Collaboration-based Misbehavior Detection System in Hybrid Vehicular Ad Hoc Networks

Nai-Wei Lo* and Tsung-Hao Hsu†
Dept. of Information Management
National Taiwan Univ. of Science and Technology
Email:nwlo@cs.ntust.edu.tw*, M9609008@mail.ntust.edu.tw†

***Abstract*—Hybrid vehicular ad hoc network (VANET) will become one of the most important dynamic communication infrastructures for human's daily life in the next decade. A hybrid VANET is composed of mobile vehicles and static road-side units (RSU) in which information is distributed among them by transmitting messages through shared wireless communication channels. Useful applications for entertainment, banking, traffic safety, etc. can be deployed onto the hybrid VANET infrastructure. As wireless technology is vulnerable to various malicious attacks, hybrid VANET also suffers from similar security threats, especially the threats from malicious vehicles. In this paper, a misbehavior detection system called MEDIA is developed to mitigate the effect of message random-dropping attack, which is a stereotype of security attack and very easy to launch by a malicious vehicle. Based on collaboration concept, the proposed system can be installed in vehicles and RSUs to monitor vehicles, detect malicious ones and isolate these vicious vehicles. The simulation results show that the MEDIA system can isolate malicious vehicles effectively, increase the data packet delivery ratio and reduce the number of control packets sent even up to 40% of vehicles are malicious in a hybrid VANET.**

***Index Terms*—Hybrid VANET, Information Security, Misbehavior Detection System**

I. Introduction

Many academic and industrial researchers have focused on vehicular ad hoc networks (VANET) about routing and security issues in recent years [1], [2]. In a VANET environment each vehicle installs a wireless on-broad unit (OBU) to communicate with other vehicles within its wireless transmission range. Advanced applications such as online gaming, Web services and real time traffic information can be easily supported through the VANET environment to drivers.

Hybrid VANET consists of mobile vehicles and static road-side units (RSU), i.e., wireless base station. These RSUs and vehicles may share information through the infrastructure of hybrid VANET. As the cost to build a hybrid VANET infrastructure is high, usually it will be constructed in urban area where the heavy traffic flow provides solid demand on advanced VANET applications.A RSU can be built along a roadway. The density of RSUs is a demand-oriented customizable parameter.

Along with many advanced applications in VANET, many institutions focus on the establishment of intelligent transportation systems (ITS) [3], [4], [5] to provide real time traffic information for drivers and alleviate the occurrence possibility of traffic accidents. In a traffic safety application system, vehicles can communicate with each other to offer current traffic condition around several street blocks. When a driver encounters a traffic accident or abnormal traffic situation, his vehicle will send warning messages to notify other nearby vehicles over its OBU device. The other vehicles can make an appropriate decision based on received warning messages.

As drivers take actions based on received traffic messages from their ITS system, how to secure the content of transmitted messages, the communication mechanism and the utilization of the shared wireless channel in VANET has become an important issue. To eliminate the attack effect from malicious vehicles, many misbehavior detection systems utilizing authentication technique and encryption mechanism are proposed [6], [7], [8], [9], [10], [11], [12] to solve malicious attacks such as eavesdropping and message dropping in a VANET environment In this study, we are focusing on more complicated security attacks such as message random-dropping attack in which a malicious vehicle randomly chooses re-

ceived messages and drops them instead of forwarding them to their destinations in order to obstruct message propagation and delivery.

Although similar topics have been investigated in MANET [13], [14], [15], [16], [17], [18], the difference of network characteristics between MANET and VANET has made the difficulty to directly adopt these MANET solutions to a VANET environment.

For this reason, we propose a novel misbehavior detection system to mitigate the influence of message random-dropping attack in a hybrid VANET environment. The proposed system uses RSUs and vehicles to monitor message transmission behavior of their neighbor vehicles. Based on the collected misbehavior data from vehicles and RSUs, each RSU starts to evaluate suspicious vehicles, identify malicious vehicles and broadcast the blacklist of malicious vehicles to isolate them in a VANET environment. We utilize network simulator to evaluate the performance of this proposed system. The simulation results show that the proposed system can alleviate the message random-dropping attack effectively.

The rest of this paper is organized as follows. We first review related work in Section II. In Section III, a misbehavior detection system called MEDIA is presented to defend against message random-dropping attack in hybrid VANETs. In Section IV, experimental simulations are conducted to evaluate the effectiveness of MEDIA system. Finally, Conclusion is given in Section V.

II. Related Work

Wang and Huang [13] proposed a novel fuzzy logic based reputation system to perform the routing path decision in order to choose a feasible routing path in a MANET environment where selfish and malicious nodes do not forward data packets normally. The system uses fuzzy logic to perform routing decision. It chooses the feasible path according to three factors: node reputation, bandwidth and hop count. Their simulation results showed that the proposed system can enhance routing efficiency in MANET. However, this paper mainly focuses on routing path selection.

Fonseca and Festag [1] described the security issues are crucial to VANET environment and they have presented several secure ad hoc routing protocols and categorized various types of routing attacks. The authors described systematically the existing approaches for secure routing. Then, the authors analyzed security requirements of VANET and summarized applicability of these secure approaches in VANET. In this paper, the authors concluded that there is more to be done in terms of VANET security in order to identify new attacks and explore the corresponding solutions.

Dotzer et al. [19] proposed a security system called VARS for VANET environment. The system determines a vehicle is legal or not depending on vehicle's behavior. If a vehicle does not forward packets, the system will detect its behavior. The system gives each target vehicle a direct trust value, and it also collects indirect trust value of target vehicle from other vehicles. The system computes the final trust value of target vehicle based on direct and indirect trust values. Finally, if the final trust value of target vehicle is lower than the trust threshold, the target vehicle will be judged as a malicious vehicle and isolated by the system.

Wang and Chigan [6] proposed a cooperation enhancement mechanism to prevent misbehaved relay action from a malicious vehicle which tries to tamper message contents during its message relay operation. The mechanism uses neighborhood watchdog to generate trust token that can detect and prevent malicious relaying vehicles to modify messages. A vehicle considers the received message trustable based on this token. Wang et al. use public key and digital signature to ensure authentication and message integrity to avoid this token been modified by malicious vehicles. In performance evaluation, the results showed the mechanism can detect and prevent malicious vehicles from modifying messages during relay transmission effectively. In this paper, the authors explained the mechanism lacks incentive to encourage nodes behaving well and it has deployment limitation in VANET. Also this paper did not consider the situation that many packets need to be relayed at the same time in VANET.

Raya et al. [7] proposed a protocol utilized in a security framework to defend against message fabrication attack. The protocol can identify and isolate misbehaving and faulty vehicles effectively.

The framework contains components such as misbehavior detection system (MDS) and local eviction of attackers by voting evaluators protocol (LEAVE). MDS is performed individually by each vehicle. When each vehicle receives message from neighbors, it will compare with an evaluation rule to classify the message is safe or not. If the comparison result shows misbehavior, MDS will pass information to LEAVE. LEAVE is a collective warning system against misbehaving vehicles. Once LEAVE receive enough reliable accusations, it reports attackers to certification authority (CA) right away. Because each vehicle is registered with CA, CA can revoke communication ability of each vehicle. Besides, the communications between each vehicle and CA is over RSUs, other base stations or FM radio equipments. RSU is a communication gateway between vehicles in VANET and CA. This paper assumed the existence of honest majority in terms of vehicles in VANET. This allows vehicles to rely on their honest neighbors in order to evict attackers. The performance from simulation results shows this protocol isolates attackers efficiently.

III. Misbehavior Detection System

Hybrid VANET establishes ITS to provide traffic information for driver and it may decrease occurrence of traffic accident. It is usually formed in urban area or highway since there usually have high vehicle flow and leads to busy and congested. In this paper, the environment we just discuss in urban area. In order to mitigate influence includes damages of life and environment from attack such as message random-dropping attack in hybrid VANET, we use RSU equipments and vehicles to monitor each vehicle behavior of message transmission collaboratively and RSU makes a final decision to decide which one vehicle is convicted. This is reasonable to let RSU as a decision maker because RSU is a trustable infrastructure. It is established and managed by government or lawful company. Besides, RSU can build at roadside everywhere depending on development cost and needs. In our paper, we build RSU at each intersection. RSU at intersection may observe more vehicles because urban area usually has high vehicle flow and traffic light at intersection may causes vehicle to stop. Besides, the distribution of vehicle is almost uniform in general and intersection has high degree of road. Therefore, RSU may have more observations to evaluate each vehicle accurately in this environment.

Our system environment assumes each RSU connects a central database server (CDS). The CDS records vehicle information about message transmission behaviors, trust value and blacklist. For vehicle, each vehicle installs a wireless on-broad unit (OBU). The OBU has wireless communication ability and it can communicate with other OBUs within its wireless transmission range. Each OBU in vehicle has behavior record table (BRT) individual. The function of BRT is the same with CDS. It records nearby vehicles information about message transmission behaviors, trust value and blacklist. Each vehicle provides information for RSU to assists to evaluate vehicles. And then RSU makes a corresponding decision for vehicle. Transmission range of RSU and vehicle are denoted a circle of dotted line. Each RSU and vehicle can communicate with each other within their wireless transmission range.

However, in this paper, there have two assumptions in the following: (1) a majority of vehicles are honest, (2) all timers in RSUs and the CDS are synchronized at every fixed period of time. An honest vehicle will not send false information in their messages to mislead receiver's behavior. Therefore, each vehicle and each RSU can accept accurate information from honest vehicles.

In the following subsections, we introduce the attack model, the misbehavior detection system architecture and the system operation flow.

A. Attack Model

The issue about protecting message securely during transmission is more necessary. Each vehicle sends traffic message with each others to offer traffic condition that drivers and passengers are interested in. In general situation, drivers make actions based on traffic message. When drivers receive warning message about traffic condition, they will detour to avoid through warning place or slow down to pass through warning place cautiously. So, it is a message-oriented environment in hybrid VANET. If the environment suffers from attack that resists the message propagation, drivers can not receive this message and can not make a corresponding action.

It may cause traffic accident to endanger drivers' and passengers' safety. So, for eliminating this influence, we focus is misbehavior of transmission message in this paper.

The misbehavior of transmission message has many types of attack. They can make huge effects to decrease performance of transmission in hybrid VANET and endanger life. Based on this reason, there has more attentions about security issues and proposes many misbehavior detection systems to mitigate this problem. However, attack will also become complicated. Each malicious vehicle wants to escape the detection of misbehavior detection system. So, malicious vehicles lead to do some complicated attacks. In our paper, we just discuss the most stereotype of attack that is message random-dropping because this attack is lunched by malicious vehicles easily. This attack selects message randomly to drop because it can disrupt the message propagation to interfere judgment of driver and may cause severe traffic accident and casualty. The problem seems to be a potential security threat. The purpose of this attack is lunched by malicious vehicles in hybrid VANET in the following: (1) a malicious vehicle does not want to provide information about traffic condition to driver or save its resource, so it does not send message normally and desires to make damages from traffic accident; (2) a malicious vehicle drops message randomly because this attack is lunched easily by malicious vehicle to escape the detection of misbehavior detection system.

We do not consider misbehavior of fabricated message because this security issue had discussed and resolved by many researchers [7], [8]. Also we do not consider masquerading attack as we assume each vehicle has unique vehicle ID and the vehicle ID is secure in OBU.

B. System Architecture

This system defends against this attack using collaboration between RSU and vehicle. Vehicle assists RSU to make an appropriate decision for malicious vehicles. The architecture of the misbehavior detection system is shown in Figure 1. The system is divided into four modules: monitoring module, evaluation module, decision module and action module. The misbehavior detection system also called MEDIA. MEDIA provides two versions for RSU and vehicle based on its needs. Each vehicle has monitor and evaluation module in MEDIA and each RSU has all of modules in MEDIA. Vehicle only needs two modules to work in this system and it can offer cheaper cost of system setup for driver. RSU plays a major role in this system. It may collect more traffic information to control entire traffic condition because it is static built at roadside and connect a central database. The arrow is represented the procedure in system and dotted arrow is represented the process of communication from vehicle to RSU. RSU receives results of evaluation module from vehicle to make an appropriate decision.

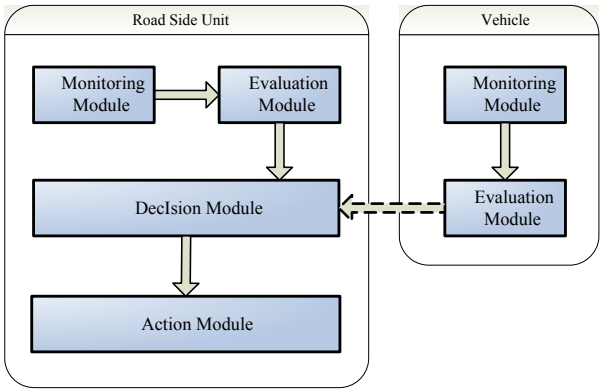

Fig. 1. MEDIA system architecture.

Initially, in monitoring module, each vehicle and RSU act as an observer. Observers have a monitor ability to collect information about message transmission behaviors of neighbor vehicles in its own BRT and CDS. After a period of time in monitoring module, observers execute their next modules in MEDIA that is evaluation module. According to their observations, each vehicle and RSU evaluates trust value of neighbor vehicles individual in evaluation module. Then, each vehicle will contact with RSU and transmit its evaluation results to RSU. The RSU receives the evaluation results from vehicles and stores them in CDS to execute a corresponding process in decision module. However, if vehicle can not contact with RSU successfully, it will keep driving and transmit this result until it contacts with RSU. If RSU receives duplicate results about vehicle, based on our assumption, RSU can utilize the latest result to update in CDS.

In decision module, there have two filtering mechanisms to discover a malicious vehicle and make a corresponding action. RSU identify obvious malicious vehicles by majority in the first filtering mechanism. It can let RSU to execute action module directly and isolates the malicious vehicles. This is an objective action because it takes into account other opinions. It is not arbitrary to announce vehicle that is convicted and it is fair for vehicle. To discover unobvious malicious vehicles, RSU utilizes an integration policy to integrate trust value from vehicles with it and execute the second filtering mechanism to detect malicious vehicles again. When RSU discover malicious vehicles in the second filtering mechanism, it executes an isolation action in action module.

Finally, when RSU is aware a malicious vehicle, it executes the isolation action for the malicious vehicle to add a record about vehicle information to blacklist in CDS and sends the blacklist to neighbor vehicles. On the contrary, if RSU is unaware a malicious vehicle, MEDIA will operate repeatedly from the beginning. When each vehicle receives the blacklist, it will store the blacklist record in BRT and do not transmit any message to malicious vehicles. For this reason, MEDIA can isolate malicious vehicles to avoid making huge damages because malicious vehicles can not receive any message to drop message selectively. However, in other to encourage malicious vehicles to forward message collaboratively, each blacklist record has an expiration time. When the expiration time reaches, system will erase the blacklist record and release the malicious vehicle. Then, each vehicle will start to send message to it. Each malicious vehicle has a chance to correct past error and becomes legal. Each module of MEDIA is elaborated in following sections.

C. System Operation Flow

1) Monitoring Module: Each vehicle and RSU has a monitoring module in MEDIA and they act as observers. This module is activated all the time in an observer and monitoring range is determined by the equipped wireless device. Because this module is activated all the time in an observer, we define an ET that is the time period between two consecutive invocations of the next evaluation module in an observer. Observers execute their evaluation modules after each ET period of time is passed.

Observes observe each expected message transmission behavior of nearby vehicles. The expected behavior is a normal message transmission behavior based on protocol model. Depending on normal protocol model, observers will observe nearby vehicles behavior of received and transmitted messages.

When vehicle moves within observers' monitoring range, observers record information about the message transmission behaviors in its own BRT and CDS.

Each vehicle stores a message transmission behavior as an observed behavior record in BRT individual and each RSU stores in CDS. The format of the observed behavior record includes packet ID, current node ID, next node ID, source node ID, destination node ID, and message timestamp. Each packet has its own packet ID. The other fields indicate the packet transmission information. Then, they will accumulate the number of observations for vehicle i that is denoted NO_i. This is because this parameter provides the credibility for evaluation result in next module. If observer monitors the vehicle i for a long time, it may has collect many monitor results for vehicle i and the value of NO_i is high. It indicates the following evaluation results may has high credibility and relatively fit to vehicle.

Then, observers compare the transmission behavior with each observed behavior record in their BRT or CDS by a comparing rule. This is because observers can distinguish between normal and abnormal behavior. Based on the comparing rule, observers erase the normal behavior records that fit for the rule to release space and keep abnormal behavior records that unfit for the rule to wait for check again in it own BRT and CDS.

2) Evaluation Module: This module computes the trust value of each observed vehicle based on observed behavior records from the monitoring module. The trust value is to measure the vehicle trustable or not. Because each vehicle and RSU collects message transmission behavior information of vehicle individually from monitoring module, they may have different opinions to evaluate trust value for vehicle.

The procedure of the evaluation module is described as follows. First, to compute the message

dropping rate for vehicle i denoted MDR_i, observers need to execute a evaluation rule. Then, observers enforce a trust value regulation policy based on MDR_i to determine how to utilize trust value management formulas in order to compute trust value of vehicle.

Since the observed behavior record in their tables from monitoring module keep abnormal records, observers can search each observed behavior record in its own storage space and accumulate the number of misbehaviors for vehicle i denoted SNM_i during the time period ET and the total number of misbehaviors for vehicle i denoted LNM_i for computing MDR_i based on an evaluation rule. The SNM_i parameter indicates a short-term record and the LNM_i parameter is a long-term record.

The computation formula of MDR_i is shown in Equation 1. The MDR_i is represented the ratio about doing misbehavior for vehicle i in the past time. Using this parameter indicates the behavior trend of vehicle i in the past time and reasons vehicle behavior in future. If the MDR_i is high, it means that vehicle has discarded a lot of messages in the past time and can predict that vehicle will drop message possibly in future. On the other hand, if the MDR_i is low, vehicle has not discards a lot of messages in the past time and the vehicle is reliable possibly in future because it has low opportunity to drop message.

$$MDR_i = LNM_i / NO_i \tag{1}$$

Since BRT in vehicle has a capacity limitation. It will also refresh out of date observed behavior record in a period of time to avoid BRT overflow that leads to increase burden of vehicle. The overflow problem causes vehicle can not store any observation and make latest decision. And then, it degrades detection performance of MEDIA and can not discover malicious vehicles effectively.

After computing these parameters, we utilize a trust value regulation policy based on MDR_i to determine how to evaluate the trust value of vehicle in trust value management formula. Besides, observers enforce the policy to mitigate false positive problem. If MDR_i is also more than message dropping rate threshold, it represents the vehicle i to drop message frequently. However, if observer discovers an event that is NO_i more than the number of observations threshold, it indicates the observer has monitored vehicle for a long time and MDR_i is much fit vehicle behavior. Then, when above conditions approve, it determines to decrease the trust value of vehicle to punish in trust value management formula. The formula of decrement is shown in Equation 2.

$$TV_k^i = TV_k^i - (EM\_Weight \times SNM_i) \tag{2}$$

In Equation 2, it means the past behavior of vehicle will impact behavior in future. TV_k^i is a trust value of vehicle i from observer k and it is a decimal and range is 0 to 2. Initially, each vehicle is neutral status. The initial trust value of them is 0.5. The EM_Weight is an evaluation weight about punishment level. It is a decimal and the range is 0 to 1. In this system, this parameter can adjust dynamically depending on evaluation level. If the system wants to set high punishment level, it can set the parameter close to 1. The formula shows an event TV_k^i will decrease obviously when SNM_i increases. Finally, it sets SNM_i to zero and recalculate the SNM_i in next a period time ET.

The system has a punishment policy for vehicle in Equation 2. However, it also needs encouragement policy for vehicle. So, on the other hand, when one of above condition is unapproved, observers determine to increase the trust value of vehicle in trust value management formula. The formula of increment is shown in Equation 3:

$$TV_k^i = TV_k^i + EM\_Weight \tag{3}$$

The trust value of vehicle will increase. Because the maximum value of TV_k^i in the system is 2, it does not increase unlimited. According to Equations 2 and 3, we know the effect of punishment more than encouragement. This is because it multiplies an evaluation weight to decrease trust value of vehicle and reminds vehicle do not uncooperative arbitrarily.

To let the trust value more accurate, there is existed a recommendation mechanism among vehicles. Each vehicle sends recommendation messages about trust value to nearby vehicles and recalculates trust value. This mechanism lets observer to evaluate trust value of vehicle objectively. The formula of computation from recommendation mechanism is in

Equation 4.The TV_r^i means trust value of vehicle i from recommender r's point of view. The TV_k^r means trust value of recommender r from observer k's point of view.

$$TV_k^i = Recom\_Weight \times TV_k^i + \frac{(1-Recom\_Weight)}{2} \times TV_k^r + \frac{(1-Recom\_Weight)}{2} \times TV_r^i \quad (4)$$

In Equation 4, in addition to consider opinion from recommender to target vehicle, the observer considers opinion from it to recommender. Using TV_r^i and TV_k^r as an indirect opinion integrates the original trust value. The $Recom\_Weight$ is a recommendation weight and it is a decimal and range is 0 to 1. This parameter sets more than 0.5 because the direct opinion is mainly. However, in this situation, it may have a recommendation problem. The recommendation problem means an event that recommender provides false recommendation to observer and lets observer confused to make false decision. But, it is not our major work to check recommendation is reliable or not. Each vehicle has high possibility to receive honest recommendation from recommender under our assumption that a majority of vehicles are honest. Besides, we can utilize previous researches to defend against the recommendation problem [20], [21].

3) Decision Module: After each vehicle evaluates trust value, it will contact and send evaluation results to the nearest RSU. Vehicle sends evaluation results to RSU when it is within transmission range of RSU. RSU is an important role in this system. It collects evaluation results from vehicles to detect malicious vehicles and makes an appropriate decision for the vehicle.

We utilize the first filtering mechanism to identify obvious malicious vehicles. Then enforce an integration policy and execute the second filtering mechanisms to discover complicated malicious vehicles that pass the first filtering mechanism.

The vote filtering mechanism is to avoid RSU makes decision arbitrarily. It makes decision by majority. Using the majority policy reaches an agreement and provides a fair judgment for vehicle. When RSU receives evaluation results from vehicles, it will compare the results with a first filtering threshold. This parameter is not defined empirically and can adjust dynamically depending on detection effect. The purpose of this mechanism will enable RSU to detect obvious malicious vehicles early. If the result is less than the first filtering threshold, it means the vehicle to be too bad. Then, the RSU accumulates the number of votes for vehicle and starts voting timer.

When the voting timer is expired, the RSU makes a corresponding decision based on voting results. The voting scheme has a voting threshold. If the number of votes reaches the voting threshold, RSU ensures the vehicle to be malicious because a certain group of vehicles. Then, RSU has an explicit decision and executes action module to isolate malicious vehicles directly.

To discover unobvious malicious vehicles, RSU utilizes a trust value integration policy to integrate trust value from vehicles with it and execute the threshold filtering mechanism to detect malicious vehicles again. The trust value integration policy in RSU is in Equation 5.

For (k=1; $k\leq$the number of trust value of vehicle$i$; k++)

$$TV_{RSU}^i = IM\_Weight \times TV_{RSU}^i + (1-IM\_Weight) \times TV_k^i \quad (5)$$

TV_{RSU}^i is the trust value of vehicle i that is evaluated by RSU. IM_Weight is an integration weight and it is a decimal and range is 0 to 1. This parameter can adjust dynamically depending on integration level. In our system, we set this parameter more than 0.5 because the RSU is a trustable infrastructure. It is established and managed by government or lawful company. According to Equation 5, if TV_{RSU}^i or TV_k^i decreases, TV_{RSU}^i will decrease. On the other hand, if TV_{RSU}^i or TV_k^i increases, TV_{RSU}^i will increase. After RSU making an integration policy, it can execute the threshold filtering mechanism to discover complicated malicious vehicles that pass the vote filtering mechanism.

In threshold filtering mechanism, RSU compares the trust value of vehicle with a second filtering threshold. This threshold also can adjust dynamically to identify malicious vehicles depending on detection effect and it is a decimal and range is 0 to 1. If the comparison result is less than the second filtering threshold, RSU makes an isolation action in action module because it verifies a fact that vehicle is a malicious vehicle. But, if the comparison result

is more than the second filtering threshold, it means the vehicle may be legal and do not execute isolation action.

4) Action Module: It is the final step in MEDIA and RSU makes an isolation action for malicious vehicles. RSU adds a record about vehicle information to blacklist in CDS. Then, RSU sends the updated blacklist to notify their nearby vehicles an event that the environment has existed malicious vehicles. When each vehicle receives blacklist, they store the blacklist record in BRT. Then, each vehicle will isolate the malicious vehicle based on the record. They do not send any message to malicious vehicles. Since the malicious vehicle can not receive any message, it can not launch message random-dropping attack to disrupt message propagation in this environment. This may ensure other vehicles to receive message successfully and driver can not pass over this message about traffic condition. Therefore, it may mitigate influence that is generated traffic accident by malicious vehicles.

In addition to this system has an isolation action that utilizes blacklist to punish for malicious vehicles, it also provides blacklist revocation mechanism for malicious vehicles. This is because this mechanism lets malicious vehicles has an incentive to forward message cooperatively. Each record has an expiration time in blacklist. When the record is out of date in blacklist, the system will erase the record to release the malicious vehicle. It encourages malicious vehicles to behave normal again.

IV. Simulation and Discussion

In this section, experimental simulations are performed to evaluate the proposed MEDIA system.

We adopt ns-2 simulator as the development environment of our experiments. A $2000m \times 2000m$ virtual road map is generated in a grid type with 200 vehicles and 81 RSUs. The size of each square grid is $200m \times 200m$. We assume each intersection of two roadways has a traffic light which has a prefixed probability to turn on its red light and stop an approaching vehicle.

For network model, we assume each vehicle and RSU support IEEE 802.11 protocol standards in the MAC layer. In addition, AODV [22] routing protocol is adopted in our experiments. Data traffic is generated with continuous bit rate (CBR). The message transmission range of a vehicle is defined as 300 meters. Each data packet size is 512 bytes in length.

TABLE I
MEDIA system parameters

Time interval to invoke evaluation scheme	15 seconds
Time interval to invoke voting scheme	30 seconds
Weighting parameter for trust value management	0.05
Weighting parameter for trust value computation	0.6
Weighting parameter for integration policy	0.7
Threshold for the number of observations	50
Threshold for message dropping rate	0.4
The first filtering threshold	0.15
The second filtering threshold	0.3

Random intersection [23] is adopted as the mobility model to simulate movement of each vehicle. The minimum moving speed is 1 km/h and the maximum moving speed is set to 1, 20, 40, 60, 80 and 100 km/h based on different simulation scenarios. In the beginning of a simulation run, each vehicle randomly selects a starting position, its driving direction and its moving speed in the map area. Notice that the moving speed of each vehicle is limited by the threshold parameters: the minimum and maximum moving speeds. If a vehicle encounters an intersection, it has 50% of probability been stopped by a red traffic light and the waiting time is 30 seconds. Each simulation run is set to 600 seconds. In order to compare the effect caused by malicious vehicles, the ratio for the number of malicious vehicles to the total number of vehicles is set to 20% and 40%, respectively. The probability for a malicious vehicle to randomly drop received messages is set to 50%. System parameters in the MEDIA system are depicted in Table I.

In order to evaluate the effectiveness of proposed MEDIA scheme, we simulate four scenarios to compare with each other. The first scenario is a hybrid VANET with malicious nodes (vehicles) in which all nodes have installed the MEDIA system; we use the term MEDIA to indicate the corresponding simulation results in diagrams shown later. The second scenario is a hybrid VANET without malicious nodes; we use the term NORMAL to indicate the corresponding simulation results. The third scenario is a hybrid VANET with malicious

nodes; we use the term ATTACK to indicate the corresponding simulation results. The fourth scenario is a hybrid VANET with malicious nodes in which all nodes have installed the VARS+RSU system; we use the term VARS+RSU to indicate the corresponding simulation results. Notice that the VARS+RSU misbehavior detection system is derived from the VARS system introduced in [19]. This system utilizes reputation concept to isolate possible malicious nodes in a VANET. To migrate the VARS scheme into a hybrid VANET environment, all RSUs in the virtual map are equipped with the same VARS system as vehicles; therefore, we name this derived system as VARS+RSU.

A. Packet Delivery Ratio

Packet delivery ratio (PDR) indicates the performance of data packet transmission in network. In this paper we define the PDR as the ratio of the number of data packets received in destination nodes to the number of data packets sent in source nodes. If a VANET suffers from message random-dropping attack, its packet delivery ratio will drop sharply.

In Figures 2 and 3, we show the simulation results among four simulation scenarios in terms of PDR, where the NORMAL scenario does not have malicious nodes in the hybrid VANET environment and the rest of three scenarios contain 20% and 40% malicious nodes, respectively. As shown in Figure 2, the MEDIA system can gain back average 66% of decrease on PDR in a VANET environment with 20% of malicious vehicles and the MEDIA system delivers average 5% more PDR than the VARS+RSU system. Similarly, the MEDIA system can gain back average 66% of decrease on PDR in a VANET environment with 40% of malicious vehicles and the MEDIA system delivers average 8% more PDR than the VARS+RSU system as shown in Figure 3.

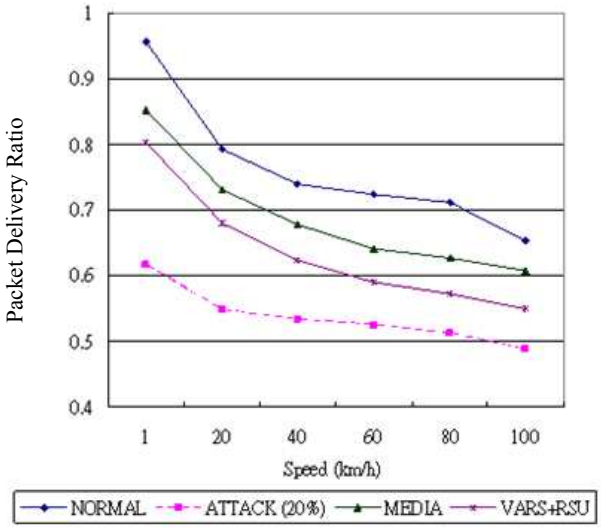

Fig. 2. Packet delivery ratio comparison among four simulation scenarios with three scenarios containing 20% malicious nodes and no malicious nodes in the NORMAL scenario.

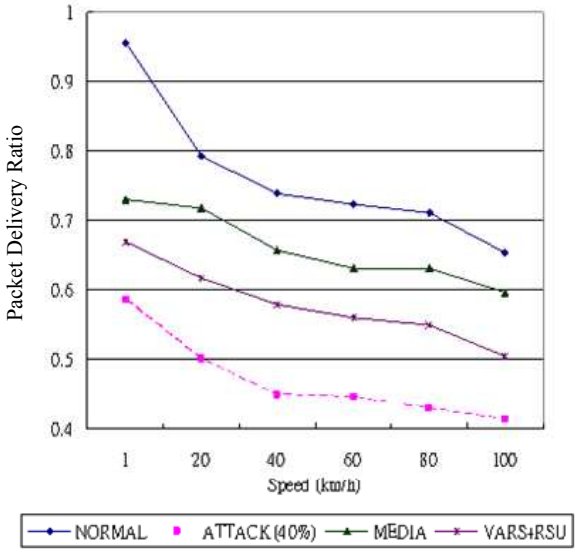

Fig. 3. Packet delivery ratio comparison among four simulation scenarios with three scenarios containing 40% malicious nodes and no malicious nodes in the NORMAL scenario.

B. Control Overhead

Control overhead is another generally used performance metric for VANET environment. In this paper we define control overhead as the number of control packets per data packet delivered, where control packet indicates both routing packet and hello packet. If a VANET suffers from message random-dropping attack, its control overhead will raise sharply.

In Figures 4 and 5, we show the simulation results among four simulation scenarios in terms of the number of control packets per data packet delivered, where the NORMAL scenario does not have malicious nodes in the hybrid VANET environment and the rest of three scenarios contain 20% and

40% malicious nodes, respectively. As shown in Figure 4, the MEDIA system can reduce average 64% of increase on control overhead in a VANET environment with 20% of malicious vehicles and the MEDIA system reduces average 2% more control overhead than the VARS+RSU system. Similarly, the MEDIA system can reduce average 60% of increase on control overhead in a VANET environment with 40% of malicious vehicles and the MEDIA system reduces average 5% more control overhead than the VARS+RSU system as shown in Figure 5.

In summary, message random-dropping attack can make serious influence on VANET performance and degrade the usability and reliability of value-added applications in hybrid VANETs. In simulation results, the case with MEDIA installed enhances average 15% of PDR and reduces average 6% of control overhead in comparison with the case that no detection system is equipped in any vehicle when 20% of vehicles are malicious. When 40% of vehicles are malicious, the case with MEDIA installed enhances about 19% of PDR and reduces about 8% of control overhead in comparison with the case that no detection system is equipped in any vehicle. The results show that MEDIA can mitigate the influence of message random-dropping attack effectively even though up to 40% of malicious vehicles exists in a hybrid VANET environment.

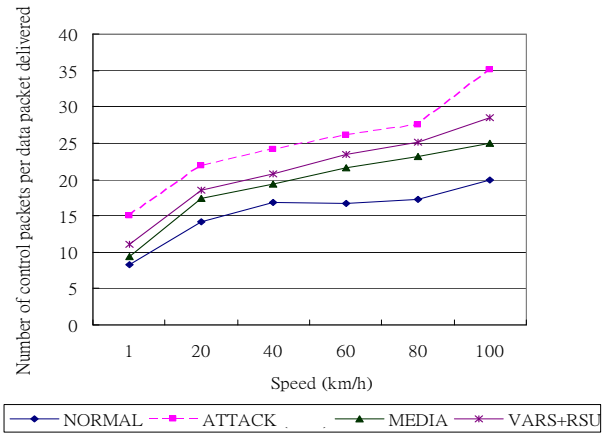

Fig. 4. Control overhead comparison among four simulation scenarios with three scenarios containing 20% malicious nodes and no malicious nodes in the NORMAL scenario.

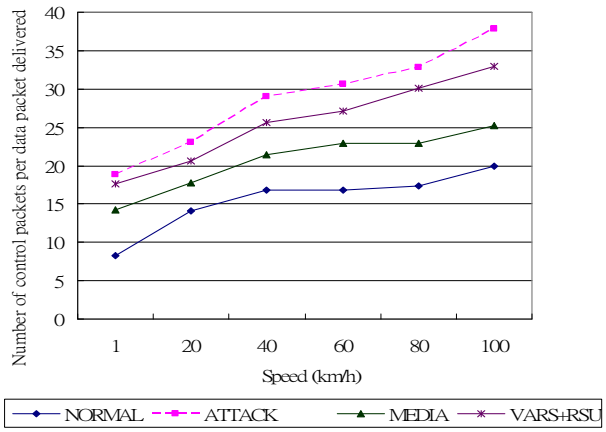

Fig. 5. Control overhead comparison among four simulation scenarios with three scenarios containing 40% malicious nodes and no malicious nodes in the NORMAL scenario.

V. Conclusion

In this paper, we develop a misbehavior detection system called MEDIA to mitigate the message random-dropping attack invoked by malicious vehicles in a hybrid VANET environment. By evaluating observed trust value of each vehicle in a pre-defined period of time, the proposed MEDIA system can identify and isolate malicious vehicles such that the degradation of network performance in terms of data packet delivery ratio and control packet overhead is largely alleviated. Based on our simulation experiments, in a VANET environment with 40% of malicious vehicles, the MEDIA system can gain back 66% of decrease on PDR in average and reduce 60% of increase on control overhead in average.

References

[1] E. Fonseca, and A. Festag, "A Survey of Existing Approaches for Secure Ad Hoc Routing and Their Applicability to VANETS," NEC Technical Report, 2006.

[2] M. Raya, and J. Hubaux, "Securing Vehicular Ad Hoc Networks," Journal of Computer Security, Vol. 15, pp. 39-68, 2007.

[3] Vehicle Infrastructure Initiative, http:/its.dot.gov/vii/.

[4] Car-to-Car Communications, http://www.car-to-car.org/.

[5] Security of Vehicular Networks@EPFL, http://ivc.epfl.ch/.

[6] Z. Wang and C. Chigan, "Cooperation Enhancement for Message Transmission in VANETs," Wireless Personal Communications, Vol. 43, pp. 141-156, 2007.

[7] M. Raya, P. Papadimitrators, I. Aad, D. Jungels, and J.P. Hubaux, "Eviction of Misbehaving and Faulty Nodes in Vehicular Networks," IEEE Journal on Selected Areas in Communications, Vol. 25, No.8, pp. 1557-1568, 2007.

[8] A. Patwardhan, A. Joshi, T. Finin and Y. Yesha, ”A Data Intensive Reputation Management Scheme for Vehicular Ad Hoc Networks,” Internetal Conference on Mobile and Ubiquitous Systems, pp. 1-8, 2006.
[9] C. Zhang, X. Lin, R. Lu and PH. Ho, ”RAISE: An Efficient RSU-aided Message Authentication Scheme in Vehicular Communication Networks,” IEEE International Conference on Communications, pp. 1454-1457, 2008.
[10] M. Raya, A. Aziz and JP. Hubaux, ”Efficient Secure Aggregation in VANETs,” Proceedings of the 3rd International Workshop on Vehicular ad Hoc Networks, pp. 67-75, 2006.
[11] X. Hong, D. Huang, M. Gerla and Z. Cao, ”SAT: Situation-Aware Trust Architecture for Vehicular Networks,” Proceedings of the 3rd International Workshop on Mobility in the Evolving Internet Architecture, pp. 31-36, 2008.
[12] F. Kong and J. Tan, ”A Collaboration-based Hybrid Vehicular Sensor Network Architecture,” Proceedings of International Conference on Information and Automation, pp. 584-589, 2008.
[13] J.-L Wang and S.-P Huang, ”Fuzzy Logic Based Reputation System for Mobile Ad Hoc Networks,” Lecture Notes in Computer Science, Vol. 4693, pp. 1315-1322, 2007.
[14] N. Nasser and Y. Chen, ”Enhanced Intrusion Detection System for Discovering Malicious Nodes in Mobile Ad hoc Networks,” Proceedings of IEEE International Conference on Communications, pp. 1154-1159, 2007.
[15] W. Yu, Y. Sun and K.Liu, ”HADOF: Defense Against Routing Disruptions in Mobile Ad Hoc Networks,” Proceedings of IEEE INFOCOM, Vol. 2, pp. 1252-1261, 2005.
[16] L. Tamilselvan and V. Sankaranarayanan, ”Prevention of Cooperative Black Hole Attack in MANET,” Journal of Networks, Vol. 3, No. 5, pp. 13-20, 2008.
[17] A. Boukerche and Y. Ren, ”A Security Management Scheme Using a Novel Computational Reputation Model for Wireless and Mobile Ad Hoc Networks,” Proceedings of the 5th ACM Symposium on Performance Evaluation of Wireless Ad Hoc, Sensor, and Ubiquitous Networks, pp. 88-95, 2008.
[18] Y. Ren and A. Boukerche, ”Modeling and Managing the Trust for Wireless and Mobile Ad Hoc Networks,” Proceddings of IEEE International Conference on Communications, pp. 2129-2133, 2008.
[19] F. Dotzer, L. Fischer and P. Magiera, ”VARS: A Vehicle Ad-hoc Network Reputation System,” Proceedings of the IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks, pp. 454-456, 2005.
[20] Y. Sun, Z. Han and K. J. R. Liu, ”Defense of Trust Management Vulnerabilities in Distributed Networks,” IEEE Communications Magazine, Vol. 46, No. 2, pp. 112, 2008.
[21] G. Theodorakopoulos and J. S. Baras, ”On Trust Models and Trust Evaluation Metrics for Ad Hoc Networks,” IEEE Journal on Selected Areas in Communications, Vol. 24, No. 2, pp. 318-328, 2006.
[22] C. Perkins, E. Belding-Royer and S. Das, ”Ad Hoc On-Demand Distance Vector (AODV) Routing,” IETF RFC 3561, July, 2003.
[23] N.W. Lo and H.-C Tsai, ”Illusion Attack on VANET Applications - A Message Plausibility Problem,” Proceedings of the 2nd IEEE Workshop on Automotive Networking and Applications, pp. 1-8, Nov. 26-30, 2007.