuses on the relative size of the group of attackers within a neighborhood necessary to dominate the entire network in the neighborhood (i.e., to eventually evict all the innocent vehicles). This combined approach does not need to a false decision probability which the vote and the sacrifice mechanisms have to address. Furthermore, a low level of mobile or fixed infrastructure network connectivity could significantly increase the performance of the proposed approach.

The method for detecting and evicting malicious vehicles enables vehicles to have secure communications for significantly longer time, compared to prior art PKI solutions, before having to communicate with Certificate Authorities and therefore significantly reducing reliance on roadside infrastructure networks. This translates to a significantly small number of roadside network access points (base stations) that will be required to support the PKI operations for V2V communications, hence significantly reducing the costs of system deployment.

The proposed method has a provable bound on the number of malicious vehicles the system can tolerate before the system loses its ability to detect and evict malicious vehicles.

Connecting Mafia Game Theory to designing a practical PKI solution for V2V communications has not been described elsewhere.

The present invention will be better understood when the following description is read in conjunction with the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 shows a system architecture for the invention.
Fig. 2 is a flow chart of actions taken by innocent vehicles.
Fig. 3 is a flow chart of actions by detective vehicles.

DETAILED DESCRIPTION

As shown in the system architecture in Fig. 1, vehicles are classified into the following categories:

5

Malicious (Mafia) vehicles 100 are vehicles that have been detected to behave significantly differently from the behaviors designed by the vehicle manufacturers. Malicious vehicles are assumed to have full knowledge of who the other malicious vehicles in a neighborhood are. That is, collusion among malicious vehicles is possible. Through collusion, "Malicious" vehicles can create a local majority to eliminate a non-Malicious vehicle. "Malicious" vehicles can adapt their behaviors to that of Innocent vehicles so that they can postpone detection. In other words, they do not have to behave malicious all the time.

10

15

Innocent vehicles 102 are vehicles that behave as designed by the vehicle manufacturers.

Detective vehicles 104 are innocent vehicles that have the ability to detect whether another vehicle is innocent or malicious.

20

Vigilante vehicles are vehicles deemed/verified by the detective vehicles as innocent vehicles.

Resident vehicles 106 are vehicles of all categories combined in a given region or neighborhood.

25

Applying the Mafia Game model to a V2V communications network, the vehicles can be viewed to be playing a game consisting of the following iterations or rounds:

30

1) Resident vehicles' Turn: Referring to Fig. 2, all Resident vehicles pick a vehicle to eliminate by majority vote 200. Each resident vehicle votes 202 to eliminate one vehicle. The votes from the Resident vehicles are received by the other vehicles 204. The vehicle receiving the most votes is then eliminated 206. In case of a tie, a vehicle is chosen

uniformly at random from the vehicles receiving the maximum number of votes. The identity of the eliminated vehicle is revealed publicly via dissemination of a “Disregard” message.

5 2) Malicious vehicles’ Turn: Malicious vehicles choose an innocent vehicle to eliminate. The only information announced publicly by the malicious vehicles will be the identity of the vehicle eliminated and whether it was a detective vehicle or not. Again, the result can be disseminated via a “Disregard” message.

10 3) Detective’s Turn (if there are detective vehicles): Each detective vehicle acquires the Malicious or Innocent status of a vehicle. This status is then revealed only to the Detective vehicles. Detectives, for instance, can be police vehicles. Here, the Detective vehicle may collect messages from other vehicles and may communicate with infrastructure-based servers to help determine whether another vehicle is malicious or not.

15

After round t , there are $R_t = R - Zt$ Resident vehicles in the system. And the Mafia Game has two possible outcomes:

20 The “Innocent” vehicles win if all “Mafia” vehicles have been eliminated and there are still “Innocent” vehicles alive.

The “Mafia” vehicles win if all “Innocent” vehicles have been eliminated when there are still “Mafia” vehicles alive.

25 Next, here are analysis results on the performance of the scheme. For analysis purpose, the following assumptions are made:

30 a) In the game without “Detective” vehicles, assume that all “Resident” vehicles can send a message to all other Resident vehicles simultaneously. This is primarily to assure later votes are not influenced by earlier ones. Otherwise, Mafia vehicles may be able to influence the majority vote in the all-vehicle Residents round, to eliminate an Innocent vehicle with greater likelihood. This can be achieved using cryptographic protocols, for example.

b) In the game with Detectives, we assume that Residents can vote anonymously and the Residents can securely exchange messages, e.g. using a PKI system, with anonymized certificates.

5

The anonymous vote is used to coordinate votes of the Vigilante vehicles with the other (at least the Innocent) vehicles. Each Resident vehicle still announces its vote in a plurality vote. The anonymous vote is necessary to keep the identity of Vigilante vehicles unknown to non-Vigilante vehicles, in particular, unknown to Mafia vehicles. In this sense, the Vigilante vehicles are indeed an 'Anti-Mafia'. The cryptographic assumptions, in particular the anonymous pre-communication round, can be removed, if there are a simple majority of Vigilante vehicles among the Resident vehicles. This is easier to achieve when there are multiple, say d detectives: In particular, for any $\epsilon > 0$, there is a d such that d detectives have a probability of winning of at least $1 - \epsilon$ against a mafia of size $(1/2 - \epsilon) R$.

15

Now it will be shown that voting will take a bounded number of sub-rounds that is polynomial in the number of "Resident" vehicles. This assumption can be satisfied even if the vehicles' votes need to be propagated over several hops, i.e., when not all vehicles are within one-hop broadcast range with each other. Furthermore, the number of computational steps each vehicle can take between rounds is also bounded by a polynomial in the number of residents.

20

The optimal strategies in the game without detectives are given as follows:

25

Innocent Vehicle's Optimal Strategy: In iteration t , each "Resident" vehicle $1 \leq s \leq R_t$ picks a random vehicle to eliminate. As long as the "Innocent" vehicles have the majority in each Residents round, a random resident vehicle will be eliminated.

30

Malicious Vehicle's Optimal Strategy: As long as the "Innocent" vehicles have the majority, the "Mafia" vehicles may as well follow the same strategy of choosing a random innocent in each Residents round.

The following results about a network with R Resident vehicles can be derived based on analysis related to the Mafia Games:

In the game without Detectives: Malicious vehicles will surely lose if the number of them is lower than the order of \sqrt{R} , have a comparable chance of winning if the number of them is in the order of \sqrt{R} , and win if the number of them is larger than order \sqrt{R} .

In the game with $d \geq 1$ Detectives, The probability of the Malicious vehicles winning is only comparable to the Innocent's winning when there are at least ηR Malicious vehicles, for some constant η that satisfies $0 < \eta \leq 1$.

The above results provide several significant insights that provide a solid foundation for designing a V2V security system without roadside infrastructure networks. These insights include, for example, if it is possible to design a malicious vehicle detection and eviction approach so the number of malicious vehicles is kept below their critical mass (for example in the order of \sqrt{R} or ηR with zero or one Detective vehicle), the system will be able to quickly evict the malicious vehicles and maintain safe and secure communications continuously. Also, the addition of a single infrastructure node can significantly decrease the power of Malicious vehicles.

20

Establishing a 'white list' of vigilante vehicles, which are known innocent vehicles rather than distributing more "Disregard" messages or CRLs is a more effective approach to increase the chance of winning for the Innocents.

25

Furthermore, the suicide of the Detective is particularly powerful, as opposed to the solitary act considered in other mechanisms. This solitary sacrifice is one interpretation of the elimination process after majority vote, which bypasses the need to model false decision probabilities.

30

With one Detective vehicle, the optimal game for the Innocent vehicles will be the following:

Suppose there is a single Detective vehicle. Referring to Fig. 3, during the first $\sqrt{\eta R}$ rounds, the detective collects information about vehicles at random 300. The other Innocents vote in each round to eliminate a vehicle at random. After $\sqrt{\eta R}$ rounds, the Detective compiles a list \mathbf{V} of so-called "Vigilante" vehicles that are vehicles known to be Innocents 302. At this stage, the number of Vigilantes $|\mathbf{V}|$ should be larger than the number of Malicious (Mafia) vehicles $|\mathbf{M}|$ (since $\sqrt{\eta} > \eta$ for $0 < \eta < 1$). The group of Vigilantes acts as an "anti-Mafia". The Detective encrypts the list of Vigilantes, and sends the encrypted list to each member of \mathbf{V} so that the Vigilantes know which vehicles are also Vigilantes 304. The Detective then asks everyone to eliminate him. Upon being eliminated, the identity of the Detective is revealed, and therefore each Vigilante knows that the messages and encrypted list they have received is genuine.

Once the detective is evicted, in each round, the highest ranking (numbered) member of \mathbf{V} selects a member outside of \mathbf{V} to be eliminated, and communicates to the other members of \mathbf{V} the identity of the vehicle to be eliminated, say p . All Innocent vehicles abstain from voting in a secure anonymous vote to coordinate/select the next vehicle p to eliminate. After this pre communication round, every non-Mafia vehicle sends a 'Disregard- p ' message..

This shows that a single Detective vehicle can significantly increase the number of Malicious vehicles needed to dominate the game to ηR , $0 < \eta < 1$ from \sqrt{R} .

Therefore, an enhanced malicious vehicle detection and eviction method is as followings:

- [1]. Consider an arbitrary geographical region.
- [2]. Time is divided into time periods of equal or variable lengths.
- [3]. For each time period:
 - a. The Resident vehicles in the region pick one vehicle to eliminate by majority vote. Each Resident vehicle picks one vehicle it wants to eliminate and sends out

its vote in a message to other vehicles. The vehicle receiving the most votes is eliminated. In case of a tie, a vehicle is chosen uniformly at random from the vehicles receiving the maximum number of votes. The identity of the eliminated vehicle is revealed publicly via dissemination of a “Disregard” message. If the eliminated vehicle is a Detective vehicle,
 5 this fact is revealed as well.

b. For each time period T: Each Detective vehicle acquires the “Malicious” or “Innocent” status of a single randomly selected vehicle. This status is then revealed only to the Detective vehicles. Here, the Detective vehicle may collect messages from other
 10 vehicles and may communicate with infrastructure-based servers to help determine whether another vehicle is malicious or not.

[4]. During the first $\sqrt{\eta R}$ time periods (rounds), the Detective vehicle compiles and maintains an up to date “white list” \mathbf{V} of “Vigilante” vehicles. At this stage, the
 15 number of Vigilantes $|\mathbf{V}|$ should be larger than the number of Malicious vehicles $|\mathbf{M}|$ (since $\sqrt{\eta} > \eta$ for $0 < \eta < 1$). The Detective vehicle encrypts the white list of Vigilantes and sends the encrypted list to each member of \mathbf{V} so that the Vigilante vehicles know which other vehicles are also vigilantes. The Detective vehicle then asks other vehicles to eliminate itself by sending out a “Disregard” message revealing its own identity. Upon
 20 being eliminated, the identity of the detective is revealed, and therefore each Vigilante vehicles know that the messages and encrypted list white list” they have received is genuine.

[5]. Once the Detective vehicle is evicted, the white list of Vigilante vehicles is
 25 known to be genuine, and can be acted upon. In each time period (round), the highest ranking (numbered) member of \mathbf{V} selects a member outside of \mathbf{V} to be eliminated by sending a “Disregard” message to all vehicles in \mathbf{V} . All innocent vehicles abstain from voting in a secure anonymous vote to coordinate on the next vehicle p to eliminate. All Vigilante vehicles vote for p . After this round, all vehicles vote for p in the majority vote,
 30 and ‘Disregard- p ’ messages are sent. This shows that a single Detective vehicle to significantly increase the number of malicious vehicles needed to dominate the game to ηR . $0 < \eta < 1$ from \sqrt{R} .

Various aspects of the present disclosure may be embodied as a program, software, or computer instructions embodied in a computer or machine usable or readable medium, which causes the computer or machine to perform the steps of the method when executed
5 on the computer, processor, and/or machine.

The system and method of the present disclosure may be implemented and run on a general-purpose computer or computer system. The computer system may be any type of known or will be known systems and may typically include a processor, memory device, a
10 storage device, input/output devices, internal buses, and/or a communications interface for communicating with other computer systems in conjunction with communication hardware and software, etc. A module may be a component of a device, software, program, or system that implements some “functionality”, which can be embodied as software, hardware, firmware, electronic circuitry, or etc.

15

The terms “computer system” and “computer network” as may be used in the present application may include a variety of combinations of fixed and/or portable computer hardware, software, peripherals, and storage devices. The computer system may include a plurality of individual components that are networked or otherwise linked to
20 perform collaboratively, or may include one or more stand-alone components. The hardware and software components of the computer system of the present application may include and may be included within fixed and portable devices such as desktop, laptop, server, and/or embedded system.

25

While there has been described and illustrated a system and method for detecting and evicting malicious vehicles in a vehicle communication network, it will be apparent to those skilled in the art that modifications and variations are possible without deviating from the principles and broad teachings of the present invention which shall be limited solely by the scope of the claims appended hereto.

CLAIMS

What is claimed is:

1. A method for vehicles to detect and evict malicious vehicles in a vehicle-to-vehicle communications network using the Mafia Game theory, comprising: malicious mafia vehicles that have been detected to behave significantly differently from the behaviors designed by the vehicle manufacturers, innocent vehicles that behave as designed by the vehicle manufacturers, vigilante vehicles that are deemed or verified by a detective vehicle as an innocent vehicle which is a vigilante vehicle, and detective vehicles that are innocent vehicles that have the ability to detect whether another vehicle is an innocent vehicle or a malicious vehicle, or a vigilant vehicle, where resident vehicles are vehicles of all categories in a region.
2. The method of claim 1, wherein time is divided into periods and during each time period the innocent vehicles will pick a vehicle to eliminate by majority vote and each innocent vehicle votes to eliminate one vehicle in each time period.
3. The method of claim 1, wherein each innocent vehicle receives votes from other vehicles in each time period and eliminates the vehicle that has received the most votes, in case of a tie, a vehicle is chosen uniformly at random from the vehicles receiving the maximum number of votes.
4. The method of claim 1, wherein a vehicle reveals the identity of the eliminated vehicle by sending a "DISREGARD" message to all other vehicles in the region.

5. The method of claim 1, wherein malicious vehicles can also behave as the innocent vehicles and choose an innocent vehicle to eliminate in each time period.
6. The method of 5, wherein a malicious vehicle reveals the identity of the vehicle eliminated and whether the eliminated vehicle was a detective vehicle or not by sending a "DISREGARD" message to other vehicles.
7. The method of claim 1, wherein each detective vehicle acquires the malicious or innocent status of a vehicle and then reveals the status to only other detective vehicles by sending a secure message to the other detective vehicles.
8. The method of claim 1, wherein during the first $\sqrt{\eta R}$ time periods where R is the total number of vehicles in the region and η is a constant value between zero and one, a detective vehicle compiles and maintains an up to date "white list" of vigilante vehicles, encrypts the up-to-date white list or changes to the white list, and sends the encrypted list to each vigilante vehicle on the white list.
9. The method of claim 8, wherein the detective vehicle requests other vehicles to eliminate itself and reveals its identity by sending a "DISREGARD" message to the other vehicles.
10. The method of claim 1, where in each time period, the highest ranking numbered member of V selects a member outside of V to be eliminated, and communicates to the other members of V the identity of the vehicle to be eliminated, say p where all innocent vehicles abstain from voting in a secure anonymous vote to coordinate/select the next vehicle p to eliminate after this pre-communication round, every (non-Mafia) vehicle sends a 'Disregard-p' message.

1/2

FIG. 1

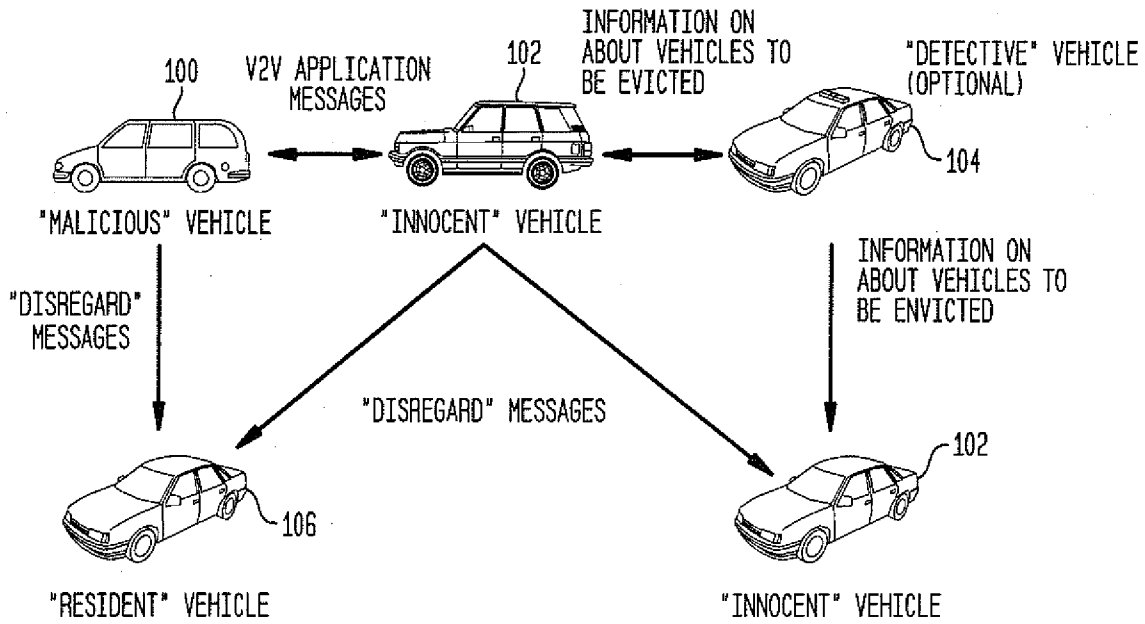
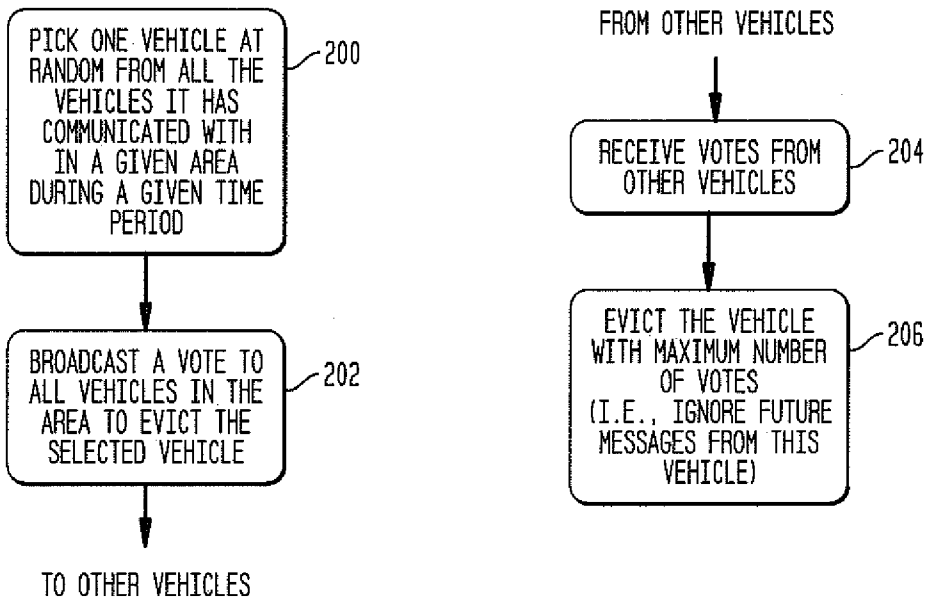
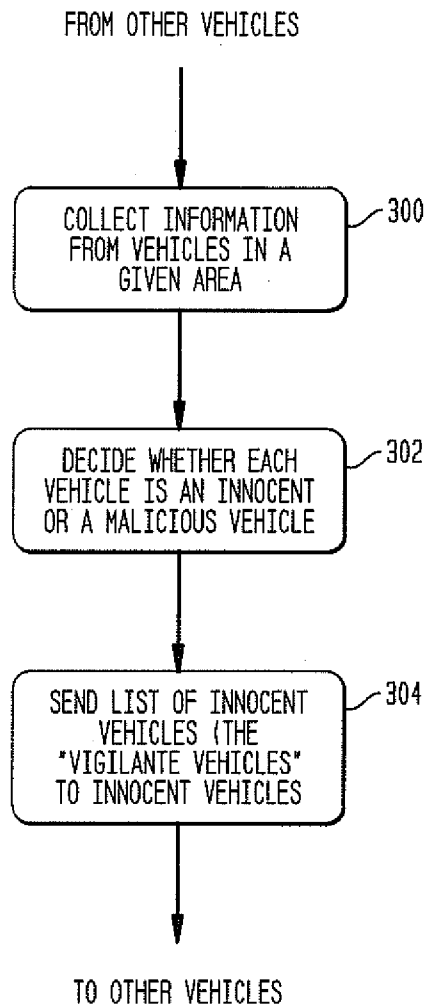


FIG. 2



2/2

FIG. 3



INTERNATIONAL SEARCH REPORT

International application No.

PCT/US2010/047293

A. CLASSIFICATION OF SUBJECT MATTER IPC(8) - G06F 17/00 (2010.01) USPC - 340/500 According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED Minimum documentation searched (classification system followed by classification symbols) IPC(8) - G06F 15/16; G06F 17/00 (2010.01) USPC - 340/500; 707/10 Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched Electronic data base consulted during the international search (name of data base and, where practicable, search terms used) PatBase, Google Scholar		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	BRAVERMAN et al. MAFIA: A THEORETICAL STUDY OF PLAYERS AND COALITIONS IN A PARTIAL INFORMATION ENVIRONMENT. The Annals of Applied Probability. 2008. [retrieved on 2010-10-14]. Retrieved from the Internet: <http://arxiv.org/pdf/math.PR/0609534>. pages. 1-23	1-10
Y	MOORE et al. Fast exclusion of errant devices from vehicular networks. Sensor, Mesh and Ad Hoc Communications and Networks, 2008 (Publication data at <http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4557749&tag>). [retrieved on 2010-10-14]. Retrieved from the Internet: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.140.4054&rep=rep1&type=pdf>. pages 1-9	1-10
A	SOOD et al. Voter models on heterogeneous networks. Phys. Rev. E. 22 April 2008 (22.04.2008) [retrieved on 2010-10-14]. Retrieved from the Internet: <http://www.ncbi.nlm.nih.gov/pmc/articles/PMC2471880/>. pages 1-14	1-10
<input type="checkbox"/> Further documents are listed in the continuation of Box C. <input type="checkbox"/>		
* Special categories of cited documents: "A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier application or patent but published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "&" document member of the same patent family		
Date of the actual completion of the international search 14 October 2010		Date of mailing of the international search report 26 OCT 2010
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201		Authorized officer: Blaine R. Copenheaver PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774